Institut für Informatik
Universität Potsdam

Quantum Cryptography

Security Analysis of Multiuser Quantum Communication with Embedded Authentication

Diplomarbeit

eingereicht am
Lehrstuhl für Theoretische Informatik
bei Prof. Dr. Christoph Kreitz
und Dr. Eva Richter

eingereicht von
Carolin Lunemann
Matrikelnummer: 720029
Studiengang Diplom-Informatik
carolin.lunemann@web.de

Potsdam, den 07. Dezember 2006

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig und ohne fremde Hilfe angefertigt und mich anderer als der im beigefügten Verzeichnis angegebenen Hilfsmittel nicht bedient habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und nicht veröffentlicht.

Potsdam, den 07.12.2006

C. Lunemann

Folgenden Personen möchte ich für ihre Hilfe danken: Herrn Prof. Dr. Kreitz für die sehr gute Betreuung, Frau Dr. Richter für die Bereiterklärung zur Zweitkorrektur, Carsten für aufschlußreiche Diskussionen der englischen Sprache und der Sprache allgemein, meinen Eltern für ihre Unterstützung während der letzten Jahre und meiner Schwester für die “erste Hilfe”.

Abstract. Three quantum cryptographic protocols of multiuser quantum networks with embedded authentication, allowing quantum key distribution or quantum direct communication, are discussed in this work (Hong et al., 2006, Lee et al., 2005, 2006). The security of the protocols against different types of attacks is analysed with a focus on various impersonation attacks and the man-in-the-middle attack. On the basis of the security analyses several improvements are suggested and implemented in order to adjust the investigated vulnerabilities. Furthermore, the impact of the eavesdropping test procedure on impersonation attacks is outlined. The framework of a general eavesdropping test is proposed to provide additional protection against security risks in impersonation attacks.

Contents

Appendices

Chapter 1

Introduction

Cryptology is the science of secure communication (*kryptos (gr)* means *hidden*). It is comprised of cryptography and cryptoanalysis, i.e. the art of code-making and the art of code-breaking, respectively. The purpose of cryptographic communication is to hide the content of the transmitted message from unauthorised disclosure but not the transmission itself as in steganography. In technical literature the term cryptography is often used to describe the entire field of cryptology.

The method of concealing the content of a message is called encryption or encoding. Its inverse process – recuperating the original content – is named decryption or decoding. A cryptographic algorithm, called cipher or code, is used for encryption and decryption. In combination with one or two keys it codes plaintext to ciphertext and vice versa.

Modern cryptographic methods are developed in accordance with Kerckhoffs' principle. It was published as one of six design laws for military ciphers (Kerckhoffs, 1883) and requires that the security of a cryptographic system must depend only on the secrecy of the key. The cipher itself can be public knowledge. Shannon reformulated the principle as "the enemy knows the system being used" (Shannon, 1949, p. 662). Compliance with Kerckhoffs' principle offers two main advantages. First, if the cipher is public during its creation, experts may discuss its quality, resulting in substantiated security analysis. And second, "Kerckhoffs's principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point." (B. Schneider in Mann (2002), p. 4). Hence, the fewer information must be kept secret, the easier the security of the system is maintained.

Cipher systems must meet the following requirements. *Data confidentiality* refers to successful concealment of the message, so that only legitimate parties gain information of its content. It is synonymous with data secrecy and privacy. *Data integrity* addresses the validity of the content. It can be compromised by unauthorised alteration, which the legitimate parties must detect. The aspect of *authentication* is mostly subdivided into user and data authentication. Any user must be authenticated, i.e. identified as legitimate, otherwise a third party may impersonate him. Data authentication proves the origin and the content of transmitted information. Hence, it is closely related to user authentication and data integrity. *Non-repudiation* holds any user responsible for actions during previous communication.

Cryptographic strength is measured by the time and the resources it would require to recover the plaintext without the key. The highest level of security is unconditional security. It offers unconditional protection against an attacker who has access to unlimited computational and technological power.

Secret communication goes back to the beginnings of our civilisation. The first cryptographic method is known as private-key or symmetric cryptography. Corresponding ciphers are based on a private key, shared between two communication parties. Symmetric cryptography developed from monoalphabetic substitution to more complex polyalphabetic substitution ciphers. Furthermore, ciphers were designed, combining substitution and supplementary ciphers, such as transposition, homophony, or polygraphy. A famous monoalphabetic substitution cipher is the Caesar cipher, named after the first recorded user Gaius Iulius Caesar (100 B.C. – 44 B.C.). An example for polyalphabetic encryption is the Vigenère chiffre published in 1585, "le chiffre undéchiffrable" for nearly 300 years until Babbage and later Kasiski deciphered it. Substitution ciphers are vulnerable to frequency analysis, the first known method of cryptoanalysis, which was published in the 9th century by Al-Kindi. Any language, written in single letters, has a characteristic letter frequency. Certain letters or combinations of letters, as bigrams or trigrams, occur with varying frequencies. Substitution ciphers preserve such plaintext patterns in the ciphertext.

At the beginning of the 20th century, polyalphabetic substitution was implemented mechanically in rotor cipher machines, e.g. the Enigma, to achieve more ciphertext complexity. The development of computers led to the possibility of using more cryptographic operations and a very large binary alphabet. The substitution concept was implemented in bit-oriented block ciphers, in which the letters are transformed to bits via ASCII code. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are examples of block ciphers, published as standards in 1977 and 2001, respectively.

Symmetric cryptography suffers from the logistic problem of key distribution. The secret key must be distributed to two parties before secure communication. This simple fact became the biggest problem of cryptography, especially with the development of the internet and the proliferation of electronic communication systems. Moreover, key distribution represents the most vulnerable phase in the communication process. According to the often quoted proverb of cryptography that "a chain is only as strong as its weakest link", key distribution also affects the security of any symmetric encryption to a great extent.

Public-key cryptography (asymmetric cryptography) is the technological revolution which solves the key distribution problem. It is based on a pair of asymmetric keys. A message is encrypted with the public key of the receiver. The resultant ciphertext is unreadable and can be securely sent. Only the receiver can decrypt the message with his private key. The private key corresponds to the public key via a mathematical one-way function in order to achieve computational infeasibility of its deduction from the public key. Hence, the public key can be published without compromising security. A certification authority authenticates the public key as key of the legitimate user.

The new cryptographic concept was published by Diffie and Hellman (1976). In 1978 Rivest, Shamir, and Adleman provided the first practical implementation, the RSA encryption (Rivest et al., 1978). It is based on the hard mathematical problem of factoring large numbers as one-way function. Later it was acknowledged that public-key cryptography had already been invented in 1969 as "non-secret communication" by Ellis, followed by Cocks' and Williamson's discovery of the one-way function factorisation around 1973. Since they all worked for the UK government communications headquarters (GCHQ), the publication of their ideas was restricted.

Public-key cryptography solves the key distribution problem, but it cannot provide unconditional security. It is based on the (current) impracticality of solving hard mathematical problems. Quantum computers could speed up the solution of these problems. In 1993 Shor published an algorithm which could, in principle, perform factorisation of large numbers with a quantum computer in polynomial time. It has not been determined yet, if a quantum computer can ever be developed to a sufficient level. But assuming its construction, it would render all existing classical techniques obsolete, except for one.

Only one classical cipher, Vernam's symmetric one-time pad, offers unconditional security, which was mathematically proven by Shannon. Each plaintext bit is combined through a xor-operation with the key character at that position. Hence, the resultant ciphertext is completely random. The one-time pad is impractical for three reasons, though. As it is a symmetric cipher based on one private key, key distribution problems are inevitable. To provide unconditional security the key must be "real random" and of the same length as the message. Furthermore, the same key can be used only once. If one of these conditions is violated, the one-time pad is no longer unbreakable.

Another concept which withstands the capability of quantum computing is quantum cryptography. It "lies at the intersection of quantum mechanics and information theory" (Gisin et al., 2001, p. 2) and utilises basic laws of quantum mechanics, which were discovered and formalised during the last century, for cryptographic purposes. Quantum cryptography was established in 1984 by Bennett and Brassard. Ekert's independent study produced the same results in 1991 without any knowledge of the previous work. Quantum cryptography provides unconditional secure key distribution and direct secure communication. The key, obtained from key distribution, is mostly used with the one-time pad, so that the unconditionally secure symmetric technique becomes feasible. Most recently, quantum multiuser networks have been researched. Thus, improvement and development of applicable authentication methods are essential.

This work analyses three different protocols for quantum key distribution and quantum direct communication in the aspect of authenticated multiuser networks. It is organised as follows. Chapter 2 briefly introduces the fundamentals of quantum cryptography. Chapter 3 outlines the general framework of this work. In chapters 4 – 6 the protocols are discussed and analysed, and additional improvements are suggested. Chapter 4 focuses on the *Quantum Authentication and Quantum Key Distribution Protocol* (henceforth protocol 1) published by Lee et al. (2006) as an arXiv eprint. In chapter 5 the protocol *Quantum Direct Communi-*

cation with Authentication is analysed. This protocol, called protocol 2 from here on, was released by Lee et al. (2005) both at arXiv and in Physical Review A. Chapter 6 discusses the protocol *Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping* published as an arXiv eprint by Hong et al. (2006) and henceforth called protocol 3. The work closes with a brief conclusion in chapter 7.

Chapter 2

Preliminary Basics

This chapter briefly introduces the fundamentals of quantum cryptography. Section 2.1 provides an overview of the basic principles of quantum mechanics. Section 2.2 describes two contemporary kinds of secret quantum communication, quantum key distribution (QKD) and quantum direct communication (QDC). Additionally, the concept of identity authentication within quantum communication settings (QIA) is discussed.

2.1 Quantum Mechanical Basics

This section briefly explains the basic fundamentals of quantum mechanics, which are most important for quantum information theory. It does not intend to give a complete account of comprehensive quantum theory with all its physical phenomena and counterintuitive paradoxa of classical conception. It mainly focuses on mathematical models of the physical system following Bouwmeester et al. (2000), Heiss (2002), Homeister (2005), and Marinescu and Marinescu (2005). The "philosophic" aspects of quantum theory are not discussed.

2.1.1 Superposition and Uncertainty

The most fundamental entity in quantum information theory is a quantum bit, called qubit. The state of an unpolarised qubit is mathematically represented as a vector of unit length in a two-dimensional complex vector space with an inner product and its associated norm (a two-dimensional Hilbert space, also called unitary space). It can be written in the traditional ket-notation of quantum mechanics, the Dirac notation, as in equation (1)

$$\begin{aligned} |\Omega\rangle &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \alpha|0\rangle + \beta|1\rangle \end{aligned} \tag{1}$$

with $\{|0\rangle, |1\rangle\}$ as basis of the vector space.

α and β are complex coefficients, called probability amplitudes, which satisfy the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$. As equation (1) shows, a qubit can be in any state which is a linear combination of the basis states $|0\rangle$ and $|1\rangle$. Hence, in contrast to a classical bit, which is either 0 or 1, the state of a qubit is undetermined. It is in a coherent superposition of $|0\rangle$ and $|1\rangle$. The "quintessential experiment on quantum superposition" is Young's double-slit experiment (Bouwmeester and Zeilinger, 2000, p. 1). Various exemplifications also deal with the phenomenon, such as Schrödinger's famous Gedankenexperiment *Schroedinger's cat* (Schrödinger, 1935) or Bruß' allegory of the Mona Lisa being both happy and sad (Bruß, 2003).

To determine its state a classical bit can be read, whereas a qubit must be observed, i.e. measured. Measuring a quantum state mathematically requires the projection of the state vector onto the two basic states. The measurement outcome depends on the amplitudes α and β. The probability of the outcome $|0\rangle$ or $|1\rangle$ is the square of its probability amplitude, i.e. $|\alpha|^2$ or $|\beta|^2$, respectively. Hence, any measurement represents an interference with the environment (decoherence) and destroys the superposition. The state is no longer uncertain after the observation.

The polarisation of a qubit is used to store a bit of information. Measuring the polarisation of a quantum state simultaneously in nonorthogonal axes is not feasible, since these bases represent incompatible observables according to a Heisenberg uncertainty principle. A quantum state cannot possess a determined value for both observables, so that only orthogonal states are distinguishable. This work uses the following polarisation axes as measurement bases: the horizontal/vertical axis $z = \{|0\rangle, |1\rangle\}$ and the 45° rotated basis $x = \{|+\rangle, |-\rangle\}$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Another important phenomenon in quantum cryptography is the fact that (perfect) cloning of an unknown quantum state is in conflict with the basic laws of quantum mechanics. The laws bar an exact copy of an undetermined qubit, as proven in the no-cloning theorem (Wootters and Zurek, 1982).

2.1.2 Unitary Transformations

Individual states quantum mechanically combine through the tensor product, e.g.

$$|1\rangle \otimes |0\rangle \;=\; \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle \;. \tag{2}$$

The state of a qubit can be changed by unitary transformation. Any calculation of a qubit is described by the multiplication of its state with a unitary matrix, i.e. a matrix M with $(M^*)^T = M^{-1}$, where $(M^*)^T$ denotes the transposed complex conjugate matrix and M^{-1} represents the inverse matrix.

The following unitary operations are applied in this work:

- Identity operation I with the matrix

  $$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

  and the results $I(|0\rangle) = |0\rangle$, $I(|1\rangle) = |1\rangle$, and $I(\alpha|0\rangle \pm \beta|1\rangle) = \alpha|0\rangle \pm \beta|1\rangle$. Performing I on a qubit is equivalent to leaving the particle untransformed.

- Hadamard operation H with the matrix

  $$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

  and the results $H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and $H(\alpha|0\rangle \pm \beta|1\rangle) = \frac{1}{\sqrt{2}}(\alpha(|0\rangle + |1\rangle) \pm \beta(|0\rangle - |1\rangle))$.

- Bitflip operation (on a qubit) X with the matrix

  $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  and the results $X(|0\rangle) = |1\rangle$, $X(|1\rangle) = |0\rangle$, and $X(\alpha|0\rangle \pm \beta|1\rangle) = \alpha|1\rangle \pm \beta|0\rangle$.

- Pauli-Z operation σ_z with the matrix

  $$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  and the results $\sigma_z(|0\rangle) = |0\rangle$, $\sigma_z(|1\rangle) = -|1\rangle$, and $\sigma_z(\alpha|0\rangle \pm \beta|1\rangle) = \alpha|0\rangle \mp \beta|1\rangle$.

Unitary operations offer two important features. They conserve the inner product, so that any unitary operation also provides its inverse transformation, e.g. $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle$. Furthermore, any unitary operation is preserved regardless of the measurement basis.

2.1.3 Entanglement and Entanglement Swapping

Entanglement (*Verschränkung*) refers to a quantum system in a superposition state with two or more (anti)correlated subsystems. An entangled state cannot be written as a tensor product of its individual states. Measurement of one particle of the system determines the state of the other particle, even if the qubits are separated from each other. Moreover, the perfect correlations between the outcomes are "basis-independent" (Bouwmeester et al., 2002, p. 151). Entanglement of particles is realised by a common source or their interaction.

Hence, entanglement allows that "widely separated particles can cooperate in an almost psychic fashion" (Feynman in Marinescu and Marinescu (2005), p. 9). Schrödinger first discovered the phenomenon, which lacks any classical analogy. This nonlocal *spukhafte Fernwirkung* (spooky action at a distance), as Einstein famously called it (QE, 2006), is assumed to be the most controversial subject of quantum theory, discussed e.g. in the famous EPR paradoxon (Einstein et al., 1935).

Bipartite Bell states (eqs. (3) – (6)), which are also termed EPR states, and tripartite GHZ states (eq. (7)) are entangled systems. They are presented in the following common notation in this work:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{3}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \tag{4}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \tag{5}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{6}$$

$$|\Theta\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{7}$$

The qubits of states $|\Phi^\pm\rangle$ and $|\Theta\rangle$ are perfectly correlated, i.e. after measurement they are in the same determined state. The particles of states $|\Psi^\pm\rangle$ are perfectly anti-correlated, that is, they are in opposite states after observation.

The process of transferring entanglement via "a noninteractive quantum measurement" (Zukowski et al., 1993, p. 4287) is called entanglement swapping (ES). Appropriate projection measurement of two particles of different origin and entangled within different systems onto an entangled state automatically collapses the states of the other two qubits into an entangled state. The non-measured qubits do not physically interact with one another, nor do they share a common past. Entanglement swapping can be performed by Bell basis measurements (see eq. (8)), i.e. projecting the qubits 1 and 3, entangled with the particles 2 and 4, respectively, onto the Bell basis. The combined Bell state of the newly entangled particles 2 and 4 is in equal superposition of all four Bell states, since the polarisation of the states is undetermined. Furthermore, upon the projection of particles 1 and 3, e.g. onto state $|\Psi^+\rangle_{13}$, qubits 2 and 4 are automatically projected onto state $|\Psi^+\rangle_{24}$ without directly interacting.

$$\begin{aligned}
|\Psi\rangle_{1234} &= |\Psi^+\rangle_{12} \otimes |\Psi^-\rangle_{34} \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_3|0\rangle_4 + |1\rangle_3|1\rangle_4\right) \\
&= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{1234} \\
&= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{1324} \\
&= \frac{1}{2}\left(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24} + |\Phi^-\rangle_{13}|\Phi^-\rangle_{24} + |\Psi^+\rangle_{13}|\Psi^+\rangle_{24} + |\Psi^-\rangle_{13}|\Psi^-\rangle_{24}\right)
\end{aligned} \tag{8}$$

Any secret communication discussed in this work is based on entangled systems. The properties of their entanglement guarantee security during transmission, since the particles are perfectly correlated for undisturbed transfer. In an entangled system a single qubit does not carry any information. According to Homeister (2005), the information is between the qubits in the correlations (p. 135).

2.2 Quantum Cryptographic Basics

Quantum cryptography applies the properties of quantum systems to cryptographic concepts. Its purpose is the protection of classical information, i.e. the key in quantum key distribution or the message in quantum direct communication, from any kind of unauthorised disclosure. Quantum cryptography developed from Wiesner's idea that "quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics" (in *Conjugate Coding*, written in the 1970's and published in 1983, see e.g. Gisin et al. (2001) for more details). He proposed the use of nonorthogonal states to provide his approach of quantum money with a non-clonable mechanism. This suggestion was taken up in the first quantum cryptographic proposal in 1984.

Quantum cryptography requires at least one quantum channel for qubit transmission and one classical channel. Information exchanged over classical channels can be intercepted without recognition. In contrast, interception of quantum transfer is automatically detected, since a quantum system can only be observed by measurement, which in turn disturbs the system. After quantum transmission the comparison of particles on a classical channel during public discussion reveals any previous eavesdropping on the quantum link. Thus, quantum cryptography offers automatic "intrusion detection mechanism", which provides a "totally new contribution to the field of cryptography" (Lomonaco, 1998, p. 27 and 7).

Secret communication over a quantum channel requires quantum cryptography. In the literature quantum cryptography is mostly abbreviated as QC. This work uses the abbreviation for secret quantum communication. Quantum communication refers either to quantum key distribution or to quantum direct communication, if the respective procedure is apparent from the context. In this work a perfect environment is assumed, including perfect, noise-free quantum channels and perfect apparatus of quantum sources and detectors.

The traditional cryptographic names of the communicating parties are Alice, for the sender, and Bob, for the receiver. The names of supplementary parties in multiuser settings are added in alphabetic order, i.e. Carol or Charlie, Dave and so forth. An attacker is called Eve or Evan, derived from eavesdropping, or Mallory, from malicious.

2.2.1 QKD

Quantum key distribution (QKD) is used as complement to classical private-key cryptography. Its objective is the arrangement of a secret, binary key, shared between two communication parties Alice and Bob. The key is applied to a symmetric cipher. The sender Alice encodes her

classical message with the key and sends the resultant ciphertext over a classical channel to the receiver Bob. Since Bob possesses the same key, he can decrypt the ciphertext and retrieve the original plaintext. Vernam's one-time pad is recommended for the symmetric encryption, since only this cipher offers unconditional security in the sense of Kerckhoffs' principle. To provide this highest level of security the key must be absolutely secret and random. Moreover, it can be used only once – a limit that led to the key distribution problem. QKD offers a solution to this problem. It substantially facilitates distribution of a "real random", secret key over long distance.

There are two main concepts of key distribution via quantum states. First, the key can be encoded in a set of nonorthogonal quantum states. Alice prepares quantum states in at least two incompatible bases and transmits the polarised qubits to Bob. Bob randomly selects one of the bases and measures each incoming particle in it. After the transmission and the measurements Alice and Bob publicly compare their chosen bases. They reject all particles which they measured in incompatible bases. Alice's and Bob's outcomes coincide for compatible measurements and form the shared raw key. After a successful public eavesdropping test, in which Alice and Bob randomly check bits of the raw key for expected correlations, they hold a shared sifted key. The procedure ensures a secret key, since any eavesdropping on the quantum transmission is detected in the eavesdropping test. Furthermore, the random choice of the basis for preparing and measuring the particles, as well as their random selection of check bits, excluded from the final sifted key, guarantees randomness of the key.

The second approach of QKD is based on pairs of entangled states. Each party receives one particle of the entangled pair. Alice and Bob then measure their qubits in one of at least two incompatible bases of random choice. In the public discussion, following the distribution of the particles, they compare their bases and reject the outcome for different bases. If they measured in the same basis, the measurement results form the shared raw key. Alice and Bob check key bits for unexpected irregularities from eavesdropping during the transmission. If the test is successful, they receive a secret and random sifted key. This approach offers the advantage that there is no information encoded in the transmitted particles. The key comes into existence only after an undisturbed transmission.

In 1984 Bennett and Brassard proposed the first QKD protocol, known as BB84 protocol (Bennett and Brassard, 1984). It is based on single particles and operates with four states which constitute two nonorthogonal bases. In 1991 Ekert published the EPR protocol (Ekert, 1991), discovering quantum cryptography independently of Bennett and Brassard. His protocol rests upon entangled EPR pairs and three nonorthogonal axes. In 1992 all three "founding fathers" (Gisin et al., 2001, p. 9) published *Quantum Cryptography* together (Bennett et al., 1992a) and, thereby, established the new discipline.

Since then many variations of the first protocols have been published, as QKD progressed quickly over the last years in both theory and implementation. Most of the protocols are probabilistic, i.e. same measurement bases are chosen with a certain probability and only the outcomes of compatible bases form the key. Depending on the respective protocol, a certain amount of key bits is rejected. Hence, not all qubits contain one bit of information.

2.2.2 QDC

In 2001 Beige, Englert, Kurtsiefer, and Weinfurter developed the new cryptographic scheme of direct communication from the solution of the so-called mean-king problem (Beige et al., 2002a,b, Englert et al., 2001). Quantum direct (secure) communication (QDC or QDSC) allows direct transfer of a secret message without previous key arrangement, i.e. the message is directly encoded in the transmitted qubits. Therefore, the transmission must be deterministic rather than probabilistic. If each particle supplies one bit (under idealistic conditions) and Alice can determine the bit value Bob decodes, it is possible to transmit a message directly over quantum channels.

In QKD the beforehand step of distributing a secret key ahead of the secret message exchange reduces the efficiency of the communication. In QDC the communication proceeds in only one step, and due to its deterministic nature, no transmitted qubit is wasted. Since the message is directly transmitted over quantum links, a QDC scheme is more demanding for security. The sender's secret message is only intelligible to the receiver and cannot leak to an unauthorised party or be modified unnoticed by an attacker, i.e. any "eavesdropper cannot only be detected but also obtains blind results" (Deng et al., 2003, p. 1).

The first proposed protocol is based on a "publicly known key" and two-particle states of single qubits with two completely indistinguishable subspaces (Beige et al., 2002a,b). The subspaces constitute two nonorthogonal bases and evenly span the (four-dimensional) Hilbert space, so "the bit in transmission is perfectly concealed in the state space" (Beige et al., 2002b, p. 3). The message and the randomly generated key determine the sender's choice of states. He transmits the qubits to the receiver and he measures all received particles randomly in one of the two nonorthogonal bases. After the transmission is completed, Alice and Bob randomly check inserted check qubits. If the transfer was secure, Alice publicly announces her key, which Bob needs to extract her message.

Shortly after the first protocol Boström and Felbinger suggested an "instantaneous" scheme, which allows direct communication without the additional information of the key (Boström and Felbinger, 2002). In their *ping-pong protocol* the encoded message is directly revealed to Bob. Classical information is communicated only in the control mode, in which the transmission security is checked. The protocol operates with entangled Bell states. One qubit – the home qubit – stays securely at Bob's place and the other qubit – the travel qubit – is transmitted to Alice (*ping*). Alice encodes her secret message in the travel qubits performing specified unitary operations. After Bob receives the travel qubits back (*pong*) he performs Bell measurement on his home qubit and the encoded travel qubit. The operations of Alice result in distinguishable Bell states and Bob can extract the message. Hence, each transmission between Bob and Alice (*ping-pong*) transmits one bit of information.

Many other QDC protocols use the *ping-pong* feature, i.e. a qubit travels to collect information, which is encoded by unitary operations. The protocols are based on single particles in mixed states or entangled states, such as bipartite EPR states or tripartite GHZ states.

Some recently published QDC schemes offer additional features for the direct communication process. Some protocols allow bidirectional communication in a so-called quantum

dialogue, in which both users can send their messages simultaneously (e.g. Nguyen (2004), Zhang (2004), Zhu et al. (2006) or Xia et al. (2006b)). Other protocols develop the beginnings of multiparty communication (Gao et al., 2005, Jin et al., 2006) or use entanglement swapping, e.g. Zhang and Man (2004a,b) with EPR states, and Xia et al. (2006a) with GHZ states and the introduction of a third party. The main benefit of transmitting the message via entanglement swapping is that no qubit encoded with a message bit must be exchanged over a channel after the particles of the entangled states are shared successfully.

In principle, QDC protocols also serve the purpose of QKD. To guarantee the randomness of the key Alice must perform the operations randomly. The disadvantage is that Alice proposes the entire key. Hence, it is only as random as Alice's operations, since Bob's actions do not influence the final key bits. The missing fairness, as emphasized in most cryptographic protocols, is even more concerning.

2.2.3 QIA

In line with the first two principles of modern cryptography, confidentiality and integrity of data, most of the discussed protocols provide high security against a wide range of attacks. The secrecy of exchanged information is ensured, since an eavesdropper only obtains blind results of the key or the message. Its integrity is guaranteed by the automatic detection of eavesdropping. The third aim, user authentication, is achieved, if the self-enforcing assumptions hold. The protocols assume a point-to-point connection, which can be accessed only by legitimate users. For public discussion an unjammable, authentic channel is assumed. An eavesdropper may listen in on the link, but cannot modify the exchanged information. These basic assumptions cannot be maintained under realistic conditions. Particularly, considerations of implementing quantum networks must include quantum identification authentication (QIA). Data authentication is provided, if data integrity and user authentication are implemented. If necessary, non-repudiation may be achieved by other methods, which are not discussed here.

The protocols are completely insecure in an impersonation or a man-in-the-middle attack without the prevailing conditions. The attacker Eve can impersonate a user during the communication and intercept the secret message (impersonation attack). Assuming Alice as the sender initialises the communication, there are two different kinds of impersonation attacks for QKD or QDC. If Eve intends to read Alice's message, she replaces the receiver Bob. She must intercept Bob's quantum and classical channels and complete his protocol tasks. This way Eve either distributes a shared key with Alice (QKD), which she can use to decode Alice's classical message, or she can extract the message directly from the system (QDC). If Eve successfully impersonates Alice, she can send Bob a message of her choice in Alice's name.

A man-in-the-middle attack is the implementation of both impersonation attacks, i.e. Eve impersonates both communication parties simultaneously. If she is successful, Eve completely controls the communication as the man-in-the-middle. In QKD Eve obtains two different keys k_{Alice} and k_{Bob}. She can decode and read Alice's classical message to Bob with the key k_{Alice},

shared between her and the sender, and write and encode a message to Bob with the key k_{Bob}, shared between her and the receiver. In a man-in-the-middle attack in QDC Eve extracts and reads Alice's message, which is directly sent to her. She then sends her own message or Alice's modified message directly to Bob.

In both attacks it is unlikely that Eve will be detected, since her attack does not cause any errors in the system. During the entire communication neither Alice nor Bob recognise her intervention.

The first QIA concept is based on a secret key, initially shared between Alice and Bob. Comparing this string during QC, Alice and Bob can verify their identities. The first protocol of this concept was published in 1995 (Crépeau and Salvail, 1995). It proposes an identification technique based on quantum oblivious transfer. Therefore, the legitimate parties can check their identities without disclosing the key. Eve may have to enter the protocol an exponential number of times to gain non-negligible information.

The idea of authenticating public discussion with the initial key realised the QIA concept differently after quantum oblivious transfer was proven insecure. Alice and Bob compare the initial key over a classical channel during the public discussion of QC. Since this phase is an inherent part of any protocol, its authentication prevents attacks against the entire communication. Eve cannot impersonate a legitimate user without possessing the key. Dušek et al. (1999) describes several methods of checking the initial secret during public discussion and suggests using the secret string only once to prevent later misuse. Since QKD provides the parties with a longer secret key, a new secret string can be "refueled from a shared provably secret key" (Dušek et al., 1999, p. 1) for future communication between the same users. Due to this self-sustaining feature, QKD protocols are *quantum secret growing protocols* or *key expansion protocols*. Zeng and Guo (2000) suggest implementing the authentication process with symmetric cryptography. The key bits determine measurement bases onto which Alice and Bob project their respective particles of EPR pairs. Alice and Bob translate the received measurement outcomes to a binary sequence and encode it with the key. The resultant ciphertext verifies their identities. Gao et al. (2004) propose a scheme of embedding an identification protocol in the QKD procedure. After successful authentication, based on EPR pairs and symmetric cryptography, the remaining EPR pairs are used for key distribution.

The quantum counterparts of the classical, initial string are initially shared entangled states, a concept first published in 1999 (Barnum, 1999). The parties use entangled pairs of particles as a catalyst to perform actions, which are impossible without the catalyst. Bob sends Alice his particles, which she projects onto the Bell basis. If her measurement results in the expected Bell state, Bob is authenticated. This quantum scheme offers several advantages over its classical counterpart. The replacement of quantum states is detected in the next communication between the legitimate parties, whereas classical information can be copied without recognition. Moreover, a stolen key allows communication with both parties. Authentication with entangled states is limited to the user who possesses the other entangled particle. Most important is the impossibility to give away copies of the particles. In Barnum's protocol only one-way authentication is proposed. It underachieves its potential of

authentication of both parties and of embedding the authentication procedure in QC. Jensen and Schack (2000) and Zhang et al. (2000) enhance the concept. The latter protocol proposes authentication in a *ping-pong* way with the travel qubit as challenge particle. This way the entangled pairs can be reused, even though the security slightly decreases. Shi et al. (2001) provides a simultaneous realisation of QKD and QIA. Bob randomly encodes his particles of the entangled states by performing operations and sends them to Alice, who measures both particles in the Bell basis. She recognises the legitimacy of the received particle and simultaneously extracts Bob's encoded information, which can be used as key.

Providing secret, initial strings or entangled states to all communication parties leads to distribution problems, which are actually intended to be solved by quantum cryptography. In 2000 a new concept was published in which Alice and Bob do not initially share a secret key or entangled states (Zeng and Zhang, 2000). It is based on the authentication technique of Zeng and Guo (2000), but a third party (henceforth called Trent) is introduced to generate the initial secret. Trent is an authority who shares a secret identification information (ID) with each registered user. He establishes this ID by means of conventional forms of identification, e.g. a personal authentication. The ID must be of sufficient length to cover several communication rounds. After successful authentication via Trent the parties can use the remaining particles for QKD. The concept of a third party was taken up in Ljunggren et al. (2000). There Trent provides the communication parties with entangled particles for their identity check. With Trent as the source of the particles, Alice relies on Bob's legitimacy and vice versa. The users can proceed with QKD with the particles remaining after the authentication process. Both protocols assume an authenticated, unjammable quantum link between Trent and each user. Such a connection may not be implemented under realistic conditions, so Eve may still impersonate Trent or any other user. Mihara (2002) proposes an authentication protocol based on GHZ states. Each party encodes the respective particles according to her or his ID. After certain operations and measurements Trent extracts the encoded information and compares it to the original ID. Since this protocol does not combine the authentication technique with any QC procedure, the identity of the communication parties is not guaranteed in subsequent communication. Eve may leave the authentication procedure undisturbed and start her impersonation attack once it is completed.

In 2005/2006 Lee, Lim, and Yang published another authentication approach which includes the authority (Lee et al., 2005, 2006). It may be implemented in a quantum network without key distribution problems, due to a renewable authentication key generated with the ID. The authority Trent prepares GHZ states and generates a new authentication key for each communication round. He encodes Alice's and Bob's particles of each GHZ state with their respective authentication key and transmits them. Alice and Bob also generate their keys to decode the particles. After correct decoding the particles are restored to their original state. Hence, Alice and Bob can compare particles during public discussion to check their identity. Moreover, they can proceed with QKD or QDC on the remaining, restored qubits. The authentication concept is discussed in detail in the following chapters (see also fig. 1 – fig. 3). Wang et al. (2006) adapt the concept of the authentication key to another authentica-

tion method, which provides multiparty simultaneous authentication. It must be considered, though, that authentication, which is not integrated into the communication procedure, does not guarantee authenticated QC.

A method with a network authority was already proposed in 1996 (Biham et al., 1996). The paper discusses the implementation of a quantum network, which features authenticated communication automatically. Alice and Bob must visit Trent's center once to program single particles for subsequent QC. At Alice's request, Trent projects her and Bob's particles onto an entangled state. Therefore, he creates correlations between the particles providing a basis for QC. Since Alice and Bob must personally visit the authority, their identities are verified. The network works at any distance without requiring quantum channels, therefore, impersonation attacks are excluded.

Chapter 3

Multiuser Quantum Communication with embedded Authentication

The chapter outlines the general framework of this work. It gives an overview of the three protocols (see figures 1, 2, and 3, pp. 18) which are discussed and analysed in the following chapters. All protocols are applied to multiuser quantum networks, in which two network parties are able to communicate without direct quantum links (s. 3.1). The embedded authentication process on the basis of an authentication key guarantees that only legitimate parties attend quantum communication. The concept of the authentication key is introduced in section 3.2. The authentication approach meets realistic requirements, since the users are not in possession of any kind of initially shared information. To protect the test procedure against security risks the framework of a general eavesdropping test is proposed (s. 3.3). Any test in the protocols must proceed according to this general procedure. Section 3.4 provides the basic definitions and methods of the security analyses in this work.

(A1) At the request of the "communication initialiser" Alice, the third party Trent prepares tripartite GHZ states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$. The subscripts A, T, and B denote the respective user Alice, Trent, and Bob.

(A2) Trent encodes the A-particle of each state with Alice's authentication key. He performs an identity operation, if the key value is 0. For the key value 1, he executes a Hadamard transformation. Accordingly, Trent encodes each B-particle with Bob's authentication key. He sends the users their encoded qubits.

(A3) After reception Alice and Bob perform the same unitary operations as determined by their keys. Correct decoding restores the GHZ states to their original state.

(A4) Alice and Bob complete the first eavesdropping test. They select check qubits on random positions, measure them in the z basis, and compare the outcomes over a public channel. In case of a successful test, i.e. their results coincide, the quantum transmission was undisturbed. Moreover, they are authenticated via Trent. If there are irregularities during the test, communication is aborted.

(C1) For QKD Alice and Bob randomly perform unitary or Hadamard operations on their remaining qubits.

(C2) Bob sends his encoded B-particles to Alice.

(C3) Alice performs Bell basis measurements on pairs consisting of an A-particle and a B-particle. Trent measures his T-particle in the x basis and announces the outcome publicly.

(C4) Alice can infer Bob's operations from the transformation of the system. Bob's operations form the raw key.

(C5) Alice and Bob accomplish the second eavesdropping test. They agree on a control subset and compare the corresponding values in dialogue form. If their results coincide, they share a secret key. Otherwise, the protocol is aborted.

Figure 1: Protocol 1 – Authenticated MQKD
Quantum Authentication and Quantum Key Distribution Protocol (Lee et al., 2006). The enumeration letters A and C denote the authentication and communication process, respectively. See chapter 4 (pp. 27) for a detailed discussion of the protocol and appendix B for the original paper.

(A1) – (A4) are completed as in protocol 1 (fig. 1).

(C1) For QDC the sender Alice generates a random bit string, which is not related to the secret message to the receiver Bob. She encodes the bit string in a control subset of A-qubits and her secret message in the remaining A-particles. She executes a Hadamard operation to send the bit 0 and a Hadamard operation with previous bitflipping to transmit the bit 1. Bob does not transform his restored B-particles. Alice sends her encoded A-qubits to the third party Trent.

(C2) Trent projects pair by pair, each consisting of one A-qubit and one T-qubit, onto the Bell basis and reveals the resultant Bell states (Trent announces 0 for $|\Phi^+\rangle$ and $|\Psi^-\rangle$ or 1 for $|\Phi^-\rangle$ and $|\Psi^+\rangle$). Bob measures his B-particles in the x basis.

(C3) Bob deduces Alice's operations from the transformation of the system and extracts her secret message.

(C4) Alice and Bob launch the second eavesdropping test. Alice reveals the positions of her check qubits and compares them with Bob. If their results coincide, Alice communicated directly with Bob. Otherwise, the protocol is aborted.

Figure 2: Protocol 2 – Authenticated MQDC
Quantum Direct Communication with Authentication (Lee et al., 2005).
The enumeration letters A and C denote the authentication and communication process, respectively. See chapter 5 (pp. 45) for a detailed discussion of the protocol and appendix B for the original paper.

(A1) At the request of the sender Alice, the third party Trent prepares two orderly sets of Bell states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_A A}$ and $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B}$. The subscripts T_A and T_B denote Trent's A- and B-checking sequence. The subscripts A and B indicate Alice's and Bob's A- and B-authentication sequence, respectively.

(A2) Trent encodes the A- and B-authentication sequence with Alice's and Bob's identification numbers ID_A and ID_B by the same operations as in protocol 1 (fig. 1), i.e. an identity operation for the value 0 and a Hadamard transformation for the value 1. He sends the encoded A- and B-authentication sequences to Alice and Bob, respectively, and stores his A- and B-checking sequences securely.

(A3) Alice and Bob decode their respective authentication sequence with their IDs and restore the original Bell states.

(A4) All three parties complete the authentication test. They measure their sequences in the z basis. Alice and Bob announce their outcomes to Trent, who compares their results with his outcomes of the checking sequences. If the test is successful, Alice and Bob are authenticated via Trent. Otherwise, the protocol is aborted.

(C1) For QDC Alice prepares a random sequence of Bell states of the types $|\Phi^+\rangle_{T_A A}$ and $|\Psi^+\rangle_{T_A A}$. Bob prepares Bell states only of the type $|\Phi^+\rangle_{T_B B}$. The subscripts denote the person who works on the particles later.

(C2) Alice forms the A-sequence consisting of her T_A-qubits. Her remaining A-particles are combined in the encoding sequence. Bob also splits his states in a B-sequence of the T_B-particles and a decoding sequence of the B-qubits. Alice and Bob send Trent the A- and B-sequence.

(C3) Each user launches the first eavesdropping test with Trent. Alice chooses random check positions of her encoding sequence and reveals them to Trent. After measurements in the z basis Trent announces his results to Alice. Bob proceeds accordingly with Trent.

(C4) If both tests are successful, Trent projects the A-sequence and the B-sequence pair by pair onto the Bell basis. Through this entanglement swapping Alice, with her encoding sequence, and Bob, with his decoding sequence, share entangled sequences.

(C5) Trent sends the resultant Bell state to Alice. Alice and Bob measure their encoding and decoding sequences in the z basis, respectively. Alice deduces Bob's measurement outcomes according to her initial state and the transformation of the system.

(C6) Alice and Bob complete the second eavesdropping test. Bob tells Alice his measurement outcome of some check qubits at random positions, and Alice checks her deduced outcomes against Bob's announced results. If the test fails, communication is aborted. Otherwise, Bob's results represent the final basis for direct communication. On this basis Alice sends her message to Bob via bitflip positions. With this additional bitflip information Bob can extract and decode Alice's message.

Figure 3: Protocol 3 – Authenticated MQDC with ES
Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping (Hong et al., 2006).
The enumeration letters A and C denote the authentication and communication process, respectively. See chapter 6 (pp. 57) for a detailed discussion of the protocol and appendix B for the original paper.

3.1 Multiuser Concept

A quantum network is an infrastructure for the transmission of quantum and classical information between the network parties. A network setting is multiuser compatible, if any authenticated user can communicate with another authenticated party in the network without a direct quantum channel. The description of a multiuser network is taken from Lee et al. (2005, 2006) and Hong et al. (2006).

The trustworthy third party Trent is introduced to implement the multiuser setting. Trent is an information center, connected to all parties of the network via quantum and classical links (fig. 4). His primary duty is to supply quantum states and to connect and authenticate the users. The provision of the link connection gives his role similarity to contemporary telephone systems. In the aspect of authentication he serves as a certification authority as known from public-key cryptography.

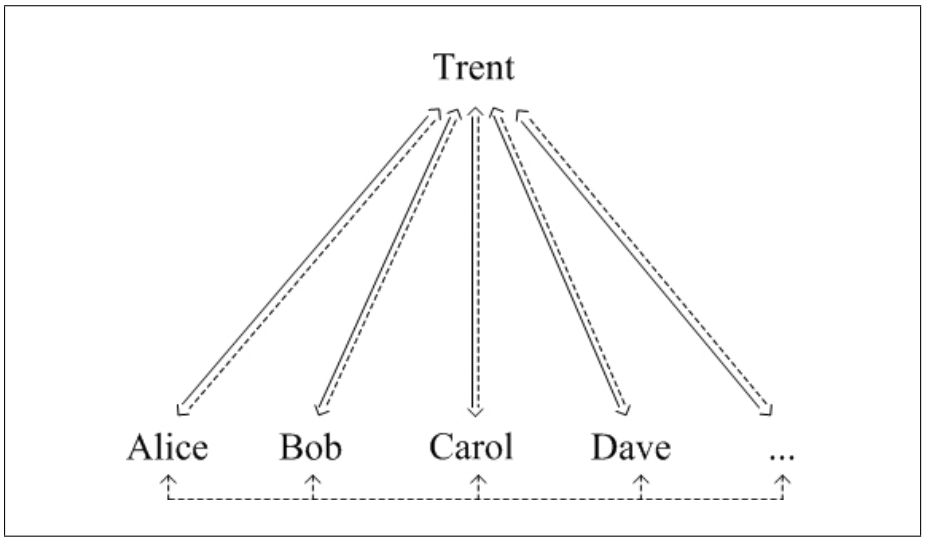

Figure 4: Network of the Multiuser Concept
The solid lines represent the quantum links. The dotted lines display classical channels.

Trent's precedent tasks before quantum communication are the registration of the network users in a personal authentication and the supply of a secret identification sequence (ID) and a hash function to calculate authentication keys. Hence, Trent shares an ID with each registered user. According to Mihara (2002, p. 1), "the existence of a TA [trusted authority] is reasonable for the real world because the information on a person's identity must exist somewhere in order to confirm the person". In addition, Trent can act as a communication assistant during quantum key distribution or quantum direct communication.

Assuming that n parties are registered in a network, the "fundamental problem is how to authenticate resources to each other while minimizing the number of cryptographic keys that must be distributed and maintained, given the potential for $n(n-1)/2$ pairs of communicating resources"(Kuhn, 2003, p. 1). The existence of Trent minimises the amount of required keys within the network to n. In contrast, almost a quadratic amount of keys is required in

private-key cryptography. Compared with settings of public-key cryptography, where $2n$ keys are needed, the amount is half in the network described here.

The authority Trent must be absolutely trustworthy, because he accesses all user identification information. If Trent was not honest, he could always impersonate a user and apply a man-in-the-middle attack. Although his honesty is assumed, Trent may gain knowledge of the exchanged information, if protocols leave him the chance of passive or active eavesdropping.

3.2 Authentication Key

The following authentication approach is qualified for the multiuser concept with realistic assumptions. It was first proposed by (Lee et al., 2005, 2006) and operates with an authentication key which is regenerated for every new communication round. All network users only need to share a secret identification sequence and hash function with Trent. The approach is the basic authentication principle in protocol 1 and protocol 2. Although designed by authors of the first protocols, authentication in protocol 3 is not entirely based on the principle.

The potential network user (U) must personally identify himself to the authority Trent, e.g. with an identity card. Trent then generates a binary user identification sequence ID_U and registers a one-way hash function of the form

$$h_U : \{0,1\}^* \times \{0,1\}^l \rightarrow \{0,1\}^m \ ,$$

where the asterisk denotes an arbitrary length, l constitutes the length of the counter of calls of the hash function (c_U), and m is a constant. ID_U and h_U must be kept secret between the user and Trent. For communication the authentication key is calculated by

$$h_U(ID_U, c_U) = id_{U1} id_{U2} \ldots id_{Un} \ .$$

Each id_{Ui} (with $i = 1, 2, \ldots, n$) represents a single binary value of the user's key. For authentication Trent encodes certain qubits with the key by performing unitary operations on them. He performs an identity operation I, if the i_{th} hashed value of $h_U(ID_U, c_U)$ is 0 ($id_{Ui} = 0$). If id_{Ui} is 1, he executes a Hadamard operation H. If the authentication key is not long enough to cover all required particles, new keys can be created by recalculating the hash function with an increased counter c_U.

It is assumed that the authentication key is recalculated (with different counter c_U) for every new communication round by the one-way hash function. Therefore, an eavesdropper cannot use his knowledge of any id_{Ui} in another authentication round. Furthermore, even if the secret hash function is known, it cannot be reversed with partial knowledge of the hashed value, since it is one-way. Thus, eavesdropping cannot yield the secret identification sequence ID_U.

3.3 About the Eavesdropping Tests

An eavesdropping test is based on a certain amount of check qubits. The testers select these qubits from the qubit set, measure them in the z basis, and compare the measurement outcomes. The network parties determine the amount of check qubits according to their desired security level.

Public discussion of any eavesdropping test must be specified more exactly for precise security analyses than in the original papers. In protocol 1 and protocol 2 the eavesdropping test during authentication is described as a comparison of the measurement results between the sender and the receiver ("Next, Alice and Bob select some of the decoded qubits, make von-Neumann measurements [z basis measurements] on them, and compare the results through the public channel."; protocol 1, p. 4 and protocol 2, p. 2). Both protocols also define the eavesdropping tests during quantum key distribution or quantum direct communication as a comparison ("Alice and Bob compare some bits of their shared key [...]" (protocol 1, p. 5) or "Alice reveals the position of her check bits and compares them with Bob's." (protocol 2, p. 3)). The specification of all eavesdropping tests in protocol 3 embody security loopholes. Alice and Bob measure their sequences and announce the outcomes to Trent in the authentication test. In the first eavesdropping test during direct communication "Alice [and Bob] randomly chooses n checking positions [...]. Trent [...] tells the outcome to Alice [and Bob]." (protocol 3, p. 4). A similar procedure is applied in the second communication test, in which Alice chooses the check positions, and Bob tells Alice his measurement result of these positions. This procedure facilitates an attacker's impersonation of Trent or Alice, respectively.

First of all, public discussion must be realised as a dialogue to prevent that the attacker Eve avoids detection in any impersonation attack. In the given monologue form, that is the first party announces the results and the second one compares them, the second party can always claim the results coincide, even if they do not. Hence, in the case that Eve impersonates the second party, she completely avoids detection. In the monologue form Eve can be detected with higher probability in an impersonation of the first user. Nevertheless, a balanced detection probability is regarded to provide more security against all attacks discussed here.

Second, the first announcements must alternate between the users. That is to say, the first party reveals her/his first measurement outcome of a check position of her/his choice. The second party compares it with her/his first result and announces whether or not their outcomes are as expected. Then the second party announces her/his second outcome of a chosen check position. The first party compares it and discloses whether the results coincide. The alternation is maintained until all check positions are compared. This procedure guarantees detection of any impersonation attack.

Third, it is an unnecessary relocation of power that one party determines the check positions. It may affect Eve's success probability in an impersonation attack, if she is in the position to choose the check qubits. Furthermore, it may jeopardise the randomness of the check qubits, if their selection is not subdivided into two parts. Protocol 1 and protocol 3

allow a selection of a control subset, which is divided between two parties in equal shares. The characteristic of protocol 2 exclude a simple circumvention of the one-sided choice. This work does not investigate the consequences of the issue further.

Finally, Trent must know the check positions of any eavesdropping test during authentication as well, even if he does not participate in it. This is not mentioned in any of the original protocols. If Trent does not eliminate the check qubits in his sequence, the results of further communication are incorrect, since the communication is based on the entanglement of the structured system.

The security analyses of protocol 1 and protocol 2, as well as of all proposals, assume that all eavesdropping tests are conducted in dialogue form. The original suggestions for the eavesdropping tests in protocol 3 are discussed in detail in sections 6.3 and 6.4. All test dialogues alternate and the selection of check qubits is divided between the two parties, if possible. Trent is informed about the check qubits of the authentication test and does not consider these qubits in further communication, which is not stated explicitly in the following.

3.4 About the Security Analysis

The security analysis of all protocols and proposals investigates single eavesdropping attacks of the third party Trent and the attacker Eve, i.e. Trent's passive and active eavesdropping and Eve's eavesdropping attacks on the authentication and the communication process. Trent represents the third party between the two communication parties, who is in possession of certain particles of the system. Hence, the condition of any protocol must prevent him from eavesdropping. Intercept-resend and translucent attacks, as well as her impersonation of Trent, are considered for Eve's eavesdropping of the user IDs. An intercept-resend attack and translucent attacks are analysed as eavesdropping attacks on the communication process.

The following translucent attacks with different unitary transformations are analysed in this work. Both unitary operations are given here as in the original papers. In the first translucent attack Eve uses ancilla $|E\rangle_E$ with the unitary operations (A) to entangle her ancilla with a particle in transmission. In the second translucent attack Eve entangles her probe $|0\rangle_E$ by the unitary transformation (B). Entanglement of the ancilla may transform the system according to the respective unitary operation.

$$\begin{aligned} U_E(|0E\rangle_{AE}) &= \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E \\ U_E(|1E\rangle_{AE}) &= \alpha'|1\rangle_A|e_{11}\rangle_E + \beta'|0\rangle_A|e_{10}\rangle_E \ , \end{aligned} \tag{A}$$

where $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha'|^2 + |\beta'|^2 = 1$ and $|\alpha\beta^*|^2 + |\alpha'^*\beta'|^2 = 0$.

$$\begin{aligned} U_E(|00\rangle_{AE}) &= |00\rangle_{AE} \\ U_E(|10\rangle_{AE}) &= |11\rangle_{AE} \end{aligned} \tag{B}$$

This work emphasises the implementation of authentication within networks. Therefore, complete scenarios of impersonation attacks are designed and analysed. Eve has the possibility to gain knowledge of exchanged information by impersonating a user in a simple impersonation attack. She can also take Trent's place or pretend to be both a user and the authority at the same time. The latter attacks are called advanced impersonation attacks from here on. Additionally, the analyses include a man-in-the-middle attack, which is a simultaneous impersonation of both users during a communication round.

The attacks are either derived from the proofs, contained in the original papers and supplemented here with detailed aspects, or new analyses. The redeveloped concept of the authentication key in the first two protocols is discussed in the original protocol 1 (p. 6). Both protocols assume that Trent is honest in all aspects and potential attacks are not investigated. For the authentication process the first translucent attack is analysed in the original protocol 1. In protocol 2 the second translucent attack is investigated. Both protocols also discuss an intercept-resend attack. Furthermore, protocol 2 describes a coherent attack on the authentication with a resultant detection probability of $\frac{1}{4}$ per check qubit. This result is given without derivation and cannot be retraced nor (dis)proved here, since this work excludes coherent attacks due to their complexity. Both protocols analyse the first translucent attack on the transmission during communication. The original protocol 3 includes only a short textual derivation as security analysis. All other attacks are designed specifically for this work. The detection probability ρ_D is calculated as in protocol 1 and protocol 2. Additionally, the success probability ρ_S is provided for some attacks to indicate Eve's information gain in case of failed detection.

A single state $|\theta_i\rangle$ out of each entire set $|\Theta\rangle$ is analysed as general basis of security. Any detection or success probability is calculated per check qubit or per qubit, respectively. All proofs assume that the authentication key consists of equal amounts of zeros and ones. Otherwise, the detection and success probabilities must be shifted accordingly. The security analysis discusses attacks launched by the single attacker Eve. If there is another attacker Evan, who independently executes his own attack of any type, Eve's results deteriorate and the detection probability increases. Detailed calculations for all security results are given in the appendices D – J.

To formalise the context of check qubit amount c and detection probability ρ_D the term $1-(1-\rho_D)^c$ is used. The success probability ρ_S is obtained accordingly with the term $1-(1-\rho_S)^q$, where q denotes the amount of qubits. In an eavesdropping test in dialogue form Eve is detected in an impersonation attack anytime she makes the first announcement. Hence, detection is possible for any second check qubit and c must be halved.

In the description of the protocols the definition of the qubit set differs formally from the notation given in the original papers for reasons of uniformity in this work. Furthermore, the breakdown of the amounts of check qubits is added in order to achieve more precision in the security analyses.

In the original protocols 1 and 2 quantum communication closes with the suggestion of implementing classical error correction to correct errors of realistic quantum systems. More-

over, standard privacy amplification is recommended to reduce Eve's potential knowledge of the key or the message. The two suggestions are not investigated further in this work.

Chapter 4

Authenticated MQKD

This section focuses on the *Quantum Authentication and Quantum Key Distribution Protocol* (protocol 1) proposed by Lee et al. (2006). The protocol enables the users Alice and Bob to distribute a secret key after they authenticated each other via the third party Trent. With this shared key Alice and Bob are then in the position to perform conventional, symmetric cryptography. Alice encrypts her plaintext message with the key and sends the ciphertext to Bob over any classical channel. Bob is able to read the message decrypting the ciphertext with the same key. The original protocol can be found in appendix B, an overview is displayed in figure 1 (p. 18).

4.1 Authentication

Assuming that Alice intends to communicate with Bob, she requests Trent to prepare an orderly set $|\Theta\rangle_{ATB}$ of n tripartite entangled GHZ states $|\theta\rangle_{ATB}$ with

$$\begin{aligned} &|\Theta\rangle_{ATB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_n\rangle)_{ATB} \text{ of} \\ &|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \text{ with } i = 1, 2, \ldots, n \ . \end{aligned} \tag{I}$$

The subscripts A, T, and B label the qubits for Alice, Trent, and Bob, respectively. The amount n is composed of $N + c_{AUTH} + c_{QKD}$, which denotes length N of the final key and the number of check qubits during authentication (c_{AUTH}) and key distribution (c_{QKD}). Alice or Trent inform Bob about Alice's communication request, which is not stated explicitly in the following anymore.

Alice's and Bob's authentication keys determine the unitary operations which Trent has to perform on the corresponding A- and B-particles of each state $|\theta_i\rangle_{ATB}$ to encode $|\Theta\rangle_{ATB}$. He transmits the respective qubits to Alice and Bob and keeps his own T-particles in a safe place. Alice and Bob decode their particles, performing the unitary operations on them as defined by their authentication keys. The GHZ states are restored to their original state after decoding, due to the properties of unitary operations.

In the following eavesdropping test Alice and Bob agree on a subset of check positions on the scale of c_{AUTH}. They measure the corresponding qubits locally in the z basis and compare the outcome of each position. This eavesdropping test must follow the procedure discussed in section 3.3. If the compared particles are still perfectly correlated, Alice and Bob know that the transmitted qubits have not been observed. Furthermore, they have authenticated each other via Trent, since only a legitimate user has the ability to restore the encoded qubits correctly with the proper authentication key. In case of an error rate higher than expected, Alice and Bob abort the protocol and restart a new communication round.

4.2 QKD

To arrange a shared key Alice and Bob encrypt secret, binary information in their $N + c_{QKD}$ restored particles, which remain after the eavesdropping test during authentication. They both randomly perform either an identity operation I, which indicates 0, or a Hadamard operation H, which represents 1. The records of their operations are stored.

Bob sends his encoded particles to Alice. Alice forms pairs consisting of one particle of her orderly sequence and one particle of Bob's transmitted sequence. She then projects pair by pair onto the Bell basis. Meanwhile, Trent measures his particle in the x basis and announces the outcome publicly.

Alice's and Bob's operations and Alice's and Trent's measurements transform the original $N + c_{QKD}$ GHZ states according to table 4.1. By means of this transformations and the supplementary knowledge of her operation, Alice is able to reconstruct Bob's operations. For instance, Alice performed an identity operation and received the Bell state $|\Phi^-\rangle_{AB}$. Trent published the result $|+\rangle_T$. Alice can then conclude that Bob executed a Hadamard operation, which means that he encoded the value 1 (cf. row 2 in tab. 4.1).

Alice and Bob agree on a subset of c_{QKD} check qubits and compare the corresponding values to check for potential eavesdropping during the transmission of Bob's encoded particles. The test must again proceed in dialogue form (s. 3.3). If their results coincide, Bob's operations on the remaining N qubits form the distributed key.

Operation of Alice		Bob		Transformation of GHZ states
I	(0)	I	(0)	$\frac{1}{\sqrt{2}}(\|\Phi\rangle^+_{AB}\|+\rangle_T + \|\Phi\rangle^-_{AB}\|-\rangle_T)$
I	(0)	H	(1)	$\frac{1}{2}(\|\Phi\rangle^+_{AB}\|-\rangle_T + \|\Phi\rangle^-_{AB}\|+\rangle_T + \|\Psi\rangle^+_{AB}\|+\rangle_T + \|\Psi\rangle^-_{AB}\|-\rangle_T)$
H	(1)	I	(0)	$\frac{1}{2}(\|\Phi\rangle^+_{AB}\|-\rangle_T + \|\Phi\rangle^-_{AB}\|+\rangle_T + \|\Psi\rangle^+_{AB}\|+\rangle_T - \|\Psi\rangle^-_{AB}\|-\rangle_T)$
H	(1)	H	(1)	$\frac{1}{\sqrt{2}}(\|\Phi\rangle^+_{AB}\|+\rangle_T + \|\Psi\rangle^+_{AB}\|-\rangle_T)$

Table 4.1: Expected Results of QKD
Source: Lee et al. (2006)
For a detailed derivation see appendix C.1.1.

4.3 Security Analysis

The security of the authentication and key distribution results from the properties of entanglement of the GHZ states. The integration of authentication into communication is an important feature of the protocol, i.e. both processes are performed using the same qubit set. It consists of particles encoded with the authentication keys. Furthermore, the attacker Eve cannot avoid any control procedure by leaving the test subset unattacked, since the check positions are not revealed until transmission is completed.

4.3.1 Eavesdropping of Trent

Even though Trent is considered trustworthy concerning the secret handling of IDs, and he is not supposed to utilise this information for any impersonation of an registered user, no protocol should give him the opportunity to passively or actively eavesdrop on the key distribution. As the analysis of protocol 1 shows, Trent cannot passively eavesdrop. No information automatically leaks to him during QKD. His only task is to measure his T-particle in the x basis. He cannot take advantage of the results $|+\rangle_T$ or $|-\rangle_T$, because each state occurs with the same probability for all possible combinations of the users' operations (cf. tab. 4.1, p. 28).

In an active eavesdropping attack Trent intercepts the qubits transmitted from Bob to Alice and resends her equally prepared states. Trent measures the intercepted B-qubits to draw conclusions on Bob's operations and the key values. If he only measures the B-particle in the z basis, Trent cannot gain any information, since 0 and 1 occur with the same probability for both of Bob's operations I_B or H_B. Measurement of the B-particle and of his own T-qubit in the z basis provide some information about the key value (see appendix D.1 for details). Trent receives the equal results for both qubits with the probability of $\frac{3}{4}$. The probability for different results is $\frac{1}{4}$ and implies a Hadamard operation by Bob. Equal outcomes assure Trent with a probability of $\frac{2}{3}$ that Bob performed an identity transformation. With this knowledge Trent may gain sufficient information of the final key. Additional transformations before his measurement do not increase Trent's success.

But Trent's intermediate measurement causes errors in the system. Alice's A-particle collapses to a fixed state due to Trent's measurement. Trent resends Alice a new qubit as Bob's particle, which he prepared according to his measurement result of the original B-particle. This newly prepared B-qubit and Alice's A-qubit may not represent a valid input for a Bell basis measurement. Furthermore, Trent can neither derive nor measure a correct x basis measurement result for his T-qubit. These irregularities can be detected in the final eavesdropping test of Alice and Bob. Consequently, communication is aborted and restarted. As Alice and Bob use different orders of their operations I and H after a restart, Trent's previous information becomes obsolete.

4.3.2 Eavesdropping on Authentication

To gain knowledge of a secret user ID in preparation of an impersonation attack in another communication round Eve must listen in on the authentication process. Eavesdropping on the authentication procedure yields authentication key values at most. The underlying ID cannot be obtained directly from eavesdropping. Eve has two possibilities for her attack. She may impersonate Trent or eavesdrop on the regular authentication using the intercept-resend or translucent technique (see appendix D.2 for detailed calculations).

To impersonate Trent Eve must prepare GHZ states and encode the respective particles with Alice's and Bob's authentication keys. Eve has no other choice but to leave all qubits unencoded or to guess the keys. In terms of the analysis, the second option – guessing the keys – is an extension of the first option and produces the same results. With both techniques Eve introduces an error into the system with the probability of 25 %. After Alice's and Bob's decoding a resultant probability of $\rho_D = 1 - \left(1 - \frac{3}{8}\right)^{c_{AUTH}}$ provides the detection of Eve in the first eavesdropping test.

Eve must listen in on the public discussion of this test. She gains some information about the performed operations with Alice's and Bob's discussed measurement result and the result of her own qubit measured in the z basis. Eve is only able to recognise a Hadamard operation. She knows that both key values id_{iA} and id_{iB} are 1 with the probability $\rho_S = 1-(1-\frac{1}{16})^{c_{AUTH}}$. Her success probability to obtain one key value id_{iA} or id_{iB} totals $1-(1-\frac{3}{16})^{c_{AUTH}}$. For over half the control subset on the scale of c_{AUTH} Eve cannot infer any key value. Furthermore, since only this small subset is publicly discussed, she does not get any information about all other key values.

If the eavesdropping test after transmission was not between the two communication parties but between each user and Trent, Eve might increase her success probability by lowering the detection probability. Each time the user makes the first announcement Eve could reveal the appropriate correlated value. Hence, detection would not occur per check qubit but only for every second qubit. If the test was not a dialogue but a monologue of a user, Eve could avoid detection entirely. In this case she as Trent only has to compare the results and determine the error rate. She could claim that all compared results coincide. However, the test definition of section 3.3 excludes this scenario. Thus, Eve may gain negligible information of the authentication keys but without influence on the test procedure and without avoidance of detection.

Alternatively, Eve may eavesdrop on the qubit transmission with an intercept-resend or a translucent attack (see p. 23). In the following, Alice's ID_A is under attack, but the analysis can be equally adapted to all other network user IDs.

Intercepting and measuring Alice's qubits in an intercept-resend attack does not yield any information for Eve. She measures 0 and 1 with the same probability for both of Trent's operations, which are determined by Alice's authentication key. Additionally, Eve introduces errors when she resends a particle to Alice which she prepares according to her measurement result. Alice detects Eve with the probability of $1-(1-\frac{1}{4})^{c_{AUTH}}$.

In the first translucent attack Eve uses ancilla $|E\rangle_E$ with the unitary operations (A) to entangle the ancilla with an A-particle during transmission, i.e. between Trent's encoding and Alice's decoding. Alice detects her attack with a probability of $\frac{\beta^2+\beta'^2}{2}$, if id_{iA} equals 0 and with a probability of $\frac{1}{2}$ for $id_{iA} = 1$. Hence, the overall detection probability of the first translucent attack with unitary operation (A) adds up to $\rho_D = 1 - \left(1 - \frac{1}{4} - \frac{\beta^2+\beta'^2}{4}\right)^{c_{AUTH}}$.

In the second translucent attack Eve entangles her probe $|0\rangle_E$ by the unitary transformation (B). There is no detection for $id_{iA} = 0$. If id_{iA} is 1, Eve is detected with the probability of $\frac{1}{2}$. Thus, the overall detection probability of the second translucent attack with the unitary operation (B) is $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_{AUTH}}$.

As the analysis shows, Eve actually gains partial knowledge of the authentication key $id_{1A}id_{2A}...id_{nA}$. However, the authentication key is recalculated with the secret identification sequence ID_A and a different counter c_A for any new communication round by $h_A = (ID_A, c_A)$. Hence, Eve's information of any id_{iA} is obsolete for future authentication. Eve needs the underlying ID_A to participate in further authentication rounds. Even if she knew the secret one-way function, she cannot reverse it, which she would have to do to receive ID_A, especially not with only partial knowledge of the authentication key.

4.3.3 Eavesdropping on QKD

Eve also uses both translucent attacks on the transmission of the B-particles, if she intends to gain knowledge of the distributed key. The B-qubits are the only transmitted particles and the key is encoded in them (see appendix D.3).

If Eve uses ancilla $|E\rangle_E$ with unitary operation (A) for a translucent attack, the detection probability totals $\rho_D = 1 - \left(1 - \frac{1}{2} - \frac{\beta^2+\beta'^2}{8}\right)^{c_{AUTH}}$. In case of launching the second translucent attack with ancilla $|0\rangle_E$ and unitary operation (B), the detection probability amounts to $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_{AUTH}}$.

An intercept-resend attack is no appropriate technique, because Eve would measure 0 and 1 with the same probability for both identity and Hadamard transformation.

4.3.4 Simple Impersonation Attacks

In a simple impersonation attack Eve impersonates a user during an entire communication round with authentication and communication. There are two different kinds of impersonation attacks, if it is assumed that Alice initialises communication. If Eve's aim is to send Bob a message of her choice but in Alice's name, she must impersonate Alice to obtain a shared key with Bob (sender impersonation). With this key she can encode her classical message and send it to Bob. In the receiver impersonation Eve impersonates Bob, the person the "communication initialiser" Alice wishes to communicate with. In this case Eve intends to intercept, decode and read Alice's classical message to Bob. Detailed calculations for both simple impersonation attacks are given in appendix D.4.

At the last stage of classical communication Alice and Bob have no possibility to recognise an attack. In the first attack a secret sign within the document, secretly arranged between

Alice and Bob before quantum communication, could lead to the detection of Eve. Nevertheless, such a sign is not assumed here because of the resultant distribution problem. In the receiver impersonation a prearranged sign would not complicate Eve's attack, since she could read it in the intercepted message and replicate it in her own message.

4.3.4.1 Sender Impersonation

In the sender impersonation Eve does not have to cut the line between Alice and the network, because it is assumed that Eve takes Alice's name, and Alice herself has no knowledge about an ongoing key distribution. Eve only needs a possibility to intercept the quantum and public channels between Alice and the network.

At Eve's request, Trent prepares n GHZ states (with $n = N + c_{AUTH} + c_{QKD}$) and sends the encoded particles to Alice and Bob. It is assumed that no identification information is necessary for such a request. Otherwise, this type of impersonation attack would inevitably fail right from the start.

In order to succeed, Eve must intercept the transmitted A-particles (the $E(A)$-particles from here on) and correctly decode them according to Alice's authentication key, which Eve does not possess. This is not only essential to pass the subsequent authentication test, but also to restore the qubits correctly for further communication. Eve may guess the decoding operations determined by Alice's authentication key or measure the particles without executing any operations on them. For both choices there is a detection probability of $\frac{1}{4}$ during the subsequent eavesdropping test with Bob. Eve can avoid detection for all of Bob's first announcements, if the test is a dialogue between the two parties. Hence, it follows that Bob can detect Eve with probability $\rho_D = 1 - (1 - \frac{1}{4})^{c_1}$ (with $c_1 = c_{AUTH}/2$). It is not likely that Eve passes the test and is authenticated as Alice with a detection probability on such a scale.

In the unlikely case that Bob does not abort communication, Eve performs identity and Hadamard transformations of her chosen order on the remaining $N + c_{QKD}$ $E(A)$-qubits. She must intercept the qubits Bob sends to Alice, which contain the encoded operations representing the key values. Eve then projects the $E(A)$- and B-qubits onto the Bell basis. After her Bell measurements and Trent's x basis measurement the GHZ states are transformed according to table 4.2 (p. 33). Eve's and Bob's operations are listed in the first and second column, respectively. Eve's previous restoring errors also cause a high detection probability in the second eavesdropping test and severe problems to obtain information of Bob's operations.

Provided that the test proceeds as a dialogue, Bob detects Eve in all of her first announcements with a probability of $\frac{3}{8}$. If Bob announces his operation at first, Eve can avoid detection by telling him an expected result. Hence, the detection probability totals $\rho_D = 1 - (1 - \frac{3}{8})^{c_2}$ (with $c_2 = c_{QKD}/2$). Apart of detection Eve has serious difficulties inferring Bob's operation to obtain the key of N bit length. Eve can only obtain information of Bob's operation with the entire results $|\Phi^-\rangle_{E(A)B}|-\rangle_T$ (row 1 and 6 in tab. 4.2) and $|\Psi^+\rangle_{E(A)B}|-\rangle_T$ (row 4 and 7 in tab. 4.2). All other results occur for both of Bob's operations, what leads to a success probability of only $\rho_S = 1 - \left(1 - \frac{1}{4}\right)^q$. Hence, Eve's success in an impersonation of the sender is highly limited by a high detection probability and a low success probability.

Operations		Transformation of GHZ states
I	I	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Phi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T - \|\Psi^-\rangle_{AB}\|-\rangle_T)$
I	H	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T + \|\Psi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|-\rangle_T)$
H	I	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T - \|\Psi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Phi^-\rangle_{AB}\|-\rangle_T)$
H	H	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T + \|\Psi^-\rangle_{AB}\|-\rangle_T)$

Table 4.2: Results of QKD I
For the sender impersonation attack subscript A must be replaced by $E(A)$. Restoring errors occur for incorrectly decoding the correctly encoded A-qubits. For the impersonation of the receiver and the authority subscripts T and B must be replaced by $E(T)$ and $E(B)$, respectively. Restoring errors appear for correctly decoding the non-encoded A-qubits.

4.3.4.2 Receiver Impersonation

In the receiver impersonation Eve does not have to cut the line between Bob and the network, if she is already able to intercept Alice's communication notification to Bob. This way Bob does not know about an ongoing communication. Furthermore, Eve needs a possibility to intercept Bob's quantum and public channels.

First of all, Eve must intercept the n B-particles (hence, the $E(B)$-particles) of the GHZ states Trent prepared at Alice's request ($n = N+c_{AUTH}+c_{QKD}$). An identification information necessary to make a request could not detect this sort of impersonation attack, because the legitimate Alice launches it. Eve must decode the $E(B)$-qubits with the unitary operations $I_{E(B)}$ and $H_{E(B)}$ determined by Bob's authentication key, which she does not have. Like in the preceding impersonation attack, correct decoding is not only essential to pass the subsequent authentication test but also to restore the qubits for key distribution. Again, with both decoding techniques detection probability in the first eavesdropping test with Alice during authentication amounts to $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_{AUTH}}$ (with $c_1 = c_{AUTH}/2$).

Assuming Eve reaches the communication stage despite the high detection probability, she chooses a key and performs the corresponding operations on the remaining $N + c_{QKD}$ qubits. Next, she transmits her encoded particles to Alice, who projects each of her encoded A-qubit with a received $E(B)$-particle onto the Bell basis. Trent measures the T-particles in the x basis. Table 4.3 (p. 34) lists the transformation of the GHZ states considering Eve's restoring problem.

With the public discussion in dialogue form Alice can detect Eve with probability $\frac{1}{2}$ when Eve reveals her result at first, i.e. $\rho_D = 1-(1-\frac{1}{2})^{c_2}$ (with $c_2 = c_{QKD}/2$). In the unlikely case that Alice fails at detecting Eve, the consequence of Eve's restoring problems leads to the following conundrum: Eve cannot know the key, although she determines it. Indeed, Alice is able to derive precisely one operation from the entire result. But all of Alice's entire results are received by both of Eve's operations. As Eve has no knowledge of Alice's operations nor

of her resultant Bell state, she cannot infer which operation Alice deduces. For example, Alice performed the identity operation I_A on her particle and her entire result is of the form $|\Phi^+\rangle_{AE(B)}|+\rangle_T$, so she infers an identity operation ($I_{E(B)}$) and records a key value of 0 (row 1 in tab. 4.3). Eve might have actually performed this operation, but a Hadamard operation $H_{E(B)}$ is equiprobable (row 4 in tab. 4.3). With H_A Alice derives a Hadamard operation of the second party from the same entire result, but $I_{E(B)}$ can also produce it (7th and 6th row of tab. 4.3, respectively). Hence, Eve does not succeed in a receiver impersonation. She ends up with no knowledge of any key value due to her restoring problems resultant from the lack of Bob's authentication key.

Operations		Transformation of GHZ states
I	I	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Phi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T + \|\Psi^-\rangle_{AB}\|-\rangle_T)$
I	H	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T + \|\Psi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Phi^-\rangle_{AB}\|-\rangle_T)$
H	I	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T - \|\Psi^-\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|-\rangle_T)$
H	H	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|-\rangle_T)$
		$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T - \|\Psi^-\rangle_{AB}\|-\rangle_T)$

Table 4.3: Results of QKD II
In the receiver impersonation attack subscript B must be replaced by $E(B)$. Restoring errors occur for incorrectly decoding the correctly encoded B-qubits. In the impersonation of the sender and the authority subscripts A and T must be changed to $E(A)$ and $E(T)$, respectively. Restoring errors appear for correctly decoding the non-encoded B-qubits.

4.3.5 Advanced Impersonation Attacks

To improve the results of a simple impersonation attack Eve can additionally impersonate the authority, which may put her in the position of gaining additional information from the possession of his T-particles. Eve must prepare GHZ states and encode them with the users' authentication keys for an advanced impersonation attack. As Eve does not know the secret user information necessary for calculating the authentication key, she has again the two possibilities of either guessing the key or leaving the particles unencoded. As already shown, the two options are equivalent in terms of the security analysis. It is assumed in the following that Eve does not attempt to encode the particles and leaves them untransformed.

In the impersonation of the sender and the authority or the receiver and the authority Eve's goal is to send Bob a fake message or to read Alice's secret message, respectively. The analysis additionally discusses a third advanced impersonation attack, an impersonation of Trent. In this attack Eve re-enacts the potential eavesdropping on the key distribution in place of Trent (s. 4.3.1). If successful, she possesses the shared key of Alice and Bob. She can write and encode a message to Bob, and decode and read Alice's message.

A secret initial sign included in the classical message is not assumed in all attacks in order to prevent distribution problems. Hence, Alice and Bob are not aware of an attacker at the last stage of classical communication. Eve can launch the attacks, even if any identification information is necessary for a request, since the legitimate Trent and his controlling function do not exist in this scenario. Detailed calculations for all attacks are given in appendix D.5.

4.3.5.1 Impersonation of Sender and Authority

Eve's first task in an impersonation of Alice and Trent is the preparation of n GHZ states (with $n = N + c_{AUTH} + c_{QKD}$). She keeps the A- and the T-qubits (henceforth, denoted $E(A)$- and $E(T)$-qubits, respectively) and sends Bob his B-particles.

Bob decodes the B-qubits with his authentication key after reception. This decoding process causes restoring errors in the system, because Eve did not encode the qubits. Thus, the restoring problem of the original states, mentioned earlier, occurs again, but now due to false (or no) encoding instead of false decoding. Although there is no restoring problem for Eve anymore, Bob can still detect her, because he considers his authentication key to be correct and automatically presumes errors of the other communication party. Due to the side, the restoring errors which occur in this first advanced impersonation attack can be formally compared to the results of the second simple impersonation attack in table 4.3 (p. 34).

The detection probability during authentication remains $\frac{1}{4}$ for each of Eve's turns to make the first announcement, i.e. $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$). Assuming the improbable case that Eve reaches the communication stage after the eavesdropping test, Bob performs identity or Hadamard operations on his restored particles for key distribution and sends his encoded qubits to Alice. After intercepting these B-particles Eve is in possession of all particles of the system. She can measure any particle of her choice to obtain knowledge of Bob's operations without detection of the measurement.

In the simple impersonation of the sender Eve reaches a success probability of $1 - \left(1 - \frac{1}{2}\right)^q$. Her success probability even worsens in the advanced impersonation attack, because now Eve cannot derive any of Bob's operations. Eve does not gain any knowledge of Bob's operation measuring the B-particle and one of her particles, since the same results occur for both of Bob's operations. Different measurement outcomes can occur for I_B on a falsely restored B-qubit or for H_B on a correctly restored B-particle. Following the protocol, that is performing operations and Bell measurements, Eve also receives the same system transformations for both of Bob's operations (see tab. 4.3). The detection probability during the second eavesdropping test increases from $1 - \left(1 - \frac{3}{8}\right)^{c_2}$ of the simple attack to $1 - \left(1 - \frac{1}{2}\right)^{c_2}$ of the advanced impersonation, since Eve cannot avoid detection for certain entire results anymore.

In comparison with the simple impersonation of Alice the restoring errors switches from Eve's $E(A)$-particle to Bob's B-particle. This effect decreases Eve's chances to deduce Bob's operations. Moreover, the detection probability during communication increases.

4.3.5.2 Impersonation of Receiver and Authority

In an impersonation of Bob and Trent Eve intercepts Alice's request to Trent and Bob, and prepares n GHZ states (with $n = N + c_{AUTH} + c_{QKD}$). She sends Alice the unencoded A-particles and keeps the B- and T-qubits (henceforth, termed $E(B)$- and $E(T)$-qubits).

Alice decodes the A-qubits with her authentication key after reception. Since Eve did not encode them, Alice's decoding leads to restoring errors. Hence, Alice can detect Eve, because she knows that her authentication key is correct and automatically presumes errors of the other communication party. Since the restoring problem occurs on the same side, the second advanced impersonation attack results in the same transformation of GHZ states as the first simple impersonation attack (tab. 4.2, p. 33).

Eve's attack can be detected in the first eavesdropping test with a probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$). In the unlikely case of the continuation of communication, Alice performs identity or Hadamard operations on her remaining qubits for key distribution. Eve does the same with her correct particles and transmits them to Alice. Alice then performs Bell measurements for each pair consisting of her A-qubit and the received $E(B)$-particle. Eve measures her $E(T)$-qubits in the x basis and reveals the outcomes to Alice (see tab. 4.2).

In the simple impersonation of the receiver Eve's restoring errors led to the conundrum that she could not know the key, although she determined it. This conundrum persists in this advanced impersonation attack. Alice can precisely derive one operation of the second party, since she knows the entire result. But all of Alice's entire results are achieved by both of Eve's operation, and Eve cannot know which of her operations Alice deduces. Her x basis measurement result of the $E(T)$-qubit does also not have an advantageous effect on Eve's success probability. Since it is publicly announced, Eve could utilise it in the simple attack anyway. Even if Alice did not recognise a preceding measurement of the $E(B)$- or $E(T)$-particles before receiving the $E(B)$-qubit, Eve could not gain any additional knowledge measuring them.

The detection probability in the second eavesdropping test amounts to 50 % for all of Eve's first announcements, i.e. $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_2}$ (with $c_2 = c_{QKD}/2$). Moreover, Alice has the chance to detect Eve beyond the eavesdropping test with an additional probability of $\frac{1}{8}$ per qubit, that is $\rho_{D_{add}} = 1 - (1 - \frac{1}{8})^q$. The entire result $|\Psi^+\rangle_{AE(B)}|-\rangle_{E(T)}$ is not supposed to occur with Alice's identity operation I_A (cf. 4th row of tab. 4.2 with 1st and 2nd row of tab. 4.1). In the same manner, H_A cannot correctly result in $|\Phi^-\rangle_{AE(B)}|-\rangle_{E(T)}$ (cf. row 6 of tab. 4.2 with row 3 and 4 of tab. 4.1).

Compared to the simple impersonation of Bob, Eve can neither increase her success probability nor decrease her detection probability in the eavesdropping tests. Actually, Eve increases the probability to be detected due to detectable irregularities beyond the tests.

4.3.5.3 Impersonation of the Authority

Trent's information gain from active eavesdropping results from the fact that he can measure his and Bob's particle together to derive Bob's operation. To do this in place of Trent Eve

must get access to his T-qubits. As the T-particles are not transmitted, Eve must impersonate Trent from the beginning.

Eve intercepts Alice's request to Trent and prepares n GHZ states (with $n = N + c_{AUTH} + c_{QKD}$). Since Eve does not know the necessary information to calculate the authentication keys, she sends the particles unencoded to Alice and Bob. Their decoding leads to restoring errors, which occur on both sides in this type of advanced impersonation attack.

With restoring errors on both sides in all transformations of the system, there is an even higher detection probability in the eavesdropping tests, as well as bigger problems to derive the key. The detection probability sums up to $1 - \left(1 - \frac{3}{8}\right)^{c_{AUTH}}$ during authentication and to $1 - \left(1 - \frac{9}{16}\right)^{c_{QKD}}$ during key distribution. Moreover and even more essential, Eve cannot deduce any key value. Hence, Eve cannot successfully impersonate Trent and eavesdrop on the communication.

4.3.6 Man-in-the-middle Attack

A man-in-the-middle attack is a combination of the simple impersonation attacks described in section 4.3.4, i.e. Eve impersonates both communication parties during an entire communication round with authentication, quantum key distribution, and public discussions. The aim of this kind of attack is to arrange two different keys k_{Alice} and k_{Bob}. After successful key arrangements Eve can decode and read Alice's classical message to Bob with the key k_{Alice}, which she shares with the sender, and write and encode a message to Bob with the key k_{Bob}, which she shares with the receiver. Again, at the stage of classical communication neither Alice nor Bob can recognise Eve's intervention anymore. Even the inclusion of a secret sign in the document would not guarantee detection, because Eve might forge it after reading Alice's original message.

Eve must impersonate Bob towards Alice and Trent and Alice towards Bob and Trent. Thus, Eve performs all communication tasks of an impersonation attack twice. After Alice's request Trent sends the encoded A- and B-qubits of the prepared GHZ states to Alice and Bob, respectively. It is not reasonable for Eve to work with one set of GHZ states, i.e. to intercept the A- and B-particles at the same time. If Eve possesses Alice's and Bob's sets of qubits, the communication cannot take place between them. If Eve sends other prepared sets to Alice and Bob instead, the necessary correlations with Trent's qubits within the system do not exist anymore. Hence, Eve must intercept the B-qubits, which are transfered to Bob, to obtain qubits correlated with the A-particles. Eve must then request – in Alice's name – another set from Trent and intercepts the A-particles to obtain correlated particles with Bob. To not arouse Trent's suspicion Eve must convince Trent that the particles of one set do not cover the entire length of the key, which is to be distributed. In that case, Trent increases the counter c_A and c_B to calculate additional authentication keys for Alice and Bob and encodes a new set of particles with these new keys. If there is any network policy, urging the users to request just one self-chosen, but fixed amount of qubits for one communication round, Eve can divide the transmitted single set into two smaller sets, one shared with Alice and another

with Bob. Alice may become suspicious of the smaller amount of qubits than she requested, so Eve must pad the original sets. She prepares each padding qubit of Bell states to keep one correlated particle for herself. Eve must avoid the inclusion of these particles in the final key, since they are not correlated with Trent's qubits. They can be used only in the first eavesdropping test during authentication.

Assuming that Eve can manage all discussed tasks, she still cannot be successful as the man-in-the-middle. Since the attack is a combination of both simple impersonation attacks, the respective detection probabilities hold and the restoring problems are maintained. Hence, Alice or Bob detect Eve with the probability of $1-\left(1-\frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) in each of the first eavesdropping tests during authentication. Furthermore, detection probability during key distribution amounts to $1-\left(1-\frac{3}{8}\right)^{c_2}$ for the sender impersonation and to $1-\left(1-\frac{1}{2}\right)^{c_2}$ in the receiver impersonation (with $c_2 = c_{QKD}/2$). Moreover, Eve's success probability to arrange k_{Alice} or k_{Bob} is 0 or $1-\left(1-\frac{1}{4}\right)^{q}$, respectively. Using any advanced impersonation attack for a man-in-the-middle attack Eve's success and detection probabilities even deteriorate.

4.4 Suggestions for Improvements

As shown in the previous security analysis, protocol 1 features high security properties for any kind of discussed attack, i.e. high detection and low success probability.

A prearranged sign, included in the final message, or a request identification may be considered to hamper Eve's impersonation attacks. An initial sign would lead to key distribution problems as known from private-key cryptography. Without such a sign the users have no chance to detect an attack at the final stage of classical communication. But if they complete the eavesdropping tests accurately, a secret sign is not necessary. Identification to authenticate a request can be arranged without key distribution problems, because each user meets Trent to share an ID. Nevertheless, there is no need of such information, since an attacker, impersonating the "communication initialiser", cannot succeed to a sufficient degree.

Despite the high security, protocol 1 may be improved in the following two aspects. Bob completely proposes the key, which has consequences regarding the randomness and fairness as emphasised in most key distribution protocols. The second and more important aspect considers the adaption of the protocol to the multiuser concept, as suggested in the original paper ("We expect our protocol can well be adjusted to be incorporated in future quantum networks.", p. 7). The extra quantum channel between Alice and Bob for the transmission of Bob's encoded key values is not compatible with multiuser networks (cf. fig. 4, p. 20). The following section discusses an improved proposal based on the original protocol 1, which implements both aspects.

4.5 Improved Proposal 1

To eliminate the use of the extra quantum channel between Alice and himself, Bob can send his encoded particles to Trent instead of Alice. Alice and Trent then exchange their measurement tasks, i.e. Alice measures her A-particles in the x basis, whereas Trent projects his T-qubits and Bob's B-particles onto the Bell basis and publicly reveals the Bell states (see tab. 4.4).

Operation of Alice		Bob		Transformation of GHZ states
I	(0)	I	(0)	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{TB}\|+\rangle_A + \|\Phi^-\rangle_{TB}\|-\rangle_A)$
I	(0)	H	(1)	$\frac{1}{2}(\|\Phi^+\rangle_{TB}\|-\rangle_A + \|\Phi^-\rangle_{TB}\|+\rangle_A + \|\Psi^+\rangle_{TB}\|+\rangle_A + \|\Psi^-\rangle_{TB}\|-\rangle_A)$
H	(1)	I	(0)	$\frac{1}{2}(\|\Phi^+\rangle_{TB}\|+\rangle_A + \|\Phi^+\rangle_{TB}\|-\rangle_A + \|\Phi^-\rangle_{TB}\|+\rangle_A - \|\Phi^-\rangle_{TB}\|-\rangle_A)$
H	(1)	H	(1)	$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{TB}\|+\rangle_A - \|\Phi^+\rangle_{TB}\|-\rangle_A + \|\Phi^-\rangle_{TB}\|+\rangle_A + \|\Phi^-\rangle_{TB}\|-\rangle_A + \|\Psi^+\rangle_{TB}\|+\rangle_A + \|\Psi^+\rangle_{TB}\|-\rangle_A + \|\Psi^-\rangle_{TB}\|+\rangle_A - \|\Psi^-\rangle_{TB}\|-\rangle_A)$

Table 4.4: Provisional Results of QKD in the Improved Proposal 1

Exchanging the measurement tasks poses new challenges. If Trent publishes $|\Phi^+\rangle_{TB}$ or $|\Phi^-\rangle_{TB}$, Alice can derive Bob's operation only with an identity operation on her side, due to the different x basis measurement results $|+\rangle_A$ or $|-\rangle_A$ for Bob's identity or Hadamard operations. Moreover, Eve can deduce H_B and a key bit of 1, if she overhears the results $|\Psi^+\rangle_{TB}$ or $|\Psi^-\rangle_{TB}$. To circumvent these problems Alice only performs an identity operation on her qubits, and the states $|\Psi^\pm\rangle_{TB}$ cannot be included in the key subset, but can be used in the test subset.

Considering Bob's complete proposal of the key, the qubit set is divided in two subsets of the same size. Bob performs identity or Hadamard operations on his first subset and sends it to Trent. He leaves his second subset untransformed (I_B) and keeps it for measurements in the x basis. Alice only performs identity operations on her first subset, but identity and Hadamard operations on her second subset. She sends Trent all qubits of the second subset and keeps the first subset for measurements in the x basis. With this modification Bob proposes the first part of the key encoded in the first subset and Alice suggests its second part by her operations on the second subset. The results of table 4.4 are modified according to these issues and listed in table 4.5 (p. 40). Table 4.6 (p. 41) shows an overview of all results, including the states which can only be used to check for eavesdropping.

First subset		
Operation of Alice	Bob	Transformation of GHZ states
I	I (0)	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{TB}\|+\rangle_A + \|\Phi^-\rangle_{TB}\|-\rangle_A)$
I	H (1)	$\frac{1}{2}(\|\Phi^+\rangle_{TB}\|-\rangle_A + \|\Phi^-\rangle_{TB}\|+\rangle_A + \|\Psi^+\rangle_{TB}\|+\rangle_A + \|\Psi^-\rangle_{TB}\|-\rangle_A)$
Second subset		
Operation of Bob	Alice	Transformation of GHZ states
I	I (0)	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_B + \|\Phi^-\rangle_{AT}\|-\rangle_B)$
I	H (1)	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_B + \|\Phi^-\rangle_{AT}\|+\rangle_B + \|\Psi^+\rangle_{AT}\|+\rangle_B - \|\Psi^-\rangle_{AT}\|-\rangle_B)$

Table 4.5: Expected Results of QKD in the Improved Proposal 1
For a detailed derivation see appendix C.1.2.

4.5.1 Protocol

At the request of Alice as the "communication initialiser", Trent prepares an orderly set $|\Theta\rangle_{ATB}$ of n tripartite entangled GHZ states $|\theta\rangle_{ATB}$ with

$$|\Theta\rangle_{ATB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_n\rangle)_{ATB} \text{ of}$$
$$|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \text{ with } i = 1, 2, \ldots, n \ . \tag{II}$$

The subscripts A, T, and B label the particles for Alice, Trent, and Bob, respectively. The amount n consists of $N + n_{DIS} + c_{AUTH} + c_{QKD}$ qubits. The N qubits form the final key, and the n_{DIS} qubits are discarded in the key arrangement to avoid the revelation of a Hadamard operation with the Bell states $|\Psi^{\pm}\rangle$ to Eve. The c_{AUTH} and the c_{QKD} qubits are used to check for eavesdropping. The amount c_{QKD} does not have to be on the same large scale as in the original protocol, because the n_{DIS} particles are also included in the test subset.

Trent encodes the respective particles of any $|\theta_i\rangle_{ATB}$ according to the authentication keys and transmits them to Alice and Bob. After reception Alice and Bob decode their qubits and, thereby, restore the original GHZ states. To test for eavesdropping Alice and Bob compare c_{AUTH} random check qubits after z basis measurements, proceeding as specified in section 3.3. If their particles are perfectly correlated, they know that the transmission was secure, and they are authenticated as legitimate network users. Otherwise, communication is aborted and restarted with a new qubit set.

For the key arrangement each user divides the set of the remaining restored $N+n_{DIS}+c_{QKD}$ particles into two subsets of the same size. Bob encrypts his secret information in his B-particles of the first subset, performing identity or Hadamard operations on them. Alice performs an identity operation on her A-particles of this subset. Bob stores the record of his operations secretly. On the second subset Alice performs identity or Hadamard operations on her A-qubits to encode her secret information, and Bob leaves his qubits untransformed (I_B). Alice keeps the record of her operations secretly.

Bob and Alice send their encoded qubits of the first and the second subset over their quantum link to Trent, respectively. Trent performs Bell measurements on pairs of qubits of the first subset, consisting of his T-qubits and Bob's B-particles, and announces the outcomes. Alice measures her A-particles in the x basis. Trent then projects his T-particles and Alice's A-qubits of the second subset onto the Bell basis and reveals these outcomes as well. Bob measures his B-particles in the x basis.

The original GHZ states of the first subset are transformed after Bob's operations and Alice's and Trent's measurements. Alice can derive Bob's operations and his proposition of the key values. In contrast, Bob deduces Alice's operations and her proposal of the key bits from the second subset (tab. 4.6).

Alice and Bob compare their results with their operations and Trent's Bell states in a second eavesdropping test dialogue. Any appearances of the n_{DIS} states $|\Psi^{\pm}\rangle_{TB}$ or $|\Psi^{\pm}\rangle_{AT}$ are used in the test subset, since these states are useless for the key arrangement. The test subset additionally includes c_{QKD} random check qubits, occurring with other Bell states. If all check qubits coincide, the remaining N qubits are translated into key values and form the final key. In case of any irregularities, the communication is aborted and a new communication round is initiated.

First subset			
Trent's announcement	Alice's outcome	Alice's conclusion	key value (proposed by Bob)
$\|\Phi^+\rangle_{TB}$	$\|+\rangle_A$	I_B	0
	$\|-\rangle_A$	H_B	1
$\|\Phi^-\rangle_{TB}$	$\|+\rangle_A$	H_B	1
	$\|-\rangle_A$	I_B	0
Second subset			
Trent's announcement	Bob's outcome	Bob's conclusion	key value (proposed by Alice)
$\|\Phi^+\rangle_{AT}$	$\|+\rangle_B$	I_A	0
	$\|-\rangle_B$	H_A	1
$\|\Phi^-\rangle_{AT}$	$\|+\rangle_B$	H_A	1
	$\|-\rangle_B$	I_A	0
Test subset			
Trent's announcement	expected outcome	possible conclusion	key value
$\|\Psi^+\rangle_{TB}$	$\|+\rangle_A$	H_B	-
$\|\Psi^+\rangle_{AT}$	$\|+\rangle_B$	H_A	-
$\|\Psi^-\rangle_{TB}$	$\|-\rangle_A$	H_B	-
$\|\Psi^-\rangle_{AT}$	$\|-\rangle_B$	H_A	-

Table 4.6: Overview of Expected Results of QKD in the Improved Proposal 1
See also table 4.4 or appendix C.1.2.

4.5.2 Security Analysis

The security of the improved protocol is still based on the properties of the GHZ state entanglement. The authentication process remains embedded within the communication, since authentication and key distribution are completed on the same qubit set, which is transmitted encoded. Eve cannot avoid any checking procedure, because the check positions are revealed after transmission.

Trent cannot be successful in passive eavesdropping, since a single Bell state $|\Phi^{\pm}\rangle$ does not reveal any information about the user's operation (cf. tab. 4.6, p. 41). To actively eavesdrop Trent does not have to intercept the user's qubits, because both users send their qubits directly to him. Furthermore, he can now fake a Bell measurement partially, i.e. he measures the received particle and his qubit in the z basis and announces a matching Bell state. For instance, if Trent measures $|0\rangle_U|0\rangle_T$ or $|0\rangle_U|1\rangle_T$, he reveals $|\Phi^{\pm}\rangle_{UT}$ or $|\Psi^{\pm}\rangle_{UT}$, respectively. Trent's success probabilities in the attack remain the same, although the system transformations differ (see appendix E.1 for details). His information gain may lead to sufficient knowledge of the distributed key, but Trent's intermediate step causes errors. As already mentioned, Trent can fake a Bell measurement only in parts. Indeed, he can derive the correct type of Bell state ($|\Phi\rangle$ or $|\Psi\rangle$), but he cannot deduce the correct exponent of the type (e.g. $|\Phi^{+}\rangle$ or $|\Phi^{-}\rangle$). Furthermore, his measurement forces the particle of the other user, intended for x basis measurement, into a fixed state. Thus, the result of the x basis measurement is random. There may be matching combinations in terms of expected, correct results, but there are certainly incorrect combinations as well. Due to these errors, Alice and Bob can detect irregularities in the process in the following eavesdropping test and abort communication without key arrangement.

Eve's eavesdropping on the authentication process remains unchanged in the improved proposal, since authentication exactly proceeds as in the original protocol (see s. 4.3.2 for details). Although Eve can achieve a nonzero success probability, the detection probability is at least 25 % per check qubit in any attack. The publicly discussed test subset, which is essential for her impersonation attack, is quite small. The authentication keys are re-newed for further communication and their calculation is based on a one-way hash function, so that Eve cannot be successful in eavesdropping on the authentication.

In an eavesdropping attack on the key distribution Eve must attack the B-qubits of the first and the A-qubits of the second subset. The detection probabilities of both translucent attacks do not change in the improved proposal, even though their derivation does (see appendix E.3). Alice and Bob still detect Eve with the probability of $\rho_D = 1 - \left(1 - \frac{1}{2} - \frac{\beta^2+\beta'^2}{8}\right)^{c_{AUTH}}$ in the first translucent attack and with the probability of $\rho_D = 1 - \left(1 - \frac{5}{16}\right)^{c_{AUTH}}$ in the second attack.

In an impersonation of the sender Eve must face detection in both eavesdropping tests and faulty system transformations because of her restoring problems of the A-qubits. The detection probability during authentication does not change in the proposal, it remains $1-\left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$). For key distribution Bob performs identity and Hadamard operations

on his B-particles of the first subset, while Eve leaves her $E(A)$-qubits untransformed ($I_{E(A)}$). On the second subset Eve performs identity and Hadamard transformations. In both subsets Eve's restoring errors must be considered (see appendix E.4 for details). In the second eavesdropping test the detection probability amounts to $1-\left(1-\frac{3}{16}\right)^{c_2}$ in the first subset and to $1-\left(1-\frac{1}{2}\right)^{c_2}$ in the second subset (with $c_2 = c_{QKD}/2$). Hence, overall detection probability adds up to 34.375 % per check qubit when Eve announces her result, i.e. $1-\left(1-\frac{11}{32}\right)^{c_2}$ (with $c_2 = c_{AUTH}/2$). In the unlikely case of remaining undetected during the entire communication round, Eve can derive Bob's operations on the first subset only for states $|\Psi^{\pm}\rangle_{TB}$, which are not considered in the key arrangement. Thus, Eve deduces a key value, but this value is not used to form the key. In the second subset Bob derives Alice's operations, and Eve must try to deduce Bob's derivation of these operations. Since she does not know Bob's x basis measurement result, she cannot deduce Bob's derivation in any case. Again, states of the types $|\Psi^{\pm}\rangle_{E(A)T}$ with an unequivocal conclusion on $H_{E(A)}$ are not considered for the key arrangement.

The second impersonation attack, the impersonation of the receiver, proceeds similarly. Again, Eve must face both eavesdropping tests and the restoring errors of her $E(B)$-particle, which induce wrong system transformations. In the key distribution phase Eve performs identity or Hadamard operations on the first subset and Alice performs these operations on the second subset (see appendix E.4 for details). Alice and Eve cannot correctly derive each others operations, regarding states only considered for the key. The detection probabilities remain the same as in the sender impersonation, that is $1-\left(1-\frac{1}{4}\right)^{c_1}$ during authentication and $1-\left(1-\frac{11}{32}\right)^{c_2}$ during key distribution (with $c_1 = c_{AUTH}/2$ and $c_2 = c_{QKD}/2$).

Eve may try to take advantage of the additional possession of Trent's T-qubits in an advanced impersonation attack. Preparing GHZ states Eve does not cause errors when decoding the particles of the impersonated user, but the correctly decoding of the legitimate user leads to restoring errors. Hence, the restoring problem is exchanged between the sides of the communication parties (see appendix E.5).

An impersonation of both the sender and the authority results in states of the type $|\Omega^{\pm}\rangle_{E(T)B}|\pm\rangle_{E(A)}$ in the first and $|\Omega^{\pm}\rangle_{E(A)E(T)}|\pm\rangle_{B}$ in the second subset with $|\Omega\rangle$ denoting $|\Phi\rangle$ or $|\Psi\rangle$. Because Trent also publishes his Bell states in the first simple impersonation attack, $|\Omega^{\pm}\rangle_{E(T)B}|\pm\rangle_{E(A)}$ or $|\Omega^{\pm}\rangle_{E(A)E(T)}|\pm\rangle_{B}$ does not provide Eve with more information as $|\Omega^{\pm}\rangle_{TB}|\pm\rangle_{E(A)}$ or $|\Omega\rangle_{E(A)T}|\pm\rangle_{B}$, respectively. To encode for key distribution Bob transforms the system of the first subset, but he also unintentionally transforms it when he decodes his particles. Thus, Eve cannot derive his operation in the key arrangement. In the second subset Eve lacks the additional information of Bob's x basis measurement to deduce Bob's derivation. The detection probability of $\rho_D = 1-\left(1-\frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) during authentication remains as in the simple impersonation attacks. The detection probability in the second eavesdropping test during key distribution slightly increases to $\rho_D = 1-\left(1-\frac{3}{8}\right)^{c_2}$. Moreover, Bob can detect Eve beyond any eavesdropping test with a probability of $\rho_{D_{add}} = \frac{1}{32}$ per qubit.

An impersonation of the receiver and the authority can likewise be analysed. In the first subset Eve does not know Alice's x basis measurement result without which she cannot deduce Alice's derivation. Eve cannot derive Alice's operation on the first subset, since she does not know, whether Alice changes her particle intentionally or not. The detection probabilities remain as given in the first advanced impersonation attack of the proposal, i.e. 25 % per any second check qubit in the first authentication test, 37.5 % per any second check qubit in the second eavesdropping test during key distribution, and 3.125 % per qubit beyond any eavesdropping test.

Eve impersonates the authority to tap the full potential of his information gain. There are even higher detection probabilities due to the restoring errors which occur on both sides of the communication parties and transform the system uncontrollably. As shown in the security analysis of the original protocol (s. 4.3.5.3), the detection probability amounts to $1 - \left(1 - \frac{3}{8}\right)^{c_{AUTH}}$ during authentication and to over 50 % per check qubit during key distribution. An additional detection probability of around 3 % per qubit is achieved beyond the tests. Again, Eve cannot be successful in the impersonation of the authority.

The improved protocol also prevents a man-in-the-middle attack, i.e. a combination of both simple impersonation attacks. A man-in-the-middle attack is impossible in the sense of useful key arrangement because of the necessary but complex management tasks, but mainly because Eve cannot be successful in at least one simple impersonation.

The adaption of the original protocol 1 to the multiuser network concept and the elimination of Bob's one-sided key suggestion does not adversely affect the security of the protocol. The analysis of the improved protocol yields the conclusion that it provides high security against all analysed attacks on a similar scale as the original protocol.

Chapter 5

Authenticated MQDC

The paper *Quantum Direct Communication with Authentication* (Lee et al., 2005) proposes two quantum direct communication protocols, which slightly vary in the tasks of the involved parties but not in the basic approach. This section focuses on the second presented protocol (protocol 2), since it is compatible to the multiuser concept. The differences of the two protocols of the original paper are shortly discussed at the end of section 5.2.

After successful authentication via the third party Trent, the sender Alice encodes her secret message bits in qubits. The receiver Bob can extract the message from the entire system after certain proceedings. Hence, the message is directly sent from Alice to Bob within the quantum system, and neither a classical channel nor conventional cryptographic techniques are needed for its transmission. The version of the original protocol, published in Physical Review A, can be found in appendix B, an overview is displayed in figure 2 (p. 18).

5.1 Authentication

The authentication of protocol 2 proceeds exactly as in protocol 1. At Alice's request, Trent prepares an orderly set $|\Theta\rangle_{ATB}$ of n tripartite entangled GHZ states $|\theta\rangle_{ATB}$ with

$$|\Theta\rangle_{ATB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_n\rangle)_{ATB} \text{ of}$$
$$|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \tag{III}$$

with $i = 1, 2, \ldots, n$ and the composition $n = N + c_{AUTH} + c_{QDC}$. The subscripts A, T, and B denote the particles for Alice, Trent, and Bob, respectively. In contrast to protocol 1, N indicates the quantity of message qubits for direct communication and not the length of the distributed key. The amount of check qubits during authentication or quantum direct communication is named c_{AUTH} or c_{QDC}, respectively. Alice or Trent inform Bob about Alice's communication request.

Trent uses Alice's and Bob's authentication keys to encode the A- and B-particles of each $|\theta_i\rangle_{ATB}$ and sends them to the users. He keeps his own T-particle in a safe place. Alice and Bob restore their particles, decoding them with their authentication keys. After measuring

c_{AUTH} random check qubits in the z basis Alice and Bob compare these results in the first eavesdropping test following the dialogue form discussed in 3.3. If their outcomes are as correlated as expected, Alice and Bob are authenticated as legitimate network users and the absence of an attacker during transmission is ascertained. Otherwise, they abort the protocol and restart a new communication round.

5.2 QDC

In preparation of direct communication Alice generates a random bit string of length c_{QDC}, which is not related to the secret message to Bob, and chooses a control subset from her remaining restored A-qubits on the scale of c_{QDC}. She encodes the bit string in the control subset and her secret message in the N remaining A-qubits. Alice executes a Hadamard operation H_A to encode the bit 0. Performing a Hadamard operation with previous bit flipping ($H_A X_A$) encodes the bit 1. Bob does not transform his restored B-particles.

After encoding Alice sends her A-particles to Trent. He forms pairs consisting of one A-qubit and one T-qubit, projects pair by pair onto the Bell basis, and reveals the resultant Bell states. In the original paper Trent announces 0 for $|\Phi^+\rangle$ and $|\Psi^-\rangle$ and 1 for the other two states $|\Phi^-\rangle$ and $|\Psi^+\rangle$. This suggestion is not pursued here, since it does not affect the security under the analysed conditions. Bob subjects his B-particles to a measurement in the x basis. Alice's operation and Trent's and Bob's measurements transform the original $N + c_{QDC}$ GHZ states as listed in table 5.1 (p. 47). Bob derives Alice's operations with his supplementary information of the x basis result. Thus, he can extract her secret message from the system retranslating her operations H_A or $H_A X_A$ into the bits 0 or 1, respectively. For instance, Trent revealed the Bell state $|\Psi^-\rangle_{AT}$, and Bob measured the state $|+\rangle_B$. Bob then deduces that Alice performed a bitflip operation followed by a Hadamard operation, i.e. Alice encoded the value 1 (cf. row 2 in tab. 5.1).

In the following second test dialogue Alice reveals the positions of her c_{QDC} check qubits to Bob and compares them with him. This dialogue varies from that given in section 3.3. As Alice reveals all check positions, Bob announces his result in accordance with Alice's check position instead of any position of his choice at his first turn. If all results coincide, no eavesdropping took place, and Alice directly communicated with Bob. In case of an error rate higher than expected, Alice initialises a new communication round.

In the other protocol proposed in Lee et al. (2005) Alice sends her encoded particles to Bob instead of Trent. Bob performs the Bell measurements with the A- and B-qubits, whereas Trent measures his T-particles in the x basis and announces the outcomes. To adapt table 5.1 of Bob's derivation of Alice's message bits to this different procedure, subscripts B and T must be exchanged. For the transmission of the A-qubits to Bob the network must include an additional direct quantum link between the users. Thus, the protocol is not applicable to the multiuser concept discussed in section 3.1.

Alice's operation	Transformation of GHZ states
H (0)	$\frac{1}{2}(\|\Phi\rangle^{+}_{AT}\|-\rangle_B + \|\Phi\rangle^{-}_{AT}\|+\rangle_B + \|\Psi\rangle^{+}_{AT}\|+\rangle_B - \|\Psi\rangle^{-}_{AT}\|-\rangle_B)$
HX (1)	$\frac{1}{2}(\|\Phi\rangle^{+}_{AT}\|+\rangle_B + \|\Phi\rangle^{-}_{AT}\|-\rangle_B - \|\Psi\rangle^{+}_{AT}\|-\rangle_B + \|\Psi\rangle^{-}_{AT}\|+\rangle_B)$

Table 5.1: Expected Results of QDC
Source: Lee et al. (2005)
For a detailed derivation see appendix C.2.1

5.3 Security Analysis

The security of the authentication and the quantum direct communication result from the properties of the GHZ state entanglement. Again, the communication parties work on one qubit set for authentication and direct communication, i.e. the authentication is embedded in the communication, and all particles are transmitted encoded. Revealing the check positions after transmission is completed prevents that the attacker Eve avoids any control procedure.

5.3.1 Eavesdropping of Trent

The analysis of protocol 2 regarding Trent's passive eavesdropping yields the conclusion that no information automatically leaks to him. Trent's task during QDC is to project Alice's and his particles onto the Bell basis and to announce the outcomes. Any Bell state of type $|\Phi^+\rangle_{AT}$, $|\Phi^-\rangle_{AT}$, $|\Psi^+\rangle_{AT}$, and $|\Psi^-\rangle_{AT}$ occurs with the same probability of $\frac{1}{4}$ for both of Alice's operations H_A or $H_A X_A$. Bob's x basis measurement result is essential to deduce her operation (cf. tab. 5.1, p. 47).

As Zhang (2006) pointed out, Trent can successfully launch an active eavesdropping attack, though (see appendix F.1 for detailed calculations). Alice sends her transformed A-qubits to Trent. An additional Hadamard operation of Trent on an A-particle preserves only Alice's bitflip operation X_A, due to the properties of a unitary Hadamard operation. Hence, measuring an A- and a T-qubit of the same state in the z basis leads to the same results for a previous Hadamard operation of Alice and to different outcomes, if Alice flipped her qubit before performing a Hadamard operation. With the knowledge of Alice's operations Trent can extract Alice's secret message bits. To avoid immediate detection he reveals any Bell state of his choice.

Trent's intermediate step increases the error rate, because Trent has no other choice but to announce a random Bell state. Additionally, Bob's particle collapses into a fixed state due to Trent's measurement. Hence, the result of Bob's x basis measurement is also random. Wrong combinations of Bell states and x basis measurement results are very likely to occur in the second eavesdropping test between Alice and Bob. Due to these irregularities they abort the communication.

Unfortunately, due to the characteristic of the protocol, the eavesdropping test can take place only after the message transfer. Hence, Trent already knows the entire message at the time of the test and the observation of the irregularities. Alice and Bob may not realise that

their message completely leaked out, since they trust Trent and perceive Eve's interception as the reason for the high error rate. Contrary to Trent's attack in the previous protocol, its consequence endangers security more profoundly here. A proposal to avoid the attack is published in Zhang (2006) and discussed in section 5.4.

5.3.2 Eavesdropping on Authentication

The attacks against authentication proceed as discussed in protocol 1, since protocol 2 uses the same authentication procedure. They are summarised here only briefly (see s. 4.3.2 for details).

In an impersonation of Trent Eve must encode the values of the respective authentication keys in the GHZ states prepared by herself. The detection probability amounts to 37.5 % per c_{AUTH} check qubits, i.e. $\rho_D = 1-\left(1-\frac{3}{8}\right)^{c_{AUTH}}$. Although the probability to derive one or both key value(s) per pair of id_{iA} and id_{iB} totals 37.5 % or 6.25 %, respectively, Eve obtains this information of the small subset only on the scale of c_{AUTH}. An intercept-resend attack and both translucent attacks offer a detection probability of at least $1-\left(1-\frac{1}{4}\right)^{c_{AUTH}}$, which highly limits Eve's potential success. Furthermore, Eve's information gain of any authentication key becomes obsolete in further communication rounds and cannot be used to reverse the (secret) one-way hash function to gather the underlying user ID.

5.3.3 Eavesdropping on QDC

Eve may attack Alice's qubits transfered to Trent by entangling her probes with the transmitted particles in a translucent attack to gain knowledge about Alice's message to Bob (see appendix F.3 for detailed calculations). Both unitary operations (A) and (B) transform the system, leading to a high detection probability of $1-\left(1-\frac{1}{2}\right)^{c_{QDC}}$. An intercept-resend attack on Alice's qubits does not lead to any knowledge gain for Eve. After intercepting the encoded A-particles Eve measures 0 or 1 with the same probability for both of Alice's operations. Thus, Eve cannot distinguish between them.

The calculation of the first translucent attack with unitary transformation (A) differs from the one given in the original paper in two aspects. First, after Alice's operations the system can be written according to the equation

$$\frac{1}{2}(|000\rangle \pm |100\rangle + |011\rangle \mp |111\rangle)_{ATB} \ , \tag{9}$$

where the upper sign line represents the state after Alice's Hadamard operation and the lower sign line denotes the state after Alice's bitflip and Hadamard operations. In the original paper the sign lines are transposed. However, the resultant term shows the same signs as the result in this analysis (cf. appendix F.3, eq. (222)). Second, the fraction in front of the result differs. It is $\frac{1}{2\sqrt{2}}$ in the original paper but $\frac{1}{4}$ in this analysis. The fraction is derived from multiplying the term by four to cover all four results $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ and then factorising $\frac{1}{2}$ to formally

calculate the Bell and the x basis measurement, e.g.

$$\begin{aligned} & \frac{1}{2}\left[(|00\rangle + |11\rangle)_{AT}(|0\rangle + |1\rangle)_B\right] \\ = \; & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B \\ = \; & |\Phi\rangle_{AT}|+\rangle_B \; . \end{aligned} \tag{10}$$

Although it depends on the fraction, the detection probability of $\rho_D = \frac{1}{2}$ is equal in both works.

5.3.4 Simple Impersonation Attacks

In a simple impersonation attack Eve impersonates a user during an entire communication round. Assuming Alice is the "communication initialiser", there are two different kinds of impersonation attacks. In the first impersonation attack Eve impersonates the sender with the aim to send Bob her own message. In an impersonation of the receiver Eve intends to read Alice's secret message. The results of both simple impersonation attacks are calculated in detail in appendix F.4.

If Eve manages to pass both eavesdropping tests without detection, neither Bob in the first attack nor Alice in the second attack can notice Eve's interception. An initial secret sign could only prevent the impersonation of the sender, but would lead to key distribution problems. Thus, it is no assumed in the following.

5.3.4.1 Sender Impersonation

Supposing the legitimate Alice does not know about an ongoing communication round, Eve does not have to cut the line between Alice and the network. She just needs a possibility to intercept Alice's quantum and public channels.

At Eve's request, Trent prepares n GHZ states (with $n = N + c_{AUTH} + c_{QDC}$), encodes the respective particles with Alice's and Bob's authentication keys, and transmits the encoded qubits. If the request was only valid with some kind of identification information, this type of impersonation attack would fail instantly.

After intercepting Alice's A-qubits (the $E(A)$-qubits from here on) Eve must make a decision regarding the decoding operations I or H determined by Alice's authentication key. As in the previous protocol 1, this decoding is not only essential for passing the eavesdropping test during authentication but also for minimising subsequent errors in the direct communication. As in the impersonation attack of protocol 1, Bob can detect Eve with a probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) in the first eavesdropping test. A detection probability on such a scale probably leads to communication abort.

In the unlikely case that Bob does not detect Eve and does not abort communication, he measures his restored $N + c_{QDC}$ particles in the x basis. According to her binary control string and her fake message, Eve performs the necessary operations on her $E(A)$-qubits and sends the particles to Trent. Trent projects each received particle with his T-qubit of the

same position onto the Bell basis and announces the outcome. Table 5.2 lists the transformations of the original GHZ states for both of Eve's operations. Some discrepancies with the expected results exist in the system, due to the fact that Eve cannot obtain perfectly restored $E(A)$-particles.

Operation	Transformation of GHZ states
H	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_B + \|\Phi^-\rangle_{AT}\|+\rangle_B + \|\Psi^+\rangle_{AT}\|+\rangle_B - \|\Psi^-\rangle_{AT}\|-\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_B + \|\Phi^-\rangle_{AT}\|-\rangle_B)$
HX	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|+\rangle_B + \|\Phi^-\rangle_{AT}\|-\rangle_B - \|\Psi^+\rangle_{AT}\|-\rangle_B + \|\Psi^-\rangle_{AT}\|+\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AT}\|-\rangle_B + \|\Phi^-\rangle_{AT}\|+\rangle_B)$

Table 5.2: Results of QDC I
For the sender impersonation attack subscript A must be replaced by $E(A)$. Restoring errors occur for incorrectly decoding the correctly encoded A-qubits. For the impersonation of the receiver and the authority subscripts T and B must be replaced by $E(T)$ and $E(B)$, respectively. Restoring errors appear for correctly decoding the non-encoded A-qubits.

In the second eavesdropping test on the c_{QDC} check qubits Bob detects Eve with the probability of $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_2}$ (with $c_2 = c_{QDC}/2$), since Eve can only avoid detection at any of Bob's turns to make the first announcement. In addition to the high detection probability Eve cannot control the message bit for any $|\Phi^{\pm}\rangle_{E(A)T}$, because both of her operations transform the system into the entire results $|\Phi^{\pm}\rangle_{E(A)T}|\pm\rangle_B$. Although Bob derives exactly one operation from the combination of Bell state and x basis result, Eve cannot deduce his derivation without the particular x basis result. Hence, Bob extracts random message bits at these positions. Eve's success probability per qubit q, i.e. the probability of controllable message bits, totals $\rho_S = 1 - \left(1 - \frac{1}{4}\right)^q$. Bob cannot recognise the message as a fake message at this last stage. But he definitely obtains different information, if any, than Eve intended to send. Thus, the impersonation of the sender has practically no chance to succeed, since the attack leads to high detection probabilities and a low success probability.

5.3.4.2 Receiver Impersonation

In the receiver impersonation Eve tries to receive Alice's secret message. Depending on the message content, Eve may only need to avoid detection in the first eavesdropping test during authentication. If the content represents valuable information to Eve even in the case that Alice recognises the leakage of the message in hindsight, Eve does not have to participate in the second eavesdropping test. She already knows the message after Alice's operations, Trent's Bell state announcements, and her x basis measurements. Again, if Eve intercepts Alice's communication notification to Bob, she does not have to cut the line between Bob and the network. The attack cannot be prevented with a request identification information, since the legitimate Alice launches the request.

After the interception of the B-particles (now the $E(B)$-particles) of the n GHZ states (with $n = N + c_{AUTH} + c_{QDC}$) Eve must decode them with unitary operations depending on Bob's authentication key. Faulty decoding leads to a higher detection probability and difficulties when extracting the final message.

The detection probability during the authentication phase remains $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$), and it is implausible that Eve reaches the communication stage. Assuming Alice does not abort communication, she performs operations H_A or $H_A X_A$ to encode her control string and her message, and sends these encoded qubits to Trent. Trent performs Bell basis measurements and announces the resultant Bell states. Meanwhile, Eve measures her $E(B)$-particle in the x basis. Table 5.3 presents the transformed GHZ states after all tasks for direct communication are implemented.

Operation	Transformation of GHZ states
H	$\frac{1}{2}(\lvert\Phi^+\rangle_{AT}\lvert-\rangle_B + \lvert\Phi^-\rangle_{AT}\lvert+\rangle_B + \lvert\Psi^+\rangle_{AT}\lvert+\rangle_B - \lvert\Psi^-\rangle_{AT}\lvert-\rangle_B)$
	$\frac{1}{2\sqrt{2}}(\lvert\Phi^+\rangle_{AT}\lvert+\rangle_B - \lvert\Phi^+\rangle_{AT}\lvert-\rangle_B + \lvert\Phi^-\rangle_{AT}\lvert+\rangle_B + \lvert\Phi^-\rangle_{AT}\lvert-\rangle_B +$ $\lvert\Psi^+\rangle_{AT}\lvert+\rangle_B + \lvert\Psi^+\rangle_{AT}\lvert-\rangle_B - \lvert\Psi^-\rangle_{AT}\lvert+\rangle_B + \lvert\Psi^-\rangle_{AT}\lvert-\rangle_B)$
HX	$\frac{1}{2}(\lvert\Phi^+\rangle_{AT}\lvert+\rangle_B + \lvert\Phi^-\rangle_{AT}\lvert-\rangle_B - \lvert\Psi^+\rangle_{AT}\lvert-\rangle_B + \lvert\Psi^-\rangle_{AT}\lvert+\rangle_B)$
	$\frac{1}{2\sqrt{2}}(\lvert\Phi^+\rangle_{AT}\lvert+\rangle_B + \lvert\Phi^+\rangle_{AT}\lvert-\rangle_B + \lvert\Phi^-\rangle_{AT}\lvert+\rangle_B - \lvert\Phi^-\rangle_{AT}\lvert-\rangle_B -$ $\lvert\Psi^+\rangle_{AT}\lvert+\rangle_B + \lvert\Psi^+\rangle_{AT}\lvert-\rangle_B + \lvert\Psi^-\rangle_{AT}\lvert+\rangle_B + \lvert\Psi^-\rangle_{AT}\lvert-\rangle_B)$

Table 5.3: Results of QDC II
In the receiver impersonation attack subscript B must be replaced by $E(B)$. Restoring errors occur for incorrectly decoding the correctly encoded B-qubits. In the impersonation of the sender and the authority subscripts A and T must be exchanged with $E(A)$ and $E(T)$, respectively. Restoring errors appear for correctly decoding the non-encoded B-qubits.

During the second eavesdropping test on the c_{QDC} check qubits Alice can detect Eve with the probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_2}$ (with $c_2 = c_{QDC}/2$). In addition to the high detection probability, both of Alice's operations lead to the same entire results, i.e. Trent's Bell states together with Eve's x basis measurement outcomes. Since Eve cannot distinguish between Alice's operations, she cannot derive Alice's message bits. Hence, Eve obtains a success probability of zero.

5.3.5 Advanced Impersonation Attacks

To improve her impersonation attack results Eve may additionally impersonate the authority. Her advantage in an advanced impersonation attack is the possibility to measure Trent's particle, which is entangled with the system. In this attack Eve must accomplish the preparation and the encoding of the GHZ states. It is assumed again that Eve transmits the users' particles unencoded. As already discussed, her other option – guessing the respective authentication key – leads to the same result.

Assuming that Alice initialises the communication, the analysis discusses two advanced impersonation attack. A supplementary third advanced impersonation attack, the impersonation of Trent, is added. If the first attack is successful, Eve can send Bob a fake message. The goal of the other two attacks is to read Alice's original message.

Because of key distribution problems an initial sign, included in the final message, cannot be assumed. An identification information necessary to launch a request does not prevent the attacks, because the legitimate Trent and his controlling function are excluded. Detailed calculation of all advanced impersonation attacks can be found in appendix F.5.

5.3.5.1 Impersonation of Sender and Authority

Eve's first task in an impersonation of Alice and Trent is the preparation of the n GHZ states (with $n = N + c_{AUTH} + c_{QDC}$). She sends Bob his unencoded B-particles and keeps the A- and T-qubits (henceforth called the $E(A)$- and $E(T)$-qubits, respectively).

After receiving the B-particles Bob decodes them with his authentication key. As Eve left the particles unencoded, restoring errors occur during Bob's decoding. Thus, Bob can detect the attack during the eavesdropping tests, because he supposes his authentication key is correct and attributes a higher error rate to an attack. The detection probability remains $1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$).

If Bob fails to abort communication, Eve encodes the $E(A)$-particles according to her control string and her message to Bob, and projects pair by pair, consisting of an $E(A)$-qubit and an $E(T)$-particle, onto the Bell basis. Bob measures his B-qubit in the x basis. After the measurements the original GHZ states are transformed as in the scenario of the simple receiver impersonation. Thus, table 5.3 (p. 51) is also valid for the results of this advanced impersonation attack with Eve's and Bob's operations in the first and second column, respectively. If Eve knew the entire result including the x basis outcome, she could derive Bob's assumptions of her operation. For instance, Eve could deduce Bob's derivation of HX from the third row with the information of her operation H and the resulting entire state $|\Phi^+\rangle_{AT}|+\rangle_B$ (second row). However, Eve is not in the possession of the entire state. Hence, she cannot derive any of Bob's assumptions of her message bit, so Bob's extraction of the message bits is uncontrollable for Eve, resulting in $\rho_S = 0$. The detection probability during the second eavesdropping test amounts to $\rho_D = 1 - \left(1 - \frac{3}{8}\right)^{c_2}$ (with $c_2 = c_{QDC}/2$).

In comparison to the results of the simple impersonation of the sender, the detection probability during authentication remains the same, whereas the detection probability during direct communication decreases from 50 % to 25 % for every second c_{QDC} check qubit. But Eve's success probability also declines from 25 % to 0 % per qubit, rendering this kind of attack worthless for Eve.

5.3.5.2 Impersonation of Receiver and Authority

After the interception of Alice's request to the legitimate Trent Eve sends Alice her respective n particles of each self-prepared GHZ state (with $n = N + c_{AUTH} + c_{QDC}$). Eve keeps the T- and

B-particles (hence, the $E(T)$- and $E(B)$-particles). Alice's decoding leads to restoring errors on the A-qubit due to Eve's non-encoding. The detection probability in the authentication test remains $1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$).

In the case that communication proceeds, Eve intercepts the A-qubits transfered to Trent after Alice performed her operations on them. The transformations of the GHZ states equal the results of the simple sender impersonation, since the restoring errors occur on the A-particle in both attacks. Table 5.2 (p. 50) can be used to obtain the GHZ transformations with Alice's and Eve's operations in the first and second column, respectively.

Although Eve possesses all particles of the system, she can only be successful in deriving Alice's operations with a state of the types $|\Psi^{\pm}\rangle_{AT}$, i.e. with the probability of 25 % per GHZ state ($\rho_s = 1 - \left(1 - \frac{1}{4}\right)^{q}$). An additional Hadamard operation before Bell measurements, leading to Trent's success in eavesdropping (cf. s. 5.3.1), preserves not only I_A and $X_A I_A$ but also H_A and $X_A H_A$. Thus, Eve cannot gain the same valuable information as Trent.

In comparison with the simple receiver impersonation, the same detection probability during authentication is obtained, whereas the detection probability during direct communication increases from 25 % to 50 % per c_2 check qubits. Alice's probabilities to detect Eve are quite high, but Eve can at least extract the message correctly with the probability of 25 % per qubit.

5.3.5.3 Impersonation of the Authority

Due to the fact that Trent's active eavesdropping promises good success (cf. s. 5.3.1), Eve may try to impersonate him. To acquire the same position Eve must intercept Alice's request to Trent, prepare n GHZ states (with $n = N + c_{AUTH} + c_{QDC}$), and transmit the users' unencoded particles to them. However, unlike Trent Eve does not know the correct encoding information, so that Alice's and Bob's decoding leads to restoring errors. The detection probability during the first eavesdropping test amounts to $\rho_D = 1 - \left(1 - \frac{3}{8}\right)^{c_{AUTH}}$, and the detection probability during the second test totals $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_{QDC}}$.

Trent's success results from distinguishable measurement results of the A- and T-particles after an additional Hadamard operation on the A-qubit. Here an additional Hadamard operation on the A-qubit also preserves only the bitflip operation X_A. But Eve cannot distinguish between Alice's operations during a measurement of the A- and $E(T)$-qubit, because of the restoring errors of both communication parties. Hence, Eve cannot obtain Trent's superior position by impersonating him, and her success probability is 0 %.

5.3.6 Man-in-the-middle Attack

In a man-in-the-middle attack Eve impersonates both communication parties during the entire communication round. The attack can be analysed as a combination of both simple impersonation attacks. If Eve launches a successful man-in-the-middle attack, she can read Alice's message to Bob on the one hand and resend Bob a modified message on the other hand. No user recognises the attack after passed eavesdropping tests, not even in case with a

secret sign in the message.

After Alice's request to Trent Eve must disguise as Bob towards Alice and Trent, and simultaneously impersonate Alice towards Bob and Trent. Both impersonations include all corresponding management and communication tasks. Again, problems appear in the distribution of the GHZ state set, since Eve cannot launch the attack with only one GHZ set (see s. 4.3.6 for a detailed discussion). Certain protocol determinations can prevent multiple requests during one communication round and lead to the instant failure of the attack.

Even if Eve manages all necessary tasks of a man-in-the-middle attack, she cannot succeed to a sufficient degree. As a combination of both simple impersonation attacks the detection probability in the first eavesdropping test already totals $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$), because Alice's and Bob's probabilities are summed up. Hence, passing the tests is highly unlikely. Additionally, Eve can only control her message to Bob with the low probability of $\frac{1}{4}$ per bit. She cannot extract Alice's message at all.

5.4 Suggestions for Improvements

The previous security analysis exposes the high security properties of protocol 2 in all discussed attacks, except Trent's active eavesdropping attack. According to Zhang (2006), a simpler, classical message transfer could be applied, if the protocol was not supposed to render Trent's knowledge of the message impossible. The sender could classically encrypt her message with the authentication key and securely send it to the authority. Trent would decrypt the message, encrypt it again with the receiver's authentication key, and securely transmit it to Bob, who could decrypt it. Section 5.5 discusses the modification suggested by Zhang (2006) in order to revise the security risk of Trent's attack.

Again, it is essential to perform the eavesdropping tests in a very accurate manner. If that is the case, there is no need for an extra sign included in the message. Such a sign is not recommended in order to keep the key amount in the network on the smallest possible scale and to avoid key distribution problems. A request identification is possible without any key distribution problem, since it can be extracted from the already existent user identification information. It would prevent the first simple impersonation attack. However, the additional identification is not necessary for the prevention, because the high detection probabilities surpass the comparatively low success probability by far.

The original paper introduces a random bit string to check the security of the channel during the second eavesdropping test. Alice encodes this string in the c_{QDC} check qubits selected by her, so the choice of the control subset does not alternate between Alice and Bob. Consequently, Alice's position becomes more powerful and the check qubits may not be as random as they are with a selection subdivided into two parts. The characteristics of the protocol do not allow a circumvention of such a procedure. If Bob chose the check qubits in equal shares with Alice, the bits selected by Bob would not be in the final message. The legibility of Alice's message might decrease depending on the number of $c_{QDC}/2$ and the expression precision within the message. The issue should be mentioned, although this work

does not investigate it further. Eve cannot take advantage of it in any attack discussed here.

5.5 Improved Proposal 2

As already mentioned, the protocol is supposed to render Trent's active eavesdropping attack impossible, although he is considered trustworthy in other aspects. Least of all, the opportunity to learn the message before the attack can be realised should be provided.

The author Zhang (2006), disclosing this security risk, also published the improvement discussed in this section. The characteristic of a bitflip operation leads to the recognisability of Alice's operations within the system, so an exchange of the bitflip operation with a Pauli-Z operation takes corrective action. Simply spoken, a Pauli-Z operation switches the sign in the original state $|\theta_i\rangle_{ATB}$ instead of the bit (see eqs. (11) and (12)). With an additional Hadamard operation this different sign causes different signs in the resulting state, leading to the required distinguishable combinations of Bell state exponent and x basis measurement outcome in the entire result (see eqs. (13), (14), and (15)).

$$X_A(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{ATB} \tag{11}$$

$$\sigma_{zA}(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ATB} \tag{12}$$

$$\begin{aligned} H_A(|\theta_i\rangle_{ATB}) &= \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \\ &= \frac{1}{2}\left(|\Phi\rangle^+_{AT}|-\rangle_B + |\Phi\rangle^-_{AT}|+\rangle_B + |\Psi\rangle^+_{AT}|+\rangle_B - |\Psi\rangle^-_{AT}|-\rangle_B\right) \end{aligned} \tag{13}$$

$$\begin{aligned} H_A X_A(|\theta_i\rangle_{ATB}) &= \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATB} \\ &= \frac{1}{2}\left(|\Phi\rangle^+_{AT}|+\rangle_B + |\Phi\rangle^-_{AT}|-\rangle_B - |\Psi\rangle^+_{AT}|-\rangle_B + |\Psi\rangle^-_{AT}|+\rangle_B\right) \end{aligned} \tag{14}$$

$$\begin{aligned} H_A \sigma_{zA}(|\theta_i\rangle_{ATB}) &= \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{ATB} \\ &= \frac{1}{2}\left(|\Phi\rangle^+_{AT}|+\rangle_B + |\Phi\rangle^-_{AT}|-\rangle_B + |\Psi\rangle^+_{AT}|-\rangle_B - |\Psi\rangle^-_{AT}|+\rangle_B\right) \end{aligned} \tag{15}$$

The security is based on these combinations of exponent and x basis state. The algebraic signs of a state cannot be measured in reality, but are used for formally correct calculations. So there is no essential difference in the procedure of the protocol – except the prevention of the eavesdropping leakage. If Trent measures an A- and a T-particle after an additional Hadamard operation, he always receives the same outcomes (cf. eq. (12)). Hence, he cannot gain knowledge of Alice's operations nor the message bits anymore.

5.5.1 Protocol

Since the procedure of protocol 2 does not change much in the improved proposal, this section does not replicate it in detail. After a successful authentication Alice encodes a random bit

string and her message bits in the c_{QDC} and N restored A-qubits, respectively. She performs a Hadamard operation H_A to encode the bit 0. To send the bit 1 she utilises a Pauli-Z operation followed by a Hadamard operation ($H_A\sigma_{zA}$). Alice sends the encoded A-particles to Trent, who performs Bell measurements on pairs of the A- and the T-qubits. After his x basis measurements Bob extracts Alice's message using table 5.4, a slight modification of the original table 5.1 (p. 47). Alice and Bob complete the second eavesdropping test, proceeding in dialogue form as specified in section 3.3.

Alice's operation	Transformation of GHZ states
H_A (0)	$\frac{1}{2}(\|\Phi\rangle^+_{AT}\|-\rangle_B + \|\Phi\rangle^-_{AT}\|+\rangle_B + \|\Psi\rangle^+_{AT}\|+\rangle_B - \|\Psi\rangle^-_{AT}\|-\rangle_B)$
$H_A\sigma_{zA}$ (1)	$\frac{1}{2}(\|\Phi\rangle^+_{AT}\|+\rangle_B + \|\Phi\rangle^-_{AT}\|-\rangle_B + \|\Psi\rangle^+_{AT}\|-\rangle_B - \|\Psi\rangle^-_{AT}\|+\rangle_B)$

Table 5.4: Expected Results of the Improved Proposal 2
See appendix C.2.2 for a detailed derivation.

5.5.2 Security Analysis

The improved proposal maintains all security properties of the original protocol. The analysed security, discussed in sections 5.3.2 – 5.3.6, remains valid in its result, as the operator combinations of Bell state exponent and x basis result does not change. Nonetheless, appendix G contains a short discussion of the modified calculations and proves that no security result changes – except the result of Trent's eavesdropping.

As section 5.5 and appendix G.1 show, Trent's success probability of active eavesdropping is diminished from 100 % to 0 %. Due to the replacement of Alice's second operation, he cannot distinguish between Alice's operations anymore nor derive a single message bit. Moreover, the detection probabilities remain high, since Trent's intermediate step increases the error rate.

Chapter 6

Authenticated MQDC with ES

This section discusses the protocol *Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping* published by Hong et al. (2006). In this protocol, called protocol 3 in this work, the third party authenticates the users Alice and Bob on the basis of one qubit set for each user. After successful authentication Alice and Bob prepare two new qubit sets and provide Trent with correlated particles. Performing entanglement swapping on these particles, Trent establishes a final basis within the quantum system for the message transfer. On this final basis Alice can send her message to Bob via bitflip positions. Thus, the users do not need a classical channel nor classical cryptographic techniques for the message transmission. The original protocol can be found in appendix B, figure 3 (p. 19) gives an overview of the procedure.

6.1 Authentication

At the request of Alice as the "communication initialiser", Trent prepares an orderly set $|\Theta\rangle$ of $2n$ entangled Bell states $|\theta\rangle$ with

$$
\begin{aligned}
&|\Theta\rangle = |\theta_1\rangle_{T_A A}|\theta_2\rangle_{T_A A}\ldots|\theta_n\rangle_{T_A A}|\theta_{n+1}\rangle_{T_B B}|\theta_{n+2}\rangle_{T_B B}\ldots|\theta_{2n}\rangle_{T_B B} \text{ of}\\
&|\theta_a\rangle_{T_A A} = |\Phi^+\rangle_{T_A A} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_A A} \text{ and}\\
&|\theta_b\rangle_{T_B B} = |\Phi^+\rangle_{T_B B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B}\\
&\text{with } a = 1, 2, \ldots, n \text{ and } b = n+1, n+2, \ldots, 2n\ .
\end{aligned}
\tag{IV}
$$

The subscripts T_A and T_B denote particles which Trent keeps as A- and B-checking sequence, and subscripts A and B indicate particles transmitted to Alice and Bob, called A- and B-authentication sequence, respectively.

Trent encodes the A- and B-authentication sequence, i.e. the A- and B-qubits of each $|\theta_a\rangle_{T_A A}$ or $|\theta_b\rangle_{T_B B}$, with Alice's and Bob's identification numbers ID_A and ID_B, respectively. Thus, here the IDs instead of the authentication keys determine the unitary operations used to encode the particles. Trent uses the same operations as in the previous authentication

method – identity operation for the value 0 and Hadamard operation for the value 1. He sends the encoded A- and B-authentication sequences to Alice and Bob, respectively, and keeps his T_A- and T_B-particles of the A- and B-checking sequences safely. Alice and Bob decode their respective authentication sequence performing the unitary operations defined by their IDs. After the decoding process the original Bell states are restored due to the properties of any unitary operation.

All three parties measure their particles in the z basis and check for the expected correlations in the following first eavesdropping tests. Alice and Bob reveal the results of their entire authentication sequences to Trent. Trent compares these announcements with his checking sequences. If all particles of an authentication sequence are still perfectly correlated with the according checking sequence, Trent authenticates Alice and Bob as legitimate network users. They can continue with direct communication. Furthermore, they can be sure that the channel was secure during the transmission, a point that is not mentioned in the original protocol. In case of a test failure, further communication is aborted and Alice initialises a new communication round.

6.2 QDC

To establish a final basis for direct communication Alice prepares a random sequence of m Bell states of the types $|\Phi^+\rangle_{T_AA}$ and $|\Psi^+\rangle_{T_AA}$ with

$$\begin{aligned}
&|\Theta\rangle_{T_AA} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_m\rangle)_{T_AA} \text{ of} \\
&|\theta_i\rangle_{T_AA} = |\Phi^+\rangle_{T_AA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \text{ and} \\
&|\theta_j\rangle_{T_AA} = |\Psi^+\rangle_{T_AA} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_AA} \\
&\text{for } i \in \mathcal{I} \text{ , } j \in \mathcal{J} \text{ , } \mathcal{I} = \mathcal{J} = \{1, 2, \ldots, m\} \text{ , and } i \neq j
\end{aligned} \tag{V}$$

with the same amount of different types $|\Phi^+\rangle_{T_AA}$ and $|\Psi^+\rangle_{T_AA}(|\mathcal{I}| = |\mathcal{J}|)$, and $m = M + c_{TRANS} + c_{ES}$. M denotes the length of the final message, and c_{TRANS} and c_{ES} represent the number of check qubits in the first eavesdropping test after transmission and in the second eavesdropping test after entanglement swapping, respectively. The original protocol names these check qubits n and q, which is changed here for consistency of the work. Alice keeps the positions of the different types of states secretly. Bob also prepares m Bell states but only of the type $|\Phi^+\rangle_{T_BB}$, i.e.

$$\begin{aligned}
&|\Theta\rangle_{T_BB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_m\rangle)_{T_BB} \text{ of} \\
&|\theta_k\rangle_{T_BB} = |\Phi^+\rangle_{T_BB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \\
&\text{for } k \in \mathcal{K} \text{ and } \mathcal{K} = \{1, 2, \ldots, m\}
\end{aligned} \tag{VI}$$

with $m = M + c_{TRANS} + c_{ES}$. Any subscript indicates the person who works on the particles later on.

Alice forms the so-called A-sequence, consisting of all her T_A-qubits, and transmits it to Trent. Her remaining A-particles are composed in the encoding sequence. Bob also splits his states in a B-sequence of the T_B-particles and a decoding sequence of the B-qubits. He sends Trent the B-sequence. After the transmission of the sequences Alice chooses c_{TRANS} random check positions of her encoding sequence for the first eavesdropping test and tells Trent which positions of the A-sequence he must consider. After measurements in the z basis Trent reveals his results to Alice, who compares her and Trent's outcome. Bob proceeds likewise in a first eavesdropping test with Trent, comparing c_{TRANS} check qubits of his decoding sequence and Trent's B-sequence.

If no eavesdropper is detected in both first tests, Trent projects each pair of qubits, consisting of one qubit of the sorted A-sequence and one particle of the orderly B-sequence, onto the Bell basis. Through this Bell measurement the entanglement between the T_A- and A-particles, and between the T_B- and B-particles swaps to an entanglement between the T_A- and T_B-particles, and between the A- and B-particles. Hence, Trent performs entanglement swapping from T_AA-pairs and T_BB-pairs of the original states to pairs of the encoding and decoding sequence with his Bell measurements of T_AT_B-pairs. Alice, with her encoding sequence, and Bob, with his decoding sequence, now share entangled sequences.

In the original protocol "Trent sends his [Bell] measurement outcomes to Alice" (p. 4), which is interpreted here as Trent's public announcement of the Bell states. Trent reveals his measurement results in the form $|\Omega^{\pm}\rangle_{T_AT_B}$ with $|\Omega\rangle$ referring to $|\Phi\rangle$ or $|\Psi\rangle$. He does not have to distinguish between the different exponents, since the states $|\Omega^{+}\rangle_{T_AT_B}$ and $|\Omega^{-}\rangle_{T_AT_B}$ lead to the same results (see C.3.1 for details).

After the reception of Trent's Bell state Alice and Bob measure their encoding and decoding sequences in the z basis. Alice can derive Bob's measurement outcomes with the help of the additional information about her initial type of Bell state ($|\Phi^{+}\rangle_{T_AA}$ or $|\Psi^{-}\rangle_{T_AA}$), Trent's Bell measurement result ($|\Phi^{\pm}\rangle_{T_AT_B}$ or $|\Psi^{\pm}\rangle_{T_AT_B}$) and her own z-measurement outcome (0 or 1) according to table 6.1 (p. 60). For instance, Alice knows her initial Bell states $|\Phi^{+}\rangle_{T_AA}$ and $|\Psi^{+}\rangle_{T_AA}$ on position 1 and position 2, respectively. Trent announced $|\Psi^{+}\rangle_{T_AT_B}$ on both positions, and Alice measured 0 on position 1 and 1 on position 2, i.e. {0,1}. Hence, she infers that Bob's measurement results is {1,1} (see rows 3 and 8 in tab. 6.1).

In a second eavesdropping test, in which Bob tells Alice his measurement outcome of c_{ES} check qubits of random positions, Alice can check her inferred outcomes of Bob's qubits against his revealed results. If the test fails, communication is aborted. In case of a successful test and, thus, a secure channel, Bob's results represent the final basis for direct communication. Alice sends her message of M bit length to Bob via bitflip positions on this basis. Since she knows Bob's results, she can tell him on which positions he has to flip the bit. With this additional bitflip information Bob can extract and decode Alice's message. Assuming Alice's message is {1,0} and Bob's result is {1,1}, Alice sends the bitflip announcements {0,1} to Bob ({0,1} = {no bitflip,bitflip}). With her announcements Bob can read Alice's message.

Bob's initial state	Alice's initial state	Trent's Bell measurement outcome	Alice's outcome	Bob's outcome
$\|\Phi^+\rangle_{T_BB}$	$\|\Phi^+\rangle_{T_AA}$	$\|\Phi^\pm\rangle_{T_AT_B}$	0	0
			1	1
		$\|\Psi^\pm\rangle_{T_AT_B}$	0	1
			1	0
	$\|\Psi^+\rangle_{T_AA}$	$\|\Phi^\pm\rangle_{T_AT_B}$	0	1
			1	0
		$\|\Psi^\pm\rangle_{T_AT_B}$	0	0
			1	1

Table 6.1: Expected Results of QDC with Entanglement Swapping
Source: (Hong et al., 2006)
See appendix C.3.1 for a detailed derivation.

6.3 Security Analysis

The properties of the Bell state entanglement guarantee the security of the particle transmission. In contrast to the previously discussed protocols, the authentication and the communication are accomplished on separate qubit sets. Only the first set, for authentication, is transmitted encoded. Hence, authentication is not embedded in communication. The non-integrated authentication has serious consequences, which drastically impair the security of the protocol, as the following analysis discloses. The attacker Eve cannot avoid any control procedure of direct communication by leaving the test subsets unattacked, since the check positions are revealed after transmission. But she can avoid the entire authentication procedure of the communication round.

6.3.1 Eavesdropping of Trent

Analysing protocol 3 in terms of Trent's passive eavesdropping shows that no information automatically leaks to him. His task is to perform entanglement swapping, projecting the T_A-qubit and the T_B-particle onto the Bell basis. He cannot leverage the results $|\Phi^\pm\rangle_{T_AT_B}$ or $|\Psi^\pm\rangle_{T_AT_B}$, since he does not know Alice's initial state nor her or Bob's z basis measurement result, which is essential to derive Alice's message bit.

Unfortunately, Trent can eavesdrop actively (see also appendix H.1). As Trent's T_B-particle and Bob's B-qubit are entangled before the entanglement swapping, Trent can force the B-qubit into a fixed state with a measurement of his T_B-particle. Due to their entanglement and Bob's utilisation of only the type $|\Phi^+\rangle_{T_BB}$, the fixed B-particle and the T_B-qubit result in the same measurement outcome. The final message transfer via bitflipping is based on Bob's result. Hence, as Trent can know the final basis, he may obtain the message.

An additional measurement of the T_A-qubit provides Trent with the information which Bell state he must announce to avoid irregularities. He can fake a Bell measurement correctly and imperceptibly, since an exponent distinction of the Bell states is needless in Trent's announcement. Not even the occurrence probabilities of Trent's faked Bell states differ from the expected ones. Trent introduces no errors. His measurement also forces Alice's A-qubit into a fixed state, but Alice measures her particle in the z basis and the collapsed state represents a valid input for a z basis measurement.

Hence, Trent's attack introduces neither errors nor irregularities into the system regarding the expected combinations of Bell states and z basis measurement results. Consequently, Alice and Bob cannot observe Trent's attack in any eavesdropping test and communication proceeds with Alice's public disclosure of the bitflip positions. To learn the entire message Trent only needs to listen in on her announcement of the bitflip positions and flip the bits in the basis received from his T_B-particle. Similar to Trent's attack in protocol 2 (s. 5.3.1), the users never get the chance to recognise that their message completely leaked out, which seriously compromises the security.

6.3.2 Eavesdropping on Authentication

There is no obvious reason for Eve to listen in on the authentication process, since authentication and communication are two separate procedures. She may launch the attack anyway, because the IDs remain valid in every communication round. They are not used to calculate the authentication keys via a hash function, but they are the authentication keys, i.e. $ID = id_1 id_2 ... id_n$ (cf. s. 3.2). Eve may use this long-term valid information in other kinds of attacks or manipulations this work does not discuss. Different from the previous authentication method of protocol 1 and protocol 2, Eve's attack on Alice's and Bob's IDs are exactly equal. Detailed calculations can be found in appendix H.2.

Impersonating the authority, Eve must prepare Bell states by herself. The analysis calculates Eve's option of leaving the qubits unencoded, because it is less complex and leads to the same results like her other option of guessing the encoding information. After Alice's and Bob's decoding and their local measurements both users announce their results to Trent. Eve intercepts the classical links to Trent using these announcements for her attack. She can infer a Hadamard operation, i.e. an identification value of 1, if she measures a different outcome than announced by a user. Hence, her success probability amounts to $\rho_S = 1 - \left(1 - \frac{1}{4}\right)^q$. Eve cannot be detected, if the eavesdropping test proceeds like originally specified. She can always inform the users about a passed authentication test, even if there are irregularities. That means Eve can launch this attack repeatedly until she gains the complete long-term valid user identification. In contrast, a user could detect Eve with the probability of 25 % for every second qubit, if the test proceeded in dialogue form as specified in section 3.3. In the original test procedure Eve could not succeed at all in a user impersonation. Nevertheless, defining a test procedure which covers all attacks with a lower detection probability promises higher security than a procedure which covers only one attack with a higher detection probability.

The other alternative to obtain the ID is to eavesdrop on the transmission during authentication with an intercept-resend or a translucent attack. Eve cannot succeed with an intercept-resend attack, because she measures 0 or 1 with the same probability of $\frac{1}{2}$ for both operations specified by the identification information value. Furthermore, resending the particle to the user, prepared according to her measurement result, introduces errors with the probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^q$.

In a translucent attack Eve can use the unitary operations (A) or (B) to entangle her ancilla with the transmitted particle. Entangling ancilla $|E\rangle_E$ with the unitary operation (A) introduces errors into the system with the probability of $1 - \left(1 - \frac{1}{4} - \frac{\beta^2+\beta'^2}{4}\right)^q$. The entanglement of ancilla $|0\rangle_E$ via the unitary operations (B) increases the error rate with the probability of $1 - \left(1 - \frac{1}{4}\right)^q$.

The authentication procedure in protocol 3 differs from the authentication of the other protocols in the following aspects. First of all, the procedure is not based on the recalculable authentication key but on the long-time valid identification information. Second, the specified checking procedure allows a successful attack against the authentication. In an impersonation of Trent Eve can avoid detection and succeed in the authentication procedure. And third, not only the subset on the scale of c_{AUTH} check qubits is publicly discussed in the test but all qubits necessary to cover an entire ID. The first two aspects represent unnecessary vulnerabilities, whereas the latter cannot be explicitly classified as risky. On the one hand, checking an entire qubit set during the authentication results in higher security, since the detection of an attack is more probable with the same detection probability per check qubit. On the other hand, it leads to the disadvantages that Eve can listen in on the entire ID and that no restoring errors occur in the communication process during impersonation attacks. If this last aspect shall be retained in the protocol, an authentication test proceeding as specified in section 3.3, and the calculation of a renewable authentication key as determined in section 3.2, are absolutely indispensable.

6.3.3 Eavesdropping on QDC

Eve may also use an intercept-resend attack or both translucent attacks to launch an eavesdropping attack on the communication. She attacks this process with the aim to find out Bob's final z basis measurement results. With these results and Alice's public bitflip announcements, Eve can read Alice's message at the end of the communication. Both sequences which are transfered to Trent can be attacked, i.e. the A-sequence and the B-sequence (see H.3 for more details).

Eve does not gain useful information with an intercept-resend attack, because the intercepted qubits are from different sequences of different origin. The whole system is not entangled yet. Furthermore, resending Trent newly prepared particles destroys the entanglement between the intercepted A- and B-sequences and the encoding and decoding sequences. Without its entanglement the system is random and useless for communication and the randomness of its particles might lead to a communication abort in one of the following eavesdropping

tests on the c_{TRANS} or the c_{ES} check qubits.

In a translucent attack, using unitary operation (A) to entangle the ancilla with the T_B-qubits of the B-sequence, Bob and Trent detect Eve in the first eavesdropping test on the c_{TRANS} check qubits with the probability of $\rho_D = 1 - \left(1 - \frac{\beta^2+\beta'^2}{2}\right)^{c_{TRANS}}$. After Trent's entanglement swapping Alice and Bob complete a second eavesdropping test on the c_{ES} check qubits. The previously introduced errors also have an impact and cause detection in this test. The detection probability here amounts to $\rho_D = 1 - \left(1 - \frac{\beta^2+\beta'^2}{2}\right)^{c_{ES}}$. The states causing this detection are erroneous, so it's a moot question whether Eve can succeed to a sufficient degree. The overall detection probability in the communication totals $\rho_D = 1-(1-\beta^2-\beta'^2)^c$ (with $c = c_{TRANS} + c_{ES}$). Entangling ancillas on both sequences which are sent to Trent even increases Eve's detection probabilities with a simultaneous rise of the erroneous states.

A translucent attack with unitary operation (B) leads to totally different results. This attack introduces errors only in combination with a following operation or a x basis measurement of the entangled system (see e.g. s. 4.3.2 or s. 4.3.3, respectively). Thus, Eve's attack does not introduce any errors in protocol 3, and consequently, there is no detection possible in the first nor the second eavesdropping test. With an attack on the B-sequence or on the B-sequence and the A-sequence Eve receives the same results as Bob, since the T_B-particle and the B-qubit coincide. She cannot derive Alice's outcome, since Eve can only attack the T_A-qubit of the A-sequence and these qubits are in the same or the opposite state as the A-qubits depending on Alice's secret initial state. However, Eve succeeds in sufficient degree by simply attacking the B-sequence.

6.3.4 Simple Impersonation Attacks

In the impersonation attacks in protocol 3 Eve does not have to impersonate a user during the entire communication round. She does not need to participate in the authentication process because of the preparation of new qubit sets for direct communication. Actually, she should not disturb this process in order to avoid the introduction of errors and the failure of authentication. An impersonation attack in protocol 3 works even in the case that identification information is necessary to launch the request, because the legitimate users perform the request and the authentication, and fail-safe authentication is very likely. A secret sign included in the message would prevent the sender impersonation, but it could not be used without causing key distribution problems. Eve may consider an imitation of the direct communication with the user she impersonates in order to distract her or him from the interruption of the real communication after authentication is completed.

Assuming that Alice initialises the communication, two different kinds of impersonation attacks are analysed. If Eve's target is to send Bob a fake message, she must impersonate the sender. In case she wants to read Alice's original message to Bob, Eve must impersonate the receiver.

6.3.4.1 Sender Impersonation

Eve starts her impersonation of Alice after she observed Alice's request to the authority and the completion of the authentication procedure. Eve then cuts the public and quantum links between Alice and the network. This intervention must take as long as Eve needs to convince Bob of the message's legitimacy, so Alice cannot alert him.

Preparing settings for direct communication, Eve forms the $E(A)$-sequence for Trent and the encoding sequence for herself from the $M + c_{TRANS} + c_{ES}$ states $|\Phi^+\rangle_{T_{E(A)}E(A)}$ and $|\Psi^+\rangle_{T_{E(A)}E(A)}$. She sends Trent the $E(A)$-sequence consisting of all $T_{E(A)}$-particles. After receiving Eve's and Bob's sequences Trent asks for the c_{TRANS} check qubits for the first eavesdropping test and measures them. Regardless of the procedure form, the test is supposed to pass, since Eve does not introduce any (restoring) errors.

In the case of an undisturbed transmission, Trent projects the qubits of the $E(A)$-sequence and the B-sequence onto the Bell basis and swaps the entanglement to the encoding and the decoding sequence. He then reveals the resultant Bell states and Eve and Bob measure their sequences in the z basis. For the second eavesdropping test Eve asks Bob for the values of the c_{ES} check qubits of her choice. If Bob's announcements correspond with Eve's inference of his values, the second test also passes without detection. Eve knows all of Bob's z basis results according to table 6.1 (p. 60), so that she can reveal her fake message to Bob, telling him the according bitflip positions.

Bob has no chance to detect Eve during the entire communication round, because Alice was correctly authenticated. Eve can completely control the message and send it in the name of Alice. Hence, if Alice is absolutely disconnected from the network, Eve's success totals 100 % with a detection probability of 0 %.

6.3.4.2 Receiver Impersonation

At her observation of Alice's request to Trent, Eve must wait until authentication is completed. After the public discussion and Trent's confirmation of its success Eve cuts the public and quantum channels between Bob and the network. Again, the intervention must last at least until Eve completely received Alice's message, that is until after the transmission of the bitflip positions.

To prepare the setting for direct communication Eve sends Trent her $E(B)$-sequence consisting of the $T_{E(B)}$-qubits of her prepared $M + c_{TRANS} + c_{ES}$ Bell states of type $|\Phi^+\rangle_{T_{E(B)}E(B)}$. Eve and Alice independently choose c_{TRANS} check positions of their encoding and decoding sequences, measure them in the z basis and compare them with Trent's measurement results. Eve is suppose to pass this first eavesdropping test without any problems.

After performing entanglement swapping Trent reveals the resultant Bell states, and Eve and Alice share entangled sequences. They measure all particles in the z basis, and Eve tells Alice the values of the c_{ES} check qubit, which Alice chose. Again, Eve is expected to pass the second eavesdropping test.

Alice can deduce Eve's measurement outcomes according to table 6.1 (p. 60), but she cannot derive Eve's existence from it. Alice sends Eve the bitflip positions and, therewith, the message. Again, the unembedded authentication and the lack of any restoring problem lead to full success on Eve's side with no detection at all.

6.3.5 Advanced Impersonation Attacks

There is no need for Eve to try a more complex, advanced impersonation attack, because she already succeeds with the simple impersonations. The only reasons to impersonate Trent is an eavesdropping attack on the authentication (s. 6.3.2) or an attempt to simplify the man-in-the-middle attack (s. 6.3.6).

6.3.6 Man-in-the-middle Attack

Combining both simple impersonation attacks in a man-in-the-middle attack Eve can fully control the communication. She can read Alice's message and simultaneously transmit her own message to Bob. No party has a reason to alert the other party, because both are convinced that they communicate with each other, because of the passed authentication with Trent. Additionally, Eve can forge an included sign without problems.

After observing Alice's request Eve awaits the authentication procedure. Trent authenticates the legitimate parties to each other, so the authentication is fail-safe. In the direct communication Eve must accomplish all communication tasks twice. She prepares two $M + c_{TRANS} + c_{ES}$ qubit sets. The first set used to impersonate the receiver contains Bell states of the type $|\Phi^+\rangle_{T_{E(B)}E(B)}$. The second set for the impersonation of the sender consists of both types of Bell states $|\Phi^+\rangle_{T_{E(A)}E(A)}$ and $|\Psi^+\rangle_{T_{E(A)}E(A)}$.

Now the attack gets technically challenging. Eve and Bob send Trent the $E(B)$- and B-sequences, respectively. As Eve needs the B-sequence in the second part of the attack to resend Bob Alice's modified message, she must somehow explain to Trent why the B-sequence arrives divided into two parts. The same can be applied to the A-sequence, which arrives subdivided into the real A-sequence and the $E(A)$-sequence. Furthermore, Eve must consider the correct order of the sequences' arrival at Trent's. If Eve manages this tasks, Trent coalesces the sequences as

$$|\Omega^+\rangle_{T_AA} \ldots |\Omega^+\rangle_{T_{E(A)}E(A)} \quad \text{and} \quad |\Omega^+\rangle_{T_{E(B)}E(B)} \ldots |\Omega^+\rangle_{T_BB}$$

with only $|\Omega^+\rangle_{T_AA}$ and $|\Omega^+\rangle_{T_{E(A)}E(A)}$ consisting of $|\Phi^+\rangle_{T_AA}$ and $|\Phi^+\rangle_{T_{E(A)}E(A)}$, and $|\Psi^+\rangle_{T_AA}$ and $|\Psi^+\rangle_{T_{E(A)}E(A)}$. Hence, Trent's A- and B-sequences are in the following form:

$$\begin{array}{ccccccc} < & \text{A-sequence} & | & \text{E(A)-sequence} & > & \text{and} \\ < & \text{E(B)-sequence} & | & \text{B-sequence} & > \end{array}$$

After the arrival of all four sequences at Trent's Eve must intercept Alice's and Bob's announcements of the c_{TRANS} check positions, adapt them and pool them with her own

positions in the right order. For instance, Eve must increase Bob's check positions by the length $M + c_{TRANS} + c_{ES}$ of her $E(B)$-sequence at the head. Eve tells Trent the adapted check positions and transfers his z basis measurement results to Alice or Bob. If she accurately recalculates the positions, Eve is not detected in this first eavesdropping test.

After the test Trent projects each pair of qubits onto the Bell basis. Through this Bell measurement the entanglement swaps between particles T_A and A, T_B and B, $T_{E(A)}$ and $E(A)$, and $T_{E(B)}$ and $E(B)$ to the qubits A and $E(B)$, and $E(A)$ and B. Alice's encoding sequence is entangled with Eve's decoding sequence, and Eve's encoding sequence is entangled with Bob's decoding sequence.

Trent reveals his measurement results, which Eve again must intercept, correctly divide, and resend to the respective user. After reception Alice, Bob, and Eve measure their encoding and/or decoding sequences in the z basis. Finally, Alice can derive the measurement outcomes of Eve (alias Bob), and Eve can derive Bob's results (cf. tab. 6.2). Again, Eve avoids detection in the second eavesdropping tests between Alice and her, and between her and Bob, if she correctly recalculates the c_{ES} check positions. With the interception of Alice's announcement of the bitflip positions Eve can decode Alice's message on the first set. Eve then resends a modified message to Bob, telling him the according bitflip positions for the second set.

First set				
Eve's state	Alice's state	Trent's Bell state	Alice's outcome (encoding seq.)	Eve's outcome (decoding seq.)
$\|\Phi^+\rangle_{T_{E(B)}E(B)}$	$\|\Phi^+\rangle_{T_AA}$	$\|\Phi^\pm\rangle_{T_AT_{E(B)}}$	0	0
			1	1
		$\|\Psi^\pm\rangle_{T_AT_{E(B)}}$	0	1
			1	0
	$\|\Psi^+\rangle_{T_AA}$	$\|\Phi^\pm\rangle_{T_AT_{E(B)}}$	0	1
			1	0
		$\|\Psi^\pm\rangle_{T_AT_{E(B)}}$	0	0
			1	1
Second set				
Bob's state	Eve's state	Trent's Bell state	Eve's outcome (encoding seq.)	Bob's outcome (decoding seq.)
$\|\Phi^+\rangle_{T_BB}$	$\|\Phi^+\rangle_{T_{E(A)}E(A)}$	$\|\Phi^\pm\rangle_{T_{E(A)}T_B}$	0	0
			1	1
		$\|\Psi^\pm\rangle_{T_{E(A)}T_B}$	0	1
			1	0
	$\|\Psi^+\rangle_{T_{E(A)}E(A)}$	$\|\Phi^\pm\rangle_{T_{E(A)}T_B}$	0	1
			1	0
		$\|\Psi^\pm\rangle_{T_{E(A)}T_B}$	0	0
			1	1

Table 6.2: Results of QDC in a Man-in-the-middle Attack

To simplify the attack Eve may consider an additional impersonation of Trent. She can therewith circumvent the sophisticated problem of the arrival of the sequences in several parts and their correct configuration. An impersonation of Trent does not raise the probability of her detection. Her only additional task is the preparation of Bell states $|\Phi^+\rangle_{T_A A}$ and $|\Phi^+\rangle_{T_B B}$ for authentication. Eve can send Alice and Bob the unencoded A- and B-particles without any problems. In fact, the users' decoding of the unencoded particles leads to restoring errors, but since the eavesdropping test is not a dialogue, Eve just (mis)informs both users about a passed authentication. After the successful authentication Eve receives Alice's and Bob's A- and B-sequences, which she entangles with her own $E(B)$- and $E(A)$-sequences, respectively. The further procedure can be derived according to the description in the preceding paragraphs.

Concluding this successful man-in-the-middle attack, Eve can avoid the authentication, and she is not detected at all during any eavesdropping test as a consequence of the unembedded authentication process. Moreover, Eve is in the position to completely control the message between Alice and Bob as the man-in-the-middle.

6.4 Suggestions for Improvements

The transmission of the particles during authentication and communication is protected by their entanglement. In the communication process the second eavesdropping test after Trent's entanglement swapping offers additional security with the potential to increase the detection probability, e.g. in the first translucent attack in section 6.3.3. In contrast to protocol 2, Alice does not reveal the message until the security of the transmission is confirmed. The final basis represents random and worthless information without her bitflip positions. Moreover, the protocol can also be used for QKD, since the final results are perfectly random. The key bits are not proposed by any user, but are random in their existence. Due to this trait, the original protocol 3 features an unchallengeable benefit.

The security analysis of protocol 3 is only discussed briefly in the original paper. The authors refer to the similarity of the BBM92 protocol (Bennett et al., 1992b), since the "qubit transmission and the checking method in our protocol is similar to the procedure in BBM92 QKD protocol" (p. 5). Thus, they conclude that the unconditional security of the BBM92 protocol applies to their protocol. Indeed, the transmission is unconditionally secure in both protocols, due to the fact that each transmitted qubit is entangled with a qubit, which is kept safely. However, the BBM92 protocol was not published in the context of authentication, nor was it analysed in terms of an authenticated multiuser network. The BBM92 security analyses, which protocol 3 refers to, focus on the unconditionally secure transmission procedure. Relying on an unconditionally secure transmission does not suffice for unconditional security in case of an "authenticated multiuser QDC scheme" (p. 2) as protocol 3.

The authentication process is not embedded within direct communication, which turns out to be a security vulnerability entailing severe consequences. The possibility of successful impersonation attacks, culminating in the feasibility of the man-in-the-middle attack, without

the need of the attacker to authenticate herself may be the most concerning fact (sections 6.3.4 – 6.3.6). Eve can leave the authentication process between the legitimate users undisturbed in order to avoid errors. She does not join the direct communication on the newly prepared qubit sets until the authentication is over. Thus, even an identification information to notify a request to Trent is not a remedy. A secret sign, included in the message, could prevent the first simple impersonation attack, but would produce key distribution problems as well. Furthermore, an included sign would not hamper a man-in-the-middle attack.

There is an appropriate allegory of the gap between authentication and communication, in which Trent is not involved because of simplicity. Alice and Bob authenticate each other over the phone by revealing secret information, which is only known to the legitimate parties. After authentication Alice dials Bob's number again for a second telephone conversation, in which she tells a secret message to the person who answers the phone. This procedure does not warrant the authentication, since the person at the other end of the line may be anybody.

The fact that Bob only uses states of the type $|\Phi^+\rangle_{T_BB}$ makes Trent's active eavesdropping and Eve's second translucent attack with unitary operation (B) on the direct communication process possible (sections 6.3.1 and 6.3.3). Although Alice does also not detect Eve's attack against her qubits, Eve cannot deduce her final measurement results, due to Alice's use of different states. Thus, Bob's exclusive state discloses his final result.

The authentication is based on the utilisation of the IDs as authentication keys, that is $ID = id_1id_2...id_n$ (s. 6.3.2). In protocol 1 and protocol 2 the authentication keys are recalculated for any new communication round via the one-way hash function, i.e. $h(ID, c) = id_1id_2...id_n$. The regeneration of the nonreversible hash function adds security on a large scale, because listening in on the authentication process does not lead to an information gain, which would be valid for future communication. Hence, the authentication in protocol 3 should be based on a recalculated authentication key, especially in case of the perpetuation of the publicly discussed c_{AUTH} check qubits which cover the entire length of the ID. In this case the significant decrease of the overall detection probability in most attacks must also be considered, since the communication phase does not inherit any restoring errors.

The specification of the test procedure in the original paper contains some risks. The eavesdropping test during authentication proceeds with Alice's and Bob's announcements to Trent and his comparison after measuring all qubits in the z basis ("Then she (he) measures her (his) sequence in the σ_z [z] basis, and announces the outcomes.", p. 3). The manipulation opportunities that come with the assumption of his righteousness represent a serious caveat of the procedure. An impersonation of the authority instantly generates a scenario, in which Eve cannot be detected when she listens in on the IDs (s. 6.3.2) or launches an advanced man-in-the-middle attack (s. 6.3.6).

As already discussed in section 6.3.2, a test dialogue according to section 3.3 constitutes a disadvantage in Eve's impersonation of a user. In the original test Eve cannot derive any key value without Trent's feedback. In a dialogue she may gather some key bits from Trent's announcements. However, higher security follows from the definition of a procedure that covers all attacks with a lower detection probability, rather than covering only one attack

with a higher detection probability. The dialogue form offers a sufficient detection probability of $1 - \left(1 - \frac{1}{4}\right)^c$ (with $c = q/2$), and Eve's partial knowledge of the authentication key does not help her, if it is one-time valid.

The first and the second eavesdropping test during the communication is similarly defined as Alice's and Bob's comparison of Trent's results or Alice's comparison of Bob's results, respectively. Again, a dialogue form allocates power to all involved parties in equal parts, although Eve still cannot be detected during an impersonation attack, because she does not introduce any errors. This position does not warrant the test specification, though. In the second test Alice must tell Bob her initial Bell state in addition to her measurement result any time she makes the first announcement.

The authors of protocol 3 already realised "some weakness including authentication process" and will publish a new version (Lee, 2006). The following section discusses improvements that leave the special core of protocol 3 unaltered.

6.5 Improved Proposals

Regarding the prevention of successful impersonation or man-in-the-middle attacks, two self-developed protocols are proposed. They are modelled on the embedded authentication of protocol 1 and protocol 2, but the characteristic of the original protocol 3 – the use of bipartite Bell states, the entanglement swapping, and the late revelation of the message – is maintained. Since the authentication process is based on the authentication keys, calculated by the one-way hash function, the long-time validity of eavesdropped authentication information is circumvented. For the purpose of QKD the revelation of the message bits via bitflip announcements can be omitted in order to distribute a perfectly random key secretly between the communication parties. The transmission of any particle remains protected by entanglement, so it is unconditionally secure. All eavesdropping tests proceed in dialogue form, as discussed in section 3.3, to avoid the relocation of power to one party and to ensure the possibility of detection in any attack. Short security analyses for both proposals can be found in the respective sections and in appendices I and J.

The improved proposal 3 is supposed to reconfigure the original protocol as congeneric as possible in line with the most essential security requirements demanded in section 6.4 (see s. 6.5.1). The specification of the authentication check qubits is maintained, that is they consists not only of a subset but of all qubits necessary to cover the entire ID. The trade-off between a higher detection probability with the same detection probability per check qubit and a higher information gain for Eve is maintainable, if the authentication key is recalculated for any new communication round. Furthermore, as no restoring problems occur, the eavesdropping test during authentication must be applied very conscientious. The proximate circumvention of Bob's exclusive use of state $|\Phi^+\rangle_{T_B B}$, and therefore, the elimination of Trent's active eavesdropping is not possible without leaving the setup of protocol 3. Eve's success probability of eavesdropping on the communication is reduced by the detection probability during authentication.

In the improved proposal 4 the original protocol is completely remodelled (see s. 6.5.2). It prevents Trent's and Eve's attacks, and additionally provides the feature of bidirectional communication. This way Alice sends Bob her message, and Bob can coevally transmit his respond to Alice without initialising a new communication round.

The authentication of the public discussion during the eavesdropping tests offers an alternative to the embedded authentication of the proposals (see also s. 2.2.3). An authenticated public discussions protects the direct communication of protocol 3 or any other QDC or QKD method against impersonations or man-in-the-middle attacks. The communication parties must therefor share a secret binary string, which originally caused key distribution problems. Approaches how to use this string in public discussion have been published, e.g. in Dušek et al. (1999).

To avoid key distribution problems an intermediate step can be introduced in the original protocol 3. In this intermediate step Trent provides Alice and Bob with a secret, shared binary string, the so called joint key. The idea of distributing an identification key goes back to Zeng and Zhang (2000). In the following, the joint key is modelled by using elements of the protocol. The authentication proceeds as in the original protocol including the difference that only a subset on the scale of c_{AUTH} is used to check for eavesdropping after Alice and Bob have decoded and restored their authentication sequences of length n (with $n = c_{AUTH} + J$). After successful authentication Trent projects the untested J particles of each sequence onto the Bell basis. Through this entanglement swapping the qubits of the A-authentication sequence in Alice's possession become entangled with the qubits of the B-authentication sequence in Bob's hand. Alice and Bob measure their sequences in the z basis, and Trent publishes his resultant Bell states. With these results Alice and Bob can derive each others outcomes according to the first four rows of table 6.1 (p. 60). A following eavesdropping test is optional, because no particles were transmitted after the first test. If this optional test is desired, Alice and Bob compare a randomly chosen subset of their measurement results. The remaining untested qubits form the shared, secret joint key of length $\leq J$. Alice and Bob then proceed with direct communication, as specified in protocol 3. They authenticate their public discussions within the communication process with the use of the secret joint key.

Eve cannot succeed in any impersonation or man-in-the-middle attack during the authentication phase, because she lacks the respective authentication key necessary to prove her legitimacy. The key is also essential to the correct restoration of the particles, which form the joint key later. Furthermore, Eve cannot be successful in these attacks during the direct communication phase, since she does not know the correct joint key for the public discussion. Hence, interlacing a joint key arrangement in the original protocol 3 prevents impersonations and the man-in-the-middle attack. Nevertheless, since the communication process is maintained unmodified, the success of Trent's active eavesdropping attack and Eve's translucent attack is not limited at all.

6.5.1 Improved Proposal 3

Proposal 3 was developed by integrating the authentication into communication, that is by using only one qubit set for both processes. The handling of the qubits is very similar to the original protocol, except that the three parties must now complete different tasks (cf. fig. 5, p. 72).

6.5.1.1 Protocol

Instead of Trent, Alice and Bob prepare Bell states for authentication. Alice prepares a set $|\Theta\rangle_{T_AA}$ of $n+m$ Bell states $|\theta\rangle_{T_AA}$ with

$$\begin{aligned}
&|\Theta\rangle_{T_AA} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_{n+m}\rangle)_{T_AA} \text{ of} \\
&|\theta_i\rangle_{T_AA} = |\Phi^+\rangle_{T_AA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \text{ and} \\
&|\theta_j\rangle_{T_AA} = |\Psi^+\rangle_{T_AA} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_AA} \\
&\text{for } i = 1, 2, \ldots, n \text{ and } j = 1, 2, \ldots, m \text{ with } i \neq j \ .
\end{aligned} \tag{VII}$$

The amount n of states $|\Phi^+\rangle_{T_AA}$ consists of $c_{AUTH} + \frac{1}{2}\ c_{ES} + N$, where c_{AUTH} covers the entire length of her authentication key, i.e. $c_{AUTH} = |h_A(ID_A, c_A)|$. The amount m of states $|\Psi^+\rangle_{T_AA}$ equals $\frac{1}{2}\ c_{ES} + M$. N and M are of the same size ($N = M$). Alice encodes her authentication key in c_{AUTH} T_A-particles of states $|\Phi^+\rangle_{T_AA}$ on random positions and forms a random orderly sequence of all her $c_{AUTH}+c_{ES}+N+M$ Bell states $|\Phi^+\rangle_{T_AA}$ and $|\Psi^+\rangle_{T_AA}$. She keeps the information about this arrangement as well as the positions of the c_{AUTH} encoded qubits secretly.

Bob only prepares $p = c_{AUTH} + c_{ES} + N + M$ Bell states of the type $|\Phi^+\rangle_{T_BB}$, i.e.

$$\begin{aligned}
&|\Theta\rangle_{T_BB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_p\rangle)_{T_BB} \text{ of} \\
&|\theta_i\rangle_{T_BB} = |\Phi^+\rangle_{T_BB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \text{ for } i = 1, 2, \ldots, p \ .
\end{aligned} \tag{VIII}$$

He encodes his authentication key in the T_B-particles of an arbitrary subset on the scale of c_{AUTH}, which covers the length of the key. He also randomly merges his c_{AUTH} encoded qubits in the T_B-sequence of his entire set and stores the information about the positions of the encoded qubits secretly. The T_A- or T_B-qubits represent the A- or B-sequences, respectively. The sequences of the remaining A- and B-qubits are named encoding and decoding sequence.

Alice and Bob send their prepared A- and B-sequences to Trent. After the transmission they reveal the positions of their c_{AUTH} encoded qubits to him. Trent decodes the qubits of the published positions with the users' authentication keys and performs z basis measurement on them. Alice and Bob also measure the respective particles in their sequences in the z basis. The other qubits remain untouched.

In the following first eavesdropping test Alice and Trent compare their measurement results of all c_{AUTH} check qubits in dialogue form as specified in section 3.3. If all A- and T_A-particles are still perfectly correlated, they both know that the particles were encoded and decoded correctly, and the channel was secure during the transmission. Hence, Alice is authenticated by Trent. Bob and Trent proceed accordingly with the c_{AUTH} B- and T_B-qubits. If Trent legitimises both users, they can continue with quantum direct communication. Otherwise, the authentication fails and communication is aborted.

In case of successful authentication, direct communication proceeds like in the original protocol. Trent measures each pair of his A- and B-sequences in the Bell basis, that is to say, he performs entanglement swapping. Therefore, not only both of these sequences become entangled but also the encoding and decoding sequences in Alice's and Bob's possession. Trent publicly announces his results $|\Phi^{\pm}\rangle_{T_A T_B}$ or $|\Psi^{\pm}\rangle_{T_A T_B}$. After receiving his outcomes Alice and Bob measure their encoding and decoding sequences in the z basis.

Alice derives Bob's measurement outcomes according to table 6.1 (p. 60) with the information of her initial Bell states, Trent's Bell states, and her z-measurement results. In the following eavesdropping test Alice and Bob check their measurement outcomes of c_{ES} qubits of random positions. They abort the communication, if the test fails. If this is not the case, Alice sends her message via bitflip positions, and Bob can decode and read it.

(A1) Alice and Bob prepare Bell states for authentication. Alice prepares the types $|\Phi^+\rangle_{T_A A}$ and $|\Psi^+\rangle_{T_A A}$, whereas Bob only prepares states of the form $|\Phi^+\rangle_{T_B B}$. The T_A- or T_B-qubits represent the A- or B-sequences, respectively, and the sequences of the A- and B-qubits are named encoding and decoding sequence.

(A2) Both users encode their respective authentication key in the T_A- or T_B-particles of a control subset, which covers the length of the key. The A- and B-sequences are then transmitted to Trent.

(A3) All three parties complete the authentication test. Alice reveals the positions of her encoded check qubits to Trent. After decoding the qubits with her authentication key Trent measures them in the z basis and compares the results with Alice. Bob proceeds accordingly with Trent. If the tests are successful, the users are authenticated. Otherwise, the protocol is aborted.

(C1) QDC proceeds as in the original protocol. Trent performs entanglement swapping by projecting his A- and B-sequences onto the Bell basis, and announces his measurement outcomes.

(C2) Both users measure their encoding and decoding sequences in the z basis. The final basis for the message transfer is established, since Alice can derive Bob's measurement outcomes.

(C3) Alice and Bob complete the second eavesdropping test by comparing random positions of the final basis. They abort the communication, if the test fails.

(C4) Alice sends her message via bitflip positions at the final basis to Bob. With the additional bitflip information Bob can extract and decode Alice's message.

Figure 5: Improved Proposal 3 of Authenticated MQDC with ES
The enumeration letters A and C denote the authentication and communication process, respectively.

6.5.1.2 Security analysis

As the improvement has no impact on Trent's eavesdropping attack, Trent can still know Bob's B-qubit by measuring his entangled T_B-particle of Bob's exclusive state $|\Phi^+\rangle_{T_B B}$ (see 6.3.1 for the details). Trent introduces no errors and there are no irregularities in the expected

final system. Alice and Bob have no chance to recognise the attack and the communication is not aborted before Alice's bitflip announcements. Hence, the entire message leaks to Trent, which remains a security risk.

Eve's eavesdropping on the authentication does not change significantly, since only the tasks in the authentication process are switched and not the core of the authentication. In proposal 3 the users instead of Trent encode the T_U-particles with her/his authentication key and transmit it to Trent. Eve must intercept these qubits in an impersonation of Trent or an intercept-resend attack. The detection as well as the success probabilities remain as in the original protocol, that is 25 % detection probability and 25 % or 0 % success probability, respectively. Unlike in the original protocol, the detection probability in an impersonation of Trent is calculated for every second check qubit due to the dialogue form of the test, i.e. $\rho_D = 1 - (1 - \frac{1}{4})^{c_1}$ (with $c_1 = c_{AUTH}/2$). The detection probabilities in a translucent attack on the T_U-particle also do not change, although the derivation must be slightly modified due to Eve's entanglement of her ancilla on a different particle of the entire system. The detection probability is at least 25 % per check qubit. Again, Eve may find out some bits of the key, since the c_{AUTH} check qubits cover the entire length of the authentication key. But simultaneously, she cannot take advantage of the short-time valid information in another communication round this time.

Compared with the original protocol, there are two differences in the security of the authentication process. Since Eve must listen in on the entire transmitted qubit set, the error rate increases during communication. And second, the authentication test is realised as a dialogue, so Eve cannot avoid detection in any attack nor conceal her introduced errors to the users.

Eve still is not successful with an intercept-resend attack when she eavesdrops on the direct communication process. The only qubits she can attack are the A- and B-sequences of different origin. The entire system is not entangled yet, and her interception destroys the entanglement between the transmitted sequences and the coding sequences.

In both translucent attacks the immediate detection probabilities, which occur during communication, must be enlarged with the detection probabilities during authentication, even if Eve wants to eavesdrop only on the communication process. Eve must attack the T_B-qubits of the B-sequence during its transmission to Trent, that is in between Bob's encoding and Trent's decoding operations. The sequence consists of the unencoded qubits for communication and the encoded particles for authentication. Eve cannot know the positions of the c_{AUTH} authentication qubits at the time of the transmission, so that she unintentionally introduces errors (see I.3).

In an attack with unitary operation (A) the detection probability is $\rho_{D_{AUTH}} = \frac{1}{4} + \frac{\beta^2+\beta'^2}{4}$ per check qubit during authentication and remains $\rho_{D_{ES}} = \beta^2 + \beta'^2$ per check qubit during communication. In a translucent attack with unitary operation (B) the security risk of full information gain with no detection is theoretically confined. Bob's exclusive use of states $|\Phi^+\rangle_{T_BB}$ is not changed in the proposal. Thus, there still may be full information gain after the entanglement swapping. But as already discussed, the unitary operation (B) introduces

errors after a subsequent operation (or a x basis measurement) on the entire entangled system. As this is the case in the authentication and Eve cannot avoid the process, the integration of authentication leads to an overall detection probability of $1 - \left(1 - \frac{1}{4}\right)^{c_{AUTH}}$. This detection probability already occurs in the first eavesdropping test, and the communication is very likely aborted. Hence, Eve does not reach the communication stage, in which she could use her information about Bob's final result for the first time.

In contrast to the original protocol, Eve needs to participate in the authentication process in a simple impersonation attack. Due to her lack of the respective authentication key, she introduces restoring errors which Trent can detect with the probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) after his decoding (see I.4 for a detailed calculation). Considering that all c_{AUTH} $|\Phi^+\rangle_{T_U U}$ are checked in this first eavesdropping test, the probability to detect Eve's attack is very high. Hence, Trent must abort the communication. Otherwise, the direct communication would proceed like described in section 6.5.1. There are no restoring errors, whose impact unexpectedly transforms the system or cause detection in the second eavesdropping test, due to the fact that the communication does not operate with restored particles. Thus, Eve could control the message. But, to point it out again, the security of this kind of authentication relies on the high detection probability for a given detection probability per check qubit.

The same holds for any advanced impersonation attack. The additional impersonation of Trent is not more advantageous for Eve. Her barrier is the authentication procedure, because she does not possess the authentication keys. The respective legitimate user detects Eve's impersonation of Trent with the probability of $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) in the first eavesdropping test. Even though Trent's position is auspicious to eavesdrop on Bob's final result, Eve cannot get in his position. For this reason an advanced impersonation attack does not benefit Eve, because there is no difference to a simple impersonation attack.

The addressed barrier to a successful impersonation attack also withstands a man-in-the-middle attack as a combination of both simple impersonations. Eve introduces restoring errors during the authentication, and she cannot reach the communication stage without participating in the authentication. The respective legitimate party detects her attack with the probability of $1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$). Hence, Eve is detected with the probability of 25 % per qubit on both subsets of c_{AUTH} length. In contrast to the original protocol, a man-in-the-middle attack is infeasible for Eve.

The elimination of the most serious security vulnerabilities of the original protocol may add security to a sufficient degree. An eavesdropping attack on the communication and all kinds of simple and advanced impersonation attacks as well as the man-in-the-middle attack are excluded in the improved proposal 3. However, Trent's possibility of active eavesdropping remains a security risk.

6.5.2 Improved Proposal 4

Proposal 4 was developed with the intension to add the feature of bidirectional communication to a quantum direct communication scheme with embedded authentication. Additionally, it comprises a solution to prevent Trent's and Eve's eavesdropping attacks. Despite these additional features, the scheme is simpler and less extensive than the original protocol and the improved proposal 3(cf. fig. 6, p. 77).

There are two final communication bases known to both users. Hence, not only Alice is able to send her message to Bob, but Bob can also send his respond back to Alice without initialising an extra communication round. Moreover, the potential message length is reduplicated because of the resultant two bases, which the users utilise for message transmission. Hence, the expenditure of time and medium highly decreases.

The specification of the c_{AUTH} check qubits during authentication is the same as in protocol 1 and protocol 2, that is the authentication key is encoded in all particles, but only a subset thereof is publicly checked. Thus, the benefits resulting from the restoring errors are retrieved. Eve must face higher overall detection probabilities and derivation problems, which lead to the decline or impossibility of controlling any message bit.

6.5.2.1 Protocol

At the request of Alice as the "communication initialiser", Trent prepares a set $|\Theta\rangle$ for each user of n bipartite entangled states $|\theta\rangle$ with

$$
\begin{aligned}
&|\Theta\rangle_{T_AA} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_n\rangle)_{T_AA} \text{ of} \\
&|\theta_i\rangle_{T_AA} = |\Phi^+\rangle_{T_AA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \text{ and} \\
&|\Theta\rangle_{T_BB} = (|\theta_1\rangle|\theta_2\rangle \ldots |\theta_n\rangle)_{T_BB} \text{ of} \\
&|\theta_i\rangle_{T_BB} = |\Phi^+\rangle_{T_BB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \text{ with } i = 1, 2, \ldots, n \ .
\end{aligned}
\tag{IX}
$$

The subscripts denote the user who works on the qubits later on. The amount n consists of $N + c_{AUTH} + c_{ES}$. N represents the length of each final basis, and c_{AUTH} and c_{ES} are the amounts of check qubits during authentication and after entanglement swapping, respectively.

Trent encodes Alice's and Bob's authentication keys in the A- and B-particles of each state $|\theta_i\rangle_{T_AA}$ and $|\theta_i\rangle_{T_BB}$, respectively. These encoded qubits form the A- and B-sequences and are transmitted to the respective user. The remaining unencoded T_A- and T_B-particles are combined in the A- and B-working sequences, which Trent keeps in a safe place.

After the reception of their sequences Alice and Bob decode all particles according to their authentication keys, so the qubits are restored to their original state. In a first eavesdropping test Alice and Trent agree on c_{AUTH} check qubits of the A-sequence and the A-working-sequence, which they measure in the z basis. They compare their results in dialogue form (s. 3.3). Bob and Trent proceed equally with the B-sequence and the B-working sequence. In the case of correlation errors in one of the tests, communication is aborted. If the compared

particles are still perfectly correlated, all parties are ensured of an undisturbed transmission. Moreover, Alice and Bob are authenticated as legitimate network user via Trent and can proceed with direct communication.

In case of an eavesdropping-free transmission, Trent projects each pair, consisting of one qubit of the orderly A-working sequence and one of the sorted B-working sequence, onto the Bell basis. Due to this entanglement swapping, Alice's A-sequence and Bob's B-sequence become entangled. Trent announces the resultant Bell state of the form $|\Omega^+\rangle_{T_AT_B}$ or $|\Omega^-\rangle_{T_AT_B}$ with exactly defined exponents and $|\Omega\rangle$ denoting $|\Phi\rangle$ or $|\Psi\rangle$. After Trent's entanglement swapping Alice and Bob independently measure their sequences in the x basis. After all measurements both users can derive each others x basis results according to table 6.3.

Trent's Bell state	Result of Alice	Result of Bob	Final basis of Alice	Final basis of Bob
$\|\Phi^+\rangle_{T_AT_B}$	$\|+\rangle_A$	$\|+\rangle_B$	0	0
$\|\Psi^+\rangle_{T_AT_B}$	$\|+\rangle_A$	$\|+\rangle_B$	0	0
$\|\Phi^-\rangle_{T_AT_B}$	$\|-\rangle_A$	$\|+\rangle_B$	1	0
$\|\Psi^-\rangle_{T_AT_B}$	$\|-\rangle_A$	$\|+\rangle_B$	1	0
$\|\Phi^-\rangle_{T_AT_B}$	$\|+\rangle_A$	$\|-\rangle_B$	0	1
$\|\Psi^-\rangle_{T_AT_B}$	$\|+\rangle_A$	$\|-\rangle_B$	0	1
$\|\Phi^+\rangle_{T_AT_B}$	$\|-\rangle_A$	$\|-\rangle_B$	1	1
$\|\Psi^+\rangle_{T_AT_B}$	$\|-\rangle_A$	$\|-\rangle_B$	1	1

Table 6.3: Expected Results of Two-Way QDC in the Improved Proposal 4
For a detailed derivation see appendix C.3.2.

A second eavesdropping test is optional. On the one hand, no particles are transmitted after the first eavesdropping test, so Eve could not attack the system after the first test. On the other hand, an additional eavesdropping test offers higher overall detection probability. According to their security preferences, the communication parties may proceed with an optional second eavesdropping test.

If an additional test is desired, Alice and Bob compare a randomly chosen subset on the scale of c_{ES} check qubits in dialogue form (s. 3.3). If all check qubits show the expected values, Alice and Bob publicly agree on a state-to-binary translation of their x basis measurement results. For instance, the result $|+\rangle$ represents 0, whereas $|-\rangle$ is translated to 1. Alice and Bob now send their messages to each other, which consist of maximally $2N$ bits in total. Bitflip announcements are used to communicate, i.e. to keep or flip the bits of the bases according to the message.

(A1) At Alice's request, Trent prepares a set of Bell states with $|\Phi^+\rangle_{T_A A} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_A A}$ or $|\Phi^+\rangle_{T_B B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B}$ for each user. He encodes Alice's and Bob's authentication keys in the A- and B-particles of each state, respectively, and transmits the encoded qubits as A- and B-sequences to the users. The T_A- and T_B-particles represent the A- and B-working sequences, which Trent keeps in a safe place.

(A2) Alice and Bob decode their sequences with their respective authentication key. Hence, all qubits are restored to their original state.

(A3) All three parties complete the mandatory eavesdropping test. Alice and Trent compare a subset of check qubits of the A-sequence and the A-working sequence after measurements in the z basis. Bob proceeds accordingly with Trent. If the tests are successful, the users are authenticated.

(C1) To establish the final bases for the message transfer Trent projects both working sequences onto the Bell basis and announces the measurement outcomes. Alice and Bob measure their A- and B-sequences in the x basis.

(C2) After all measurements both users can derive each others x basis results. Thus, they share two final bases of secret values. Another eavesdropping test is optional.

(C3) Alice and Bob send their messages to each other via bitflip announcements for the values of a final basis.

Figure 6: Improved Proposal 4 of Authenticated Bidirectional MQDC with ES
The enumeration letters A and C denote the authentication and communication process, respectively.

6.5.2.2 Security analysis

The modified procedure provides the proposal with additional security to the effect that all discussed attacks are prevented either by high detection probability or by infeasibility. The modification of the measurement basis from the z basis to the x basis substantially reduces the risk of exclusively utilising states of the type $|\Phi^+\rangle_{T_A A}$ and $|\Phi^+\rangle_{T_B B}$. In contrast to the original protocol 3 and the improved proposal 3, Trent cannot be successful in an active eavesdropping attack. If Trent fakes the Bell measurement, measuring the users' particle in the z basis instead of the Bell basis and announcing the theoretically matching Bell state, he still cannot derive the users' x basis measurement result. Furthermore, Trent introduces errors into the measurement results, since a state measured in the z basis results in a random x basis measurement outcome (see J.1). The improved proposal still prevents passive eavesdropping, because Trent cannot derive any final measurement results from his resultant Bell state (cf. tab. 6.3, p. 76).

Compared with the original protocol, Eve's eavesdropping attack on the authentication does not vary in its procedure but in its results (see J.2 for details). To gain knowledge of an ID Eve impersonates Trent or attacks the encoded sequences transmitted from Trent to Alice or Bob. In an impersonation of Trent Eve's detection and success probabilities total $1-(1-\frac{1}{4})^{c_1}$ (with $c_1 = c_{AUTH}/2$), because Eve can only differentiate the decoding operations in case of an encoding error on her side. The detection probabilities in an intercept-resend attack and in both translucent attacks also remain at least 25 % per check qubit as in the original protocol. The essential improvements in the authentication of the proposal are the embedded authentication, the adjustment of the eavesdropping test into dialogue form, and the adaption of the authentication key according to section 3.2. All aspects together prevent

Eve's authentication attacks. Additionally, the c_{AUTH} check qubits represent only a subset of all encoded qubits, which entails restoring problems of an attacker resulting in additional detection probabilities during communication.

If Eve intends to eavesdrop on the direct communication, she also attacks the transmission of the encoded A- and B-sequences. No other information is transmitted over quantum links during the entire communication round. Hence, the detection probabilities of Eve's eavesdropping attack on the authentication remain valid here, which are sufficient to ensure communication or the abort of communication. An additional, optional eavesdropping test on the c_{ES} check qubits can be applied before sending the messages on the final bases via bitflip announcements. The direct communication process inherits errors which Eve introduced during authentication. Hence, the optional test also offers detection, and Eve has serious derivation problems regarding the final bases. By reason of their complexity only the initial terms for these calculations are given in appendix J.3.

A sender or receiver impersonation is not successful (see J.4 for detailed calculations). Due to Eve's lack of the authentication key, she introduces errors into the system with the probability of $\frac{1}{4}$. Hence, the detection probability amounts to $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1}$ (with $c_1 = c_{AUTH}/2$) during the first mandatory eavesdropping test. In the second optional eavesdropping test this probability recurs, that is $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_2}$ (with $c_2 = c_{ES}/2$). Furthermore, any Bell state occurs for all x basis measurement combinations in an impersonation. Thus, Eve can neither draw a definite conclusion on the final basis of the legitimate user nor derive her or his assumption of her basis.

The impersonation of Trent and Alice or Bob do not have to be calculated in detail, but can be derived from the simple impersonation attacks. An restoring error occurs on Eve's qubit in a simple attack due to incorrect decoding, whereas it appears on the side of the legitimate user in an advanced attack due to incorrect encoding. Hence, Eve's impersonation of Alice and Trent in the first advanced impersonation attack can be derived from Eve's simple impersonation of Bob, and Eve's impersonation of Bob and Trent in the second advanced impersonation attack shows the same errors as in a simple impersonation of Alice. Thus, the overall detection probability totals $\rho_D = 1 - \left(1 - \frac{1}{4}\right)^{c_1} + 1 - \left(1 - \frac{1}{4}\right)^{c_2}$ in both attacks (with $c_1 = c_{AUTH}/2$ and $c_2 = c_{QDC}/2$) and Eve cannot be successful in an advanced impersonation.

Eve cannot be successful in the third advanced impersonation attack either, that is in an impersonation of Trent. This result can be deduced from the fact that Trent is not in the position of beneficial eavesdropping. Thus, even if Eve managed to get in his position without introducing errors into the system, she could not succeed. The derived proof in appendix J.5 circumstantiates her failure. Eve cannot derive any bit of the final bases. Furthermore, the detection probabilities amount to $\rho_D = 1 - \left(1 - \frac{1}{2}\right)^{c_1}$ in the first eavesdropping test (with $c_1 = c_{AUTH}/2$) and to $\rho_D = 1 - \left(1 - \frac{3}{8}\right)^{c_{ES}}$ in the second test between Alice and Bob.

Since Eve is not successful in any impersonation attack, she cannot consider a man-in-the-middle attack. The communication is already supposed to be aborted after the first eavesdropping tests because of the high detection probabilities of $\rho_D = 1 - (1 - \frac{1}{4})^c_1$. Even in the case of a failed detection, Eve cannot control any bit of the final bases.

Proposal 4 improves the original protocol to the results that it prevents all attacks and requires less complex protocol tasks. Moreover, it reduces the number of required transmissions and eavesdropping tests and increases the potential length of the message. Apart of the advanced security, the most important achievement of the modification is that it offers bidirectional communication.

Chapter 7

Conclusion

Quantum cryptography applies the properties of quantum systems to cryptographic concepts with the purpose of protecting the transmitted information from any kind of unauthorised disclosure. It exploits quantum mechanical features, such as superposition, entanglement, decoherence, uncertainty, and the no-cloning theorem, and offers automatic "intrusion detection" (Lomonaco, 1998) as a new contribution to cryptography. Quantum cryptography progresses rapidly. Several books provide a basic introduction to quantum mechanics and most include a chapter of quantum cryptographic basics, e.g. Bouwmeester et al. (2000), Heiss (2002), Bruß (2003), Homeister (2005), and Marinescu and Marinescu (2005). Lomonaco (1998, 2001) offers entertaining introductions. Bennett et al. (1992a) and Gisin et al. (2001) contain comprehensive disquisitions on quantum cryptography. For current research the Cornell University Library offers the eprint service arXiv. Related articles are also published in the journals Physical Review A and Physical Review Letters of the American Physical Society.

Three quantum cryptographic protocols of multiuser quantum networks with embedded authentication were discussed and analysed in this work. The secret communication of all protocols is based on entangled systems. The properties of their entanglement guarantee security during the transmission, since the transmitted particle is perfectly correlated for undisturbed transfer to the particle, which is kept safely, and does not carry any information. The aspect of authentication developed from the insight that quantum cryptographic protocols are completely insecure in an impersonation or a man-in-the-middle attack for realistic assumptions.

Protocol 1 (Lee et al., 2006) and protocol 2 (Lee et al., 2005) serve the purpose of quantum key distribution and quantum direct communication, respectively. Protocol 3 (Hong et al., 2006) was originally developed for quantum direct communication. Due to the characteristic of the protocol, it may also accomplish quantum key distribution. All protocols are applied with an authority Trent in multiuser quantum networks, in which any two registered users can securely communicate without a direct quantum channel between them. Trent registers a network user in a personal authentication and provides her or him with a secret identification sequence (ID). The authentication in any new communication round is based on a renewable authentication key, recalculated by a one-way hash function with the ID and a counter. Hence, the secret ID does not become obsolete in further communication, not even if

the authentication key has been eavesdropped. The authentication exploits the feature that any unitary transformation provides its inverse transformation. The particles are transmitted encoded and restored to their original state via the decoding operations. Since the authentication is embedded in the communication, there is no gap between both processes, in which an attacker may replace a legitimate party. The existence of Trent minimises the amount of essential secret information within the network to n (for n registered network parties), which represents a considerable reduction compared to the amount of $n(n-1)/2$ and $2n$ required for private-key and public-key cryptography, respectively.

The concept of the multiuser network meets realistic conditions, since no direct quantum links between the network users are required. The authentication process represents a novel authentication approach, which seems to be most auspicious in current research for realisable network implementations. The communication parties do not share any kind of initial information, and the key amount is limited to the most obtainable scale. Furthermore, due to the integration of authentication into communication, restoring errors occur during an impersonation attack. These errors are not only detectable in the authentication process, but they also entail detection in any eavesdropping test of the communication, if the legitimate parties check only a subset of their qubits during authentication. Eve cannot avoid the control procedure because of this integration and the revelation of the check qubits, once transmission is completed. Moreover, the restoring errors lead to severe derivation problems of the attacker in the reconstruction of the legitimate user's operations or measurement outcomes, resulting in a very restricted controllability of the key or the message bits.

In this work all protocols were analysed with regard to the most important requirements of cipher systems, i.e. data confidentiality, data integrity, and user authentication. As single attacks Trent's passive and active eavesdropping and Eve's eavesdropping attacks on the authentication and the communication process were investigated. Since the work focused on an authenticated multiuser network, complete scenarios of impersonation attacks, culminating in a man-in-the-middle attack, were also designed and analysed. On the basis of the security analysis several improvements were suggested to adjust the investigated vulnerabilities or to adapt the protocol to the multiuser concept. The improvements were implemented in the proposals 1 – 4.

Idealistic conditions and a perfect environment were assumed in this work. Hence, any error during the transmission was traced back to an unauthorised attacker. Further research is required to analyse more realistic conditions, and analyses regarding other types of attacks, e.g. coherent attacks, are essential. An analysis of the impact of supplementary techniques, such as error correction codes or privacy amplification, is still to be undertaken for the discussed protocols.

Protocol 1 allows secure quantum key distribution after the communication parties are authenticated as legitimate. Subsequently, the secret key is applied to classical private-key cryptography. This beforehand step of key distribution ahead of the secret message exchange reduces the efficiency of the communication. Further reductions of efficiency are prevented by reason of the deterministic trait of the protocol.

Protocol 1 offers high detection probability and low success probability in all analysed attacks. Furthermore, it can be implemented in a multiuser quantum network as shown in the improved proposal 1. The extra quantum channel between Alice and Bob for the transmission of Bob's encoded key values was eliminated to achieve this aim. Alice and Trent had to exchange their measurement tasks and the encoding operations were adapted. The proposal also avoids Bob's one-sided suggestion of the distributed key to achieve the randomness and fairness as emphasised in most key distribution protocols. A key proposal of both parties was realised by dividing the qubit set into two subsets, so that Bob proposes the first part of the key encoded in the first subset, and Alice suggests its second part on the second subset. Proposal 1 features high security on a similar scale as the original protocol 1.

In Protocol 2 Alice can directly send her message to Bob within the quantum system after they are both authenticated. Since the secure communication is completed in one step without conventional cryptography, its efficiency rises in comparison to quantum key distribution.

Protocol 2 also provides high security in all analysed attacks, except Trent's active eavesdropping as pointed out in Zhang (2006). Trent can distinguish Alice's encoding operations, due to the respective transformation of the system via Hadamard and bitflip operations. Zhang (2006) coevally published the improvement of exchanging the bitflip operation with a Pauli-Z operation to prevent Trent's attack. His suggestion was implemented in the improved proposal 2. Apart from the exchanged operations, the procedure did not essentially change, and all security properties of the original protocol 2 were maintained.

Protocol 1 and protocol 2 are based on tripartite GHZ states. Protocol 3 operates on bipartite Bell states, which can be realised more easily than GHZ states. It was published for the purpose of quantum direct communication with the transfer of the message on a final basis through Alice's bitflip announcements. The final basis consists of Bob's measurement results, which Alice can derive. In contrast to the other two protocols, which work with encoding operations, the final basis of protocol 3 is arranged via entanglement swapping. The revelation of the message bits via bitflip announcements features an outstanding benefit. Without the bitflip positions the values of the final basis randomly come into existence. Therefore, the protocol may also be used for quantum key distribution as discussed in this work.

However, protocol 3 was proven insecure in the analysis. Several vulnerabilities in the authentication process, which differs from the authentication method of the first two protocols, were investigated. Furthermore, Trent is successful in an active eavesdropping attack, because he is in possession of the qubits correlated to Bob's qubits, which represent the final basis for the message transfer. Moreover, Eve can launch a successful translucent attack on the communication without being detected, and different kinds of impersonation attacks as well as the man-in-the-middle attack are feasible. These attacks are possible, since the authentication process is not integrated into communication. Two different proposals, which are based on the embedded authentication method of protocol 1 and protocol 2, were developed for rectification.

The improved proposal 3 reconfigured the original protocol as congeneric as possible in line with the most essential security requirements. That way, all attacks can be avoided, ex-

cept Trent's eavesdropping. In the improved proposal 4 the original protocol was completely remodelled to the effect that it prevents all attacks and additionally offers bidirectional communication. Thus, Alice sends Bob her message, and Bob can transmit his response to Alice without initialising a new communication round. As the original protocol, proposal 4 serves the purpose of quantum key distribution and quantum direct communication. It combines the authentication and communication process into a single step, so that only one transmission of qubits must be completed during the entire communication round. Thus, only one eavesdropping test is mandatory to achieve high security. The potential message length increases by 100 % because of the resultant two bases which the users can utilise for the message transfer. Hence, the expenditure of time and medium profoundly decreases. Apart from these achievements, proposal 4 requires less complex protocol tasks. On account of the discussed issues, the improved proposal 4 features outstanding advantages, but further research is essential.

In all protocols and proposals a secret sign, included in the final message, could avoid any kind of Eve's impersonation attacks. Such a sign was not assumed in the security analyses, since it would lead to distribution problems of the initial secret. A request identification might be considered without any distribution problem in order to prevent the first simple impersonation attack or to hamper a man-in-the-middle attack. Provided that the test proceeds as a dialogue, Bob's probability to detect Eve in all of her first announcements ranges between $\frac{1}{4}$ and $\frac{1}{2}$, though. Eve's success probability maximally amounts to $\frac{1}{4}$ per qubit. Due to this high security, an additional identification is not required to protect the protocols against the attacks.

The specification of the eavesdropping test procedure as given in this work is essential to achieve maximum security. Any public discussion was realised as a dialogue with the first announcements alternating between the parties in order to attain a balanced detection probability in all impersonation attacks. Any unnecessary one-sided determination of the check positions was eliminated and the selection of the control subset was divided in equal shares whenever possible. The consequences of non-compliance with this general procedure were discussed in detail in the security analyses. The specific realisation of the eavesdropping tests and all insights into the consequences are new.

The outstanding benefit of quantum cryptography, in comparison with its classical counterpart, arises from the automatic eavesdropping detection, the avoidance of key distribution problems, and its resistance to the code-breaking capability of quantum computing. Vernam's one-time pad represents the only conventional encryption method, whose security quantum computers cannot undermine. Due to its symmetric nature, it cannot be implemented without key distribution problems, though. Taking into consideration that public-key cryptography has been researched years before it was published, the development of quantum computers may already be more advanced at present than is known publicly.

Although "quantum cryptography has marched from theory to laboratory to real products" (Stix, 2004) during the last decades, scientific and technological research is still required, and quantum cryptography must yet evolve "into an instrument that can be operated in an economic environment" (SECOQC, 2006). In spite – or because – of the outstanding strength

of quantum cryptography, its commercial realisation may be uncertain for another reason. According to Gisin et al. (2001, p. 45), the "apparent strength of QC [quantum cryptography] might turn out to be its weak point: the security agencies would equally be unable to break quantum cryptograms".

List of Figures

List of Tables

Bibliography

American Physical Society. Website. URL `http://publish.aps.org`; date: November 2006.

arXiv. Eprint service of the Cornell University Library. URL `http://www.arxiv.org`; date: November 2006.

H. Barnum. Quantum secure identification using entanglement and catalysis. *arXiv eprint: quant-ph/9910072 v1*, 1999.

A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter. Secure communication with single-photon two-qubit states. *arXiv eprint: quant-ph/0101066 v4*, 2002a.

A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter. Secure communication with a publicly known key. *arXiv eprint: quant-ph/0111106 v2*, 2002b.

C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, 1984.

C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. *Scientific American*, pages 26–33, 1992a. German edition: Quanten-Kryptographie. *Spektrum der Wissenschaft Digest: Quantenphänomene*, pages 90-98, 1999.

C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum Cryptography without Bell's Theorem. *Physical Review Letters*, 68:557–559, 1992b.

E. Biham, B. Huttner, and T. Mor. Quantum Cryptographic Network based on Quantum Memories. *arXiv eprint: quant-ph/9604021 v1*, 1996.

K. Boström and T. Felbinger. Deterministic Secure Direct Communication Using Entanglement. *arXiv eprint: quant-ph/0209040 v2*, 2002.

D. Bouwmeester and A. Zeilinger. The Physics of Quantum Information: Basic Concepts. In D. Bouwmeester, A. Ekert, and A. Zeilinger, editors, *The Physics of Quantum Information*, pages 1–14. Springer, 2000.

D. Bouwmeester, A. Ekert, and A. Zeilinger, editors. *The Physics of Quantum Information*. Springer, 2000.

D. Bouwmeester, J. C. Howell, and A. Lamas-Linares. Quantum Information Science Using Photons. In D. Heiss, editor, *Fundamentals of Quantum Information*, pages 149–197. Springer, 2002.

D. Bruß. *Quanteninformation: Turingmaschine, Komplexitẗ, Superposition, Verschränkung, No-cloning-Prinzip, Bell'sche Ungleichung, Quantenteleportation, Quantenkryptographie, Quantencomputer, Quantenalgorithmen, Quantenspiele*. Fischer-Taschenbuch-Verlag, 2003.

C. Crépeau and L. Salvail. Quantum Oblivious Mutual Identification. In L. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology - EUROCRYPT '95*, pages 133–146. Springer, 1995.

F.-G. Deng, G. L. Long, and X.-S. Liu. A Two-Step Quantum Direct Communication Protocol Using Einstein-Podolsky-Rosen Pair Block. *arXiv eprint: quant-ph/0308173 v1*, 2003.

W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.
available at URL `http://www-ee.stanford.edu/~hellman/publications/24.pdf`;
date: November 2006.

M. Dušek, O. Haderka, M. Hendrych, and R. Myška. Quantum identification system. *Physical Review A*, 60:149, 1999.

A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, 47:777–780, 1935.

A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67: 661–663, 1991.

B.-G. Englert, C. Kurtsiefer, and H. Weinfurter. Universal unitary gate for single-photon two-qubit states. *Physical Review A*, 63:032303, 2001.

F. Gao, F. Guo, Q. Wen, and F. Zhu. A quantum key distribution and identification protocol based on entanglement swapping. *arXiv eprint: quant-ph/0412014 v1*, 2004.

T. Gao, F. L. Yan, and Z. X. Wang. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. *arXiv eprint: quant-ph/0406082 v2*, 2005.

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *arXiv eprint: quant-ph/0101098 v2*, 2001.

D. Heiss, editor. *Fundamentals of Quantum Information*. Springer, 2002.

M. Homeister. *Quantum Computing Verstehen*. Vieweg, 2005.

C. Hong, J. Kim, H. Lee, and H. Yang. Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping. *arXiv eprint: quant-ph/0601194 v2*, 2006.

J. G. Jensen and R. Schack. Quantum authentication and key distribution using catalysis. *arXiv eprint: quant-ph/0003104 v3*, 2000.

X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um. Three-party quantum secure direct communication based on Greenberger-Horne-Zeilinger states. *arXiv eprint: quant-ph/0601125 v1*, 2006.

D. Kahn. *The Codebreakers*. Scribner Book Company, 2nd edition, 1996.

A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38, 1883.
available at URL `http://www.petitcolas.net/fabien/kerckhoffs`;
date: November 2006.

D. R. Kuhn. A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography. *arXiv eprint: quant-ph/0301150*, 2003.

H. Lee, May 2006. private email communication.

H. Lee, J. Lim, and H. Yang. Quantum Direct Communication with Authentication. *Physical Review A*, 73:042305, 2005.
also available at *arXiv eprint: quant-ph/0512051 v1*.

H. Lee, J. Lim, and H. Yang. Quantum Authentication and Quantum Key Disribution Protocol. *arXiv eprint: quant-ph/0510144 v2*, 2006.

D. Ljunggren, M. Bourennane, and A. Karlsson. Authority-based user authentication in quantum key distribution. *Physical Review A*, 62:022305, 2000.

S. J. Lomonaco. A Quick Glance at Quantum Cryptography. *arXiv eprint: quant-ph/9811056 v1*, 1998.

S. J. Lomonaco. A Talk on Quantum Cryptography or How Alice outwits Eve. v. 1.5, 2001.
URL `http://www.cs.umbc.edu/~lomonaco/qcryptotalk/CryptoDrama.pdf`;
date: November 2006.

C. C. Mann. Homeland Insecurity. *The Atlantic online*, 2002.
URL `http://www.theatlantic.com/doc/200209/mann`; date: November 2006.

D. C. Marinescu and G. M. Marinescu. *Approaching Quantum Computing*. Pearson, 2005.

T. Mihara. Quantum identification schemes with entanglements. *Physical Review A*, 65: 052326, 2002.

B. A. Nguyen. Quantum dialogue. *arXiv eprint: quant-ph/0406130 v1*, 2004.

QE. Quantum Entanglement. Wikipedia-Websites. URL `http://en.wikipedia.org/wiki/Quantum_entanglement` and `http://de.wikipedia.org/wiki/Quantenverschr%C3%A4nkung` ; date: November 2006.

R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21:120–126, 1978.
available at URL `http://theory.lcs.mit.edu/~rivest/`; date: November 2006.

B. Schneider. *Applied Cryptography*. John Wiley and Sons, 2nd edition, 1996.

E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807–812; 823–828; 844–849, 1935.
English translation by J. D. Trimmer in *Proceedings of the American Philosophical Society*, 124:323-338, 1980.
available at URL `http://www.tu-harburg.de/rzt/rzt/it/QM/cat.html#star`;
date: November 2006.

SECOQC. Website. URL `http://www.secoqc.net`; date: November 2006.

C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28:656–715, 1949.
available at URL `http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf`;
date: November 2006.

B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo. Quantum Key Distribution and Quantum Authentication Based on Entangled State. *arXiv eprint: quant-ph/0102058 v1*, 2001.

S. Singh. *Geheime Botschaften - Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets*. Deutscher Taschenbuch Verlag, 6th edition, 2005.

D. Stinson. *Cryptography - Theory and Practice*. CRC Press, Inc., 2nd edition, 2002.

G. Stix. Best-Kept Secrets. *Scientific American Magazine*, 2004.
URL `http://www.sciam.com/article.cfm?articleID=000479CD-F58C-11BE-AD0683414B7F0000`;
date: November 2006.

J. Wang, Q. Zhang, and C.-J. Tang. Multiparty simultaneous quantum identity authentication based on entanglement swapping. *arXiv eprint: quant-ph/0605006 v1*, 2006.

Wikipedia. Websites. URL `http://en.wikipedia.org` and `http://de.wikipedia.org`;
date: November 2006.

K. W. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

Y. Xia, C.-B. Fu, F.-Y. Li, S. Zhang, K.-H. Yeon, and C.-I. Um. Controlled Secure Direct Communication by Using GHZ Entangled State. *arXiv eprint: quant-ph/0601145 v1*, 2006a.

Y. Xia, C.-B. Fu, S. Zhang, S.-K. Hong, K.-H. Yeon, and C.-I. Um. Quantum Dialogue by Using the GHZ State. *arXiv eprint: quant-ph/0601127 v1*, 2006b.

G. Zeng and G. Guo. Quantum authentication protocol. *arXiv eprint: quant-ph/0001046 v1*, 2000.

G. Zeng and W. Zhang. Identity verification in quantum key distribution. *Physical Review A*, 61:022303, 2000.

Y.-S. Zhang, C.-F. Li, and G.-C. Guo. Quantum authentication using entangled state. *arXiv eprint: quant-ph/0008044 v2*, 2000.

Z. Zhang. Deterministic Secure Direct Bidirectional Communication Protocol. *arXiv eprint: quant-ph/0403186 v1*, 2004.

Z.-J. Zhang. Improving the security of quantum direct communication with authentication. *arXiv eprint: quant-ph/0604125 v2*, 2006.

Z. J. Zhang and Z. X. Man. Secure Bidirectional Quantum Communication Protocol without Quantum Channel. *arXiv eprint: quant-ph/0403217 v4*, 2004a.

Z. J. Zhang and Z. X. Man. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. *arXiv eprint: quant-ph/0403218 v1*, 2004b.

A.-D. Zhu, Y. Xia, Q.-B. Fan, and S. Zhang. Secure direct communication based on secret transmitting order of particles. *Physical Review A*, 73:022338, 2006.

M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping. *Physical Review Letters*, 71:4287–4290, 1993.

Anhang A

Deutsche Zusammenfassung (German Abstract)

Kryptologie ist die Wissenschaft der geheimen Kommunikation. Sie umfasst die Teilgebiete Kryptographie, die Kunst der Verschlüsselung, und Kryptoanalyse, die Studie von Methoden, kryptographische Verfahren zu unterlaufen. In der Fachliteratur wird Kryptographie jedoch meist als Oberbegriff für die Wissenschaft der geheime Kommunikation verwendet.

Kryptographische Verfahren schützen die Kommunikation vor unberechtigtem Zugriff. Klassische Kryptographietechniken sind zum einen die symmetrische Kryptographie mit einem geheimen Schlüssel, den beide Kommunikationspartner besitzen müssen (*private-key cryptography*). Zum anderen entstand um 1970 die asymmetrische Kryptographie, bei der jeder Kommunikationspartner einen öffentlichen Schlüssel zum Verschlüsseln und einen geheimen Schlüssel zum Entschlüsseln besitzt (*public-key cryptography*). Die asymmetrische Kryptographie wurde als Lösung des Schlüsselverteilungsproblemes entwickelt, dass bei der symmetrischer Kryptographie auf Grund des Gebrauchs eines einzigen geheimen Schlüssels unweigerlich auftritt und im Zeitalter der modernen Kommunikation zu großen logistischen Schwierigkeiten führt. Die Sicherheit der asymmetrischen Kryptographie basiert auf der Unmöglichkeit, die zugrunde liegenden mathematisch schwer lösbaren Probleme mit heutiger Rechnerkapazität zu berechnen. Mit der Entwicklung eines Quantencomputers würden jedoch auf Grund der extrem hohen Rechenleistung alle asymmetrischen Kryptographiemethoden obsolet.

Quantenkryptographie bietet jene Sicherheit, die von potenziellen Quantencomputern nicht unterlaufen werden kann, ohne Schlüsselverteilungsprobleme hervor zu rufen. Diese neue Art der Kryptographie, basierend auf grundlegenden Gesetzmäßigkeiten der Quantenmechanik, wird seit dem Ende des 20 Jahrhunderts erforscht und nutzt spezielle Eigenschaften von Quantensystemen, wie Superposition, Verschränkung, Dekoheränz und Unschärfe. Zudem bietet die Quantenkryptographie die Möglichkeit, unberechtigtes Belauschen der Kommunikation zu entdecken, was einen völlig neuen Aspekt innerhalb der Kryptographiewissenschaft darstellt.

In der Quantenkryptographie werden zwei verschiedene Kommunikationsverfahren verwendet. Mit Hilfe der Quantenschlüsselverteilung (*quantum key distribution*) können zwei Kommunikationspartner einen geheimen Schlüssel vereinbaren, mit dem sie dann ihre ge-

heime Nachricht symmetrisch ver- und entschlüsseln. Als symmetrische Verschlüsselung wird das *one-time pad* von Vernam angewandt, das einzige klassische Verfahren, welches beweisbare Sicherheit gegenüber Quantencomputern bietet. Durch die Kombination der Quantenschlüsselverteilung und der klassischen Kryptographietechnik wird Vernams Verfahren realistisch einsetzbar, da das Problem der Schlüsselverteilung sicher gelöst wird. Im zweiten quantenkryptographischen Verfahren, der direkten Quantenkommunikation (*quantum direct communication*), kann die Nachricht ohne vorhergehenden Schlüsselaustausch sicher innerhalb des Quantensystems übertragen werden. Ein neues Forschungsgebiet innerhalb der Quantenkryptographie stellen Quantennetzwerke mit mehrere Benutzer dar (*multiuser quantum networks*). Durch diese Entwicklung wird die Anwendung und Verbesserung von Authentifikationsmethoden essenziell.

In dieser Diplomarbeit werden drei verschiedene quantenkryptographische Protokolle mit dem Schwerpunkt auf authentifizierten Quantennetzwerken analysiert. Die Informationsübertragung basiert in allen Protokollen auf verschränkten Quantensystemen. Die Protokolle führen eine dritte Person als Netzwerkinstanz ein, die die Benutzer authentifiziert. Die Authentifikation basiert auf einem Authentifikationsschlüssel, der für jede neue Kommunikation mittels eines Zählers und einer geheimen ID, die nur der Netzwerkauthorität und dem jeweiligen Nutzer bekannt ist, durch eine Einweg-Hashfunktion neu berechnet wird. Durch die ständige Erneuerung der Authentifikationsschlüssels ist die Sicherheit der Authentifikation selbst im Falle eines Angriffs auf den Schlüssel während einer vorhergehenden Quantenkommunikation gewährleistet. Auf Grund der Netzwerkinstanz minimiert sich die Anzahl an geheimer Anfangsinformation (hier der ID) bei einem Netzwerkpotenzial von n registrierten Nutzern auf n. Zudem kann das Quantennetzwerk unter Einbeziehung der Instanz so aufgebaut werden, dass keine direkten Quantenkanäle zwischen den Benutzern benötigt werden.

Die Authentifikation ist im Kommunikationsprozess eingebettet. Ein Angreifer, der sich als einer der legitimen Kommunikationspartner ausgibt (*impersonation attacks*, Personifikationsattacken), muss somit an dem Authentifikationsprozess teilnehmen und wird im Quantensystem Fehler verursachen. Diese Fehler werden nicht nur während der Authentifikation, sondern auch während der nachfolgenden Kommunikation entdeckt. Darüber hinaus beeinträchtigen sie mit einer bestimmten Wahrscheinlichkeit die Korrektheit und die Eindeutigkeit der ausgetauschten Information.

In der Sicherheitsanalyse aller Protokolle werden unterschiedliche Angriffsszenarien untersucht. Als Angreifer auf die Informationsübertragung wird sowohl die Netzwerkauthorität als auch ein unabhängiger Angreifer in Betracht gezogen. Zudem wird ein Angriff auf den Authentifikationsprozess analysiert. Da bei dieser Arbeit der Schwerpunkt auf authentifizierten Netzwerken liegt, werden komplette Szenarien für verschiedene Personifikationsattacken entwickelt und untersucht. Um die Gefahr von Personifikationen realistisch abschätzen zu können, wird in dieser Arbeit außerdem eine Spezifikation zur Überprüfung der Sicherheit festgelegt und erläutert. Ein fehlerhaftes Überprüfungsverfahren kann die Sicherheit des kompletten Protokolls untergraben. Auf Basis der Sicherheitsanalyse und den Netzwerkanforderungen werden für alle Protokolle entsprechende Verbesserungen vorgeschlagen und umgesetzt.

Protokoll 1 (Lee et al., 2006) dient den Anwendern zur Vereinbarung eines geheimen Schlüssels, nachdem sie korrekt authentifiziert wurden. Die Sicherheit des Schlüssels bestätigt sich in der Sicherheitsanalyse. Die, der Analyse nachfolgenden, Verbesserungsvorschläge betreffen hauptsächlich den Aspekt, das Protokoll netzwerkkompatibel zu realisieren. Protokoll 2 (Lee et al., 2005) ermöglicht es den Benutzern im Falle einer erfolgreichen Authentifikation direkt zu kommunizieren. Die einzige Sicherheitslücke des Protokolls wurde bereits von Zhang (2006) aufgedeckt und geschlossen. Sein Vorschlag wird hier umgesetzt und analysiert. Protokoll 3 (Hong et al., 2006) wurde ursprünglich für die direkte Kommunikation entwickelt. Es wird hier jedoch erläutert, dass das Protokoll auch zum Zwecke der Schlüsselverteilung eingesetzt werden kann. Das Protokoll weist allerdings mehrere Schwachstellen auf und ist in seiner Orginalform auf Grund der mangelnden Sicherheit in Personifikationsattacken nicht für Netzwerke geeignet. Um die Schwachstellen zu beheben werden zwei verschiedene Verbesserungsansätze verfolgt. In der ersten Weiterentwicklung ist beabsichtigt, das Orginalprotokoll nur soweit zu verändern, wie es die Beseitigung der schwerwiegendsten Mängel erfordert. Der zweite Verbesserungsansatz erhält nur die grundlegenden Protokolleigenschaften, während mehrere Prozesse neu umgesetzt werden. Auf Grund dieser Änderungen wird die Sicherheit optimal verbessert. Darüber hinaus ermöglicht der Ansatz bidirektionale Kommunikation, d.h. Kommunikation vom Sender zum Empfänger und umgekehrt.

Die Diplomarbeit gliedert sich wie folgt. Kapitel 1 enthält eine kurze Einführung in die Kryptographie. In Kapitel 2 werden die grundlegenden quantenkryptographischen Gesetze und Verfahren erläutert. Die allgemeinen Rahmenbedingungen, auf denen diese Arbeit basiert, werden in Kapitel 3 behandelt. In den Kapiteln 4 – 6 werden die drei Protokolle vorgestellt, diskutiert und analysiert. Zusätzlich werden Verbesserungen vorgeschlagen und umgesetzt. Die Arbeit schließt in Kapitel 7 mit einer kurzen Zusammenfassung der wichtigsten Ergebnisse.

Appendix B

Original Protocols

Protocol 1

Quantum Authentication and Quantum Key Distribution Protocol
(Lee et al., 2006)

Protocol 2

Quantum Direct Communication with Authentication
(Lee et al., 2005)
Please note that for this publication the version published at arXiv is attached and not the version published in Physical Review A, although it is stated otherwise in the text.

Protocol 3

Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping
(Hong et al., 2006)

arXiv:quant-ph/0510144 v2 11 Jan 2006

Quantum Authentication and Quantum Key Distribution Protocol

Hwayean Lee[1,2,3], Jongin Lim[1,2], and HyungJin Yang[2,4]

Center for Information Security Technologies(CIST)[1],
Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
Graduate School of Information Security(GSIS)[2]
Institut für Experimentalphysik, Universität Wien, Austria[3]
Department of Physics, Korea University, Chochiwon,Choongnam, Korea[4]
{hylee, jilim, yangh}@korea.ac.kr

Abstract. We propose a quantum key distribution protocol with quantum based user authentication. Our protocol is the first one in which users can authenticate each other without previously shared secret and then securely distribute a key where the key may not be exposed to even a trusted third party. The security of our protocol is guaranteed by the properties of the entanglement.

1 Introduction

Quantum key distribution(QKD) is the most actively researched field in Quantum Cryptography. Since BB84 protocol[1] was proposed by Bennett and Brassard in 1984 as a start, many QKD protocols have been proposed[2–4] and implemented[5–7]. The great advantage of QKD is to provide the provable security of distributed keys[8–10]. However, it is assumed that the quantum channel is directly connected and previously authorized to the designated users in those protocols. This assumption is not suitable on the consideration of quantum networks. To authenticate users on the quantum networks, Quantum Authentication protocols[11–18] are proposed since Crepeau and L. Salvail first proposed a quantum identification protocol in 1995. Some Quantum Authentication protocols assume that the users have some authentication information such as entangled states[11–13] and authentication sequence[14, 15]. As mentioned above, these protocols can not be operated on the quantum networks. Other quantum authentication protocols[16–18] introduced a trusted third party. Quantum authentication protocols proposed by Zeng and Zhang[16] in 2000 and Mihara[17] in 2002 are only for authentication. Alice and Bob can authenticate each other and distribute key without previously shared information only in one protocol proposed by Ljunggren and et al.[18]. The major disadvantage of this protocol is the leakage of the key to the trusted third party.

In this paper, we propose a Quantum Key Distribution protocol with authentication. The proper users, Alice and Bob can authenticate each other without previously shared secret and share a secret key without leakage of information

to anyone. We organize this paper as follows. First, we propose a new QKD protocol with user authentication in chapter 2. Our QKD protocol is composed of two parts: one is authentication and the other key is distribution. Greenberger - Horne - Zeilinger (GHZ) states[19] are used to authenticate users and distribute a secret key. The security analysis of our protocol is discussed in chapter 3 and at last our conclusion is presented in chapter 4.

2 Quantum Authentication and Quantum Key Distribution protocol

2.1 Authentication

We assume that Alice and Bob do not share any prior secret information or entanglement states for authentication. To identify each other in the communication, they are supposed to introduce a trusted third party, Trent. Trent plays a role like a CA(certificate authority) in PKI(Public Key Infrastructure)[20, 21]. If there are n users in quantum networks, then $\frac{n(n-1)}{2}$ keys are needed to communicate freely when there is no Trent. Besides, each user must distribute $n-1$ secret keys with other users. However, only n keys are needed when Trent exists and each user just needs to distribute one secret key with Trent. Trent may be a loophole for security. However it can be overcome using similar methods applied to CA.

We assume that Alice has registered her secret identity ID_A and a one-way hash function $h_A : \{0,1\}^* \times \{0,1\}^l \rightarrow \{0,1\}^m$, where $*$ means an arbitrary length, l is the length of a counter, and m is a constant. Bob has also registered his secret identity ID_B and a one-way hash function h_B to Trent. This information is assumed to be kept secret between the user and Trent. Authentication key can, then, be generated by a hashed value $h_{user}(ID_{user}, c_{user})$ where c_{user} is a counter which is the number of the calls of the one way hash function h_{user}.

If Alice wants to distribute a key with Bob, she notifies this fact to Bob and Trent. On receiving the request, Trent generates N GHZ tripartite states $|\Psi\rangle = |\psi_1\rangle|\psi_2\rangle...|\psi_N\rangle$. For simplicity the following GHZ state $|\psi_i\rangle$ is supposed to be prepared.

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$$

where the subscripts A, T and B correspond to Alice, Trent, and Bob, respectively. In this paper, we represent the z basis as $\{|0\rangle, |1\rangle\}$ and the x basis as $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Next, Trent encodes Alice's and Bob's particles of GHZ states with their authentication keys, $h_A(ID_A, c_A)$ and $h_B(ID_B, c_B)$, respectively. For example, if the ith value of $h_A(ID_A, c_A)$ is 0, then Trent makes an identity operation I to Alice's particle of the ith GHZ state. If it is 1, Hadamard operation H is applied. If the authentication key does not have enough length to cover all GHZ particles, new authentication keys can be created by increasing the counter until the authentication keys shield all GHZ particles. After making operations on

the GHZ particles, Trent distributes the states to Alice and Bob and keeps the remaining for him.

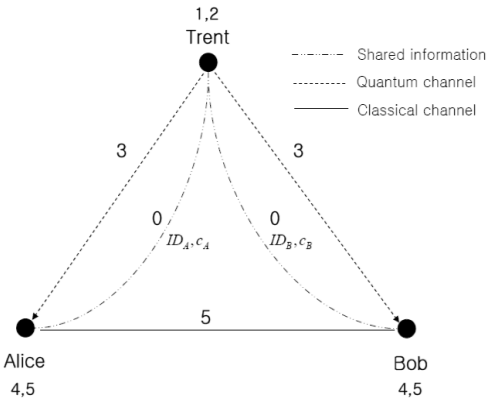

Fig. 1. Procedures of Authentication 0. Alice and Bob register their secret identities and hash functions to Trent. 1. Trent generates GHZ states $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$. 2. Trent makes unitary operations on $|\psi\rangle$ with Alice's and Bob's authentication key. 3. Trent distributes GHZ particles to Alice and Bob. 4. Alice and Bob make reverse unitary operations on their qubits with their authentication key, respectively. 5. Alice and Bob choose the position of a subset of GHZ states and make a local measurement in the z basis on them and compare the results.

On receiving the qubits, Alice and Bob make reverse unitary operations on their qubits with their authentication key $h_A(ID_A, c_A)$ and $h_B(ID_B, c_B)$, respectively. This authentication procedure can be written in the following form of sequences of local unitary operation, the initial state:

$$|\psi_i\rangle_1 \;=\; \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$$

state after Trent's transformation

$$\begin{aligned} |\psi_i\rangle_2 \;&=\; \{[1 - h_A(ID_A, c_A)]I + [h_A(ID_A, c_A)]H\}_A \\ &\otimes \{[1 - h_B(ID_B, c_B)]I + [h_B(ID_B, c_B)]H\}_B |\psi_i\rangle_1 \end{aligned}$$

and finally the state after Alice's and Bob's local operations

$$\begin{aligned} |\psi_i\rangle_3 \;&=\; \{[1 - h_A(ID_A, c_A)]I + [h_A(ID_A c_A)]H\}_A \\ &\otimes \{[1 - h_B(ID_B, c_B)]I + [h_B(ID_B, c_B)]H\}_B |\psi_i\rangle_2 \\ &=\; |\psi_i\rangle_1 \end{aligned}$$

where $|\psi_i\rangle$ is the state of the i-th GHZ particle and the subscript 1, 2, and 3 represents the three steps of authentication.

Next, Alice and Bob select some of the decoded qubits, make von-Neumann measurements on them, and compare the results through the public channel. If the error rate is higher than expected, then Alice and Bob abort the protocol. Otherwise they can confirm that the other party is legitimate and the channel is secure. They then execute the following key distribution procedures.

2.2 Key Distribution

Alice and Bob randomly make an operation either identity operation I or Hadamard operation H on the remaining GHZ particles. They keep the record of the operations which they made. For example, 0 represents I and 1 indicates H. After making unitary operations, Bob sends his encrypted GHZ particles to Alice. On receiving the qubits, Alice makes Bell measurements on pairs of particles consisting of her qubit and Bob's qubit. On the other hand, Trent measures his third qubit in the x basis and reveals the measurement outcomes. In this paper we use the following notations of Bell states.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}$$

Alice can infer Bob's unitary operations and sometimes discover the existence of Eve using the table [1]. For example, if Trent discloses $|+\rangle$, Alice chooses I operation and her Bell measurement result is $|\Phi^-\rangle$, then Alice can infer that Bob made a H operation and he sent 1. On the other hand, if Trent makes public $|+\rangle$, Alice makes I operation and obtains $|\Psi^-\rangle$, then Alice can detect an error.

Table 1. Operations on reversed GHZ states(i.e. $|\psi\rangle$) and published information

Operation		Transformation of GHZ states
Alice	Bob	after Alice's and Bob's operations
$I(0)$	$I(0)$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_a + \|\Phi^-\rangle_{AB}\|-\rangle_a)$
$I(0)$	$H(1)$	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_a + \|\Phi^-\rangle_{AB}\|+\rangle_a + \|\Psi^+\rangle_{AB}\|+\rangle_a + \|\Psi^-\rangle_{AB}\|-\rangle_a)$
$H(1)$	$I(0)$	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_a + \|\Phi^-\rangle_{AB}\|+\rangle_a + \|\Psi^+\rangle_{AB}\|+\rangle_a - \|\Psi^-\rangle_{AB}\|-\rangle_a)$
$H(1)$	$H(1)$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_a + \|\Psi^+\rangle_{AB}\|-\rangle_a)$

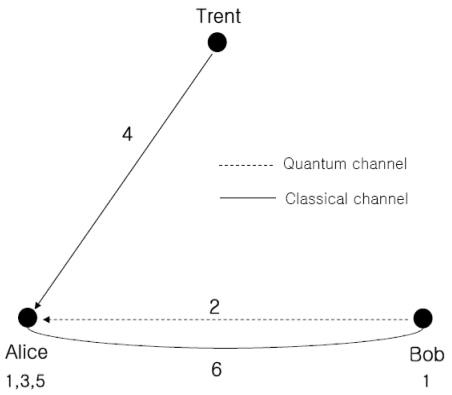

Fig. 2. Procedures of Key distribution 1. Alice and Bob make identity operations I (0) or Hadamard operations H (1) randomly on the remaining GHZ particles after authentication. 2. Bob sends his encoded particles to Alice. 3. Alice makes Bell measurements on pairs of particles consisting of her qubit and Bob's qubit. 4. The arbitrator measures his qubits in the x basis and publishes the results. 5. Alice infers Bob's operation using the table [1]. 6. Alice and Bob select check bits and compare them.

Alice and Bob compare some bits of their shared key (Bob's operation sequence). If the error rate is higher than the acceptable level, they throw away the shared sequence and restart the protocol. Otherwise they use the remaining sequences as a secret key. Usual error correction can be implemented to correct the remaining errors. Alice and Bob can reduce the Eve's knowledge of a shared key by standard privacy amplification[22, 23].

3 Security Analysis

In the assumption, user identity and a hash function are enrolled to Trent and the information is kept secret only between the owners and the arbitrator. Moreover Trent is supposed to be a honest person whom Alice and Bob can trust.

We first analyze the process of authentication. Suppose Eve intercepts the qubits heading to Alice or Bob and disguises her or him. Let Eve use the following unitary operation U_{AE} on Alice's and her qubit $|e\rangle$.

$$U_{AE}|0e\rangle_{AE} = \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E$$

$$U_{AE}|1e\rangle_{AE} = \beta'|0\rangle_A|e_{10}\rangle_E + \alpha'|1\rangle_A|e_{11}\rangle_E$$

where $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha'|^2 + |\beta'|^2 = 1$ and $\alpha\beta^* + \alpha'^*\beta' = 0$. If a bit of Alice's authentication key is 0 (1), the total states $|\xi_0\rangle$ (or $|\xi_1\rangle$) of system and Eve's

probe after Alice's and Bob's reverse operation is as follows.

$$|\xi_0\rangle = U_{AE}\{\frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})\}|e\rangle_E$$

$$= \frac{1}{\sqrt{2}}\{\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|100\rangle_{ATB}|e_{01}\rangle_E + \beta'|011\rangle_{ATB}|e_{10}\rangle_E + \alpha'|111\rangle_{ATB}|e_{11}\rangle_E\}$$

$$|\xi_1\rangle = H_A U_{AE}\{H_A\frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})\}|e\rangle_E$$

$$= \frac{1}{2\sqrt{2}}\{|000\rangle_{ATB}(\alpha|e_{00}\rangle_E + \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E + \alpha'|e_{11}\rangle_E) + |001\rangle_{ATB}(\alpha|e_{00}\rangle_E - \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E - \alpha'|e_{11}\rangle_E) + |110\rangle_{ATB}(\alpha|e_{00}\rangle_E + \beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E - \alpha'|e_{11}\rangle_E) + |111\rangle_{ATB}(\alpha|e_{00}\rangle_E - \beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E + \alpha'|e_{11}\rangle_E)\}$$

Eve can be detected with probability $\frac{1+\beta^2+\beta'^2}{4}$(when the probability of 0 and 1 in an authentication key is same) in the authentication phase. If the number of the check bits in the authentication process is c, then Alice and Bob can find out the existence of Eve with probability of $1 - (\frac{1+\alpha^2+\alpha'^2}{4})^c$. Eve is, therefore, always revealed if c is large enough. Hence if the authentication is passed, then Alice and Bob confirm the other party is the designated user.

Moreover, the original secret identities of users cannot be revealed even if Eve estimates some bits of the authentication key i.e. the hashed value. Eve can infer only some bits of the authentication key by checking bits in the authentication process. However Eve cannot reverse the hash function with partial information of the hashed value obtained from the checking bits in the authentication process. Besides Eve cannot infer the next authentication key since it is used only once and changed every time.

After authentication process, only Bob's qubits are transmitted. Eve will make operations on these qubits in key distribution phase. Suppose Eve use the above unitary operation U_{BE} on Bob's and her qubit $|E\rangle$. Then we can get the following states of total system composed by Alice, Bob, Trent and Eve. Equation (1) is derived from the situation when Alice and Bob choose I, equation (2) when they apply different unitary operations(H and I), and equation (3) is when they make H operations.

$$\begin{aligned}(1)\ \frac{1}{2\sqrt{2}}\Big[&|\Phi^+\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E) + |-\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E)\big\}\\ &+|\Phi^-\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E) + |-\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E)\big\}\\ &+|\Psi^+\rangle_{AB}\big\{|+\rangle_T(\beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E) + |-\rangle_T(\beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E)\big\}\\ &+|\Psi^-\rangle_{AB}\big\{|+\rangle_T(\beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E) + |-\rangle_T(\beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E)\big\}\Big]\end{aligned}$$

$$
\begin{aligned}
(2)\ \tfrac{1}{4}\Big[&|\Phi^+\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E + \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E) \\
&\quad + |-\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E \mp \beta|e_{01}\rangle_E \pm \beta'|e_{10}\rangle_E)\big\} \\
&+|\Phi^-\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E - \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E) \\
&\quad + |-\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E \pm \beta|e_{01}\rangle_E \pm \beta'|e_{10}\rangle_E)\big\} \\
&+|\Psi^+\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E + \beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E) \\
&\quad + |-\rangle_T(\mp\alpha|e_{00}\rangle_E \pm \alpha'|e_{11}\rangle_E + \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E)\big\} \\
&+|\Psi^-\rangle_{AB}\big\{|+\rangle_T(-\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E + \beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E) \\
&\quad + |-\rangle_T(\pm\alpha|e_{00}\rangle_E \pm \alpha'|e_{11}\rangle_E + \beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E)\big\}\Big]
\end{aligned}
$$

$$
\begin{aligned}
(3)\ \tfrac{1}{2\sqrt{2}}\Big[&|\Phi^+\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E) + |-\rangle_T(\beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E)\big\} \\
&+ |\Phi^-\rangle_{AB}\big\{|+\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E) - |-\rangle_T(\beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E)\big\} \\
&+ |\Psi^+\rangle_{AB}\big\{|+\rangle_T(\beta|e_{01}\rangle_E + \beta'|e_{10}\rangle_E) + |-\rangle_T(\alpha|e_{00}\rangle_E + \alpha'|e_{11}\rangle_E)\big\} \\
&+ |\Psi^-\rangle_{AB}\big\{|+\rangle_T(\beta|e_{01}\rangle_E - \beta'|e_{10}\rangle_E) - |-\rangle_T(\alpha|e_{00}\rangle_E - \alpha'|e_{11}\rangle_E)\big\}\Big]
\end{aligned}
$$

As shown in the above equations, Eve can be detected with probability $\frac{1}{2} + \frac{\beta^2+\beta'^2}{8}$ per check bit in the key distribution phase. Hence Eve can be detected with certainly if enough check bits are used in the key distribution. In this regard, Alice and Bob can identify and securely distribute a key with certainty using our protocol.

4 Conclusions

We propose a quantum key distribution protocol with quantum based user authentication. User authentication is executed without previously shared secret and by validating the correlation of GHZ states. A key can be securely distributed by using the remaining GHZ states after authentication. By the properties of the entanglement of GHZ states, even the trusted third party, Trent can not get out the distributed key. We expect our protocol can well be adjusted to be incorporated in future quantum networks.

We acknowledge helpful discussion with Andreas Poppe and Hannes Hübel. This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD)(KRF-2005-213-D00090).

References

1. C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York , 1984), p.175-179
2. Artur K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
3. Charles H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)
4. Charlse H. Bennett, Gilles Brassard and N. D. Mermin, Phys. Rev. Lett. 68, pp557-559 (1992)
5. Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter and Anton Zeilinger, Phys. Rev. Lett. 84 pp4729-4732 (2000)

6. R. Hughes, G. Morgan and C. Peterson, J. Modern Opt. 47, 533-547 (2000)
7. Nicolas Gisin, Gregoire Ribordy,Wolfgang Tittel and Hugo Zbinden , Reviews of Modern Physics vol 74 pp145 195 (2002)
8. P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441-444 (2000)
9. D. Mayers, quant-ph/9802025 (1998).
10. H.-K. Lo and H.F. Chau, Science 283, 2050-2056(1999); also quant-ph/9803006
11. M. Curty and D. J. Santos, Phys. Rev. A 64, 062309 (2001)
12. Bao-Sen Shi, Jian Li, Jin-Ming Liu,Xiao-Reng Fan, Guang-Can Guo , Physics letters A 281 83-87 (2001)
13. M. Curty, D. J. Santos, E. Perez, and P. Garcia-Fernandez, Phys. Rev. A 66, 022301 (2002)
14. C. Crepeau and L. Salvail, in Advances in Cryptology Springer-Verlag, Berlin, pp. 133 146 (1995)
15. M. Dusek, O. Haderka, M. Hendrych, and R. Myska, Phys. Rev. A 60, 149-156 (1999)
16. Guihua Zeng and Weiping Zhang, Phys. Rev. A vol 61, 022303 (2000)
17. T. Mihara , Phys. Rev. A 65, 052326 (2002)
18. D. Ljunggren, M. Bourennane, and A. Karlsson, Phys. Rev. A 62, 022305 (2000)
19. D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, American Journal of Physics 58, 1131 (1990)
20. Douglas R. Stinson CRYTPTOGARPHY Theory and Practice
21. RFC2459, X.509 Public Key Infrastructure Certificate and CRL Profile
22. Christian Cachin and Ueli M. Maurer, J. Cryptology(1997) 10; 97-110 (1997)
23. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden Reviews of Modern Physics 74, 145-195(2002)

arXiv:quant-ph/0512051 v1 6 Dec 2005

Quantum Direct Communication with Authentication

Hwayean Lee[1,2,4], Jongin Lim[1,2], HyungJin Yang[2,3]

Center for Information Security Technologies(CIST)[1],
Graduate School of Information Security(GSIS)[2]
Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
{hylee, jilim, yangh}@korea.ac.kr
Department of Physics, Korea University, Chochiwon, Choongnam, Korea[3]
Institut für Experimentalphysik, Universität Wien, Austria[4]
{hwayean.lee}@univie.ac.at,

Abstract. We propose two Quantum Direct Communication (QDC) protocols with user authentication. Users can identify each other by checking the correlation of Greenberger-Horne-Zeilinger (GHZ) states. Alice can directly send a secret message to Bob using the remaining GHZ states after authentication. Our second QDC protocol can be used even though there is no quantum link between Alice and Bob. The security of the transmitted message is guaranteed by properties of entanglement of GHZ states.
PACS : 03.67.Dd

1 Introduction

Quantum Cryptography utilizes the original characteristics of quantum mechanics such as superposition, entanglement and so on. Using these properties, some information can be secretly shared between users through a quantum channel. The information can be a key or a message. Quantum Key Distribution (QKD) protocols are used to share a key and Quantum Direct Communication (QDC) protocols are employed to send a message.

Many QKD protocols have been proposed since Bennett and Brassard first proposed a quantum key distribution protocol[1] in 1984. The security of some QKD protocols was theoretically proven in [2–4]. On the other hand, QDC starts to be researched nowadays. First QDC protocol was proposed by Beige et al.[5] in 2002. It was followed by other QDC protocols[6–10].

In most QDC protocols except two protocols proposed by Beige et al. [5] and Deng et al. [6], the receiver(Bob) must begin the protocol to get a secret message from the sender(Alice). For example Bob should generate single photons[7, 8] or Bell states[9] or qutrit states[10] and transmit all or some part of them to Alice. In addition, most QDC protocols are vulnerable to the man in the middle attack.

We propose two QDC protocols, which combine user authentication and direct communication in quantum world at first time. To authenticate users, an authentication method proposed in [11] is introduced. After authentication Alice

can send a secret message directly to Bob. This message may not be leaked to a third party. Moreover Alice and Bob can communicate without a quantum link between them in our second QDC protocol. We present our QDC protocols in the chapter 2, then analyze the security of them in chapter 3 and make conclusions in chapter 4.

2 Quantum Direct Communication Protocols

Our quantum direct communication protocols are composed of two parts: one is an authentication and the other a direct communication. The third party, Trent is introduced to authenticate the users participating in the communication. He is assumed to be more powerful than other users and he supplies the Greenberger-Horne -Zeilinger (GHZ) states[12].

2.1 Authentication

User's secret identity sequence and a one-way hash function are known to Trent. This information must be kept secret between the user and the arbitrator. Suppose Alice's(Bob's) identity sequence and her(his) one-way hash function are $ID_A(ID_B)$ and $h_A(h_B)$, respectively. For example, a one-way hash function is $h : \{0,1\}^* \times \{0,1\}^c \rightarrow \{0,1\}^l$, where * is arbitrary length, c the length of a counter and l a fixed number. Alice's(Bob's) authentication key shared with Trent can be calculated as $h_A(ID_A, c_A)\big(h_B(ID_B, c_B)\big)$, where $c_A(c_B)$ is the counter of calls on Alice's(Bob's) hash functions. Authentication keys are used to determine unitary operations on GHZ particles heading from the arbitrator to the owner. Users can authenticate each other by checking the correlation of the GHZ states taken the reverse unitary operations.

If Alice wants to send a secret message to Bob, she notifies this fact to Bob and Trent. On receiving the request, Trent generates N GHZ tripartite states $|\Psi\rangle = |\psi_1\rangle ... |\psi_N\rangle$. For simplicity the following GHZ state $|\psi_i\rangle$ is supposed to be prepared.

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$$

where the subscripts A, T and B correspond to Alice, Trent, and Bob, respectively. In this paper, we represent the z basis as $\{|0\rangle, |1\rangle\}$ and the x basis as $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Next, Trent encodes Alice's and Bob's particles of GHZ states with their authentication keys, $h_A(ID_A, c_A)$ and $h_B(ID_B, c_B)$, respectively. For example, if the ith value of $h_A(ID_A, c_A)$(or $h_B(ID_B, c_B)$) is 0, then Trent makes an identity operation I to Alice's (Bob's) particle of the ith GHZ state. If it is 1, Hadamard operation H is applied. If the authentication key $h_A(ID_A, c_A)$ (or $h_B(ID_B, c_B)$) does not have enough length to cover all GHZ particles, new authentication keys can be created by increasing the counter until the authentication keys shield all GHZ particles. After making operations on the GHZ particles, Trent distributes the states to Alice and Bob and keeps the remaining for him.

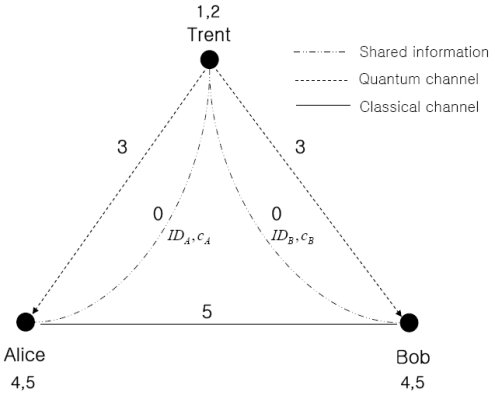

Fig. 1. Procedures of Authentication 0. Alice and Bob register their secret identity and hash functions to Trent, respectively. 1. Trent generates GHZ states $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$. 2. Trent makes unitary operations on $|\psi\rangle$ with Alice's and Bob's authentication key. 3. Trent distributes GHZ particles to Alice and Bob. 4. Alice and Bob make reverse unitary operations on their qubit with their authentication key, respectively. 5. Alice and Bob choose the position of a subset of GHZ states and make a local measurement in the z basis on them and compare the results.

On receiving the qubits, Alice and Bob decode the qubits with unitary transformations which are defined by their authentication keys, $h_A(ID_A, c_A)$ and $h_B(ID_B, c_B)$, respectively. Next, Alice and Bob select some of the decoded qubits, make von-Neumann measurements on them, and compare the results through the public channel. If the error rate is higher than expected, then Alice and Bob abort the protocol. Otherwise they can confirm that the other party is legitimate and the channel is secure. They then execute the following message transmission procedures.

2.2 Direct Communication Protocol 1

Alice selects a subset of GHZ states in the remaining sets after authentication and keeps it secret. Alice chooses a random sequence which has no connection with the secret message to transmit to Bob. Following this random sequence, Alice performs unitary transformations on the qubits selected for this check process. Before encoding the message and the random sequence, Alice can encode the secret message with a classical Error Correction Code (ECC) such as the Hamming Code, the Reed-Solomon code and the BCH code, so that Bob could be able to correct errors in the decoded message. For example, if the error rate of the quantum channel is 20% and the length of codeword is n, then any classical ECCs can be used, where the minimum length of the code d is larger than $\lfloor \frac{2n}{5} \rfloor + 1$. If the bit of the random sequence, or the message is 0, then Alice performs on her GHZ particle with Hadamard operation H. Otherwise, Alice

acts at her qubit with first Bit flip operation X and then Hadamard operation H. After making all unitary operations, Alice transfers all encoded qubits to Bob.

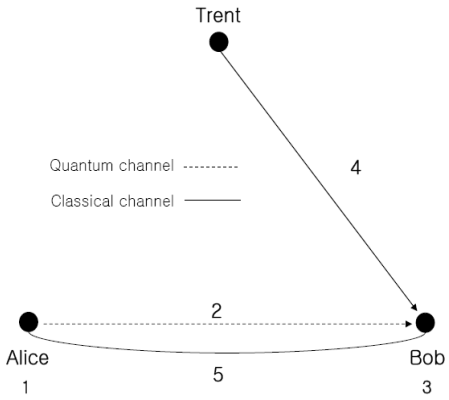

Fig. 2. Procedures of the first Direct Communication protocol 1. Alice chooses a subset of GHZ states and a random sequence. Alice performs unitary transformation both on the qubits selected for this check process following this random sequence and on the remaining qubits following the secret message. For example if the bit is 0, she makes a Hadamard operation H, otherwise a bit flip operation and a Hadamard operation HX. 2. Alice sends the qubits to Bob. 3. Bob makes Bell measurements on pairs of particles consisting of his qubits and Alice's qubit. 4. Trent makes von Neumann measurements on his GHZ particles and reveals the results. 5. Alice and Bob compare the check bits.

Bob makes Bell measurements on pairs of particles consisting of his qubit and Alice's qubit. In this paper we use the following notations of Bell states.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}$$

Trent measures his third qubit in the x basis and publishes the measurement outcomes. Bob recovers Alice's message using the table [1]. For example, if Bob measures $|\Phi^+\rangle$ and Trent reveals $|+\rangle$, then Bob can infer Alice made HX operation and she sent 1.

Table 1. Operations on the decrypted GHZ state(i.e. $|\psi\rangle$) and Transformation of the GHZ state

Alice's Operation	Transformation of GHZ states after Alice's operation
$H(0)$	$\frac{1}{2}\big(\|\Phi^+\rangle_{AB}\|-\rangle_T + \|\Phi^-\rangle_{AB}\|+\rangle_T + \|\Psi^+\rangle_{AB}\|+\rangle_T - \|\Psi^-\rangle_{AB}\|-\rangle_T\big)$
$HX(1)$	$\frac{1}{2}\big(\|\Phi^+\rangle_{AB}\|+\rangle_T + \|\Phi^-\rangle_{AB}\|-\rangle_T - \|\Psi^+\rangle_{AB}\|-\rangle_T + \|\Psi^-\rangle_{AB}\|+\rangle_T\big)$

After obtaining all messages, Bob notifies this fact to Alice. Alice reveals the position of the check bits and compares the bits with Bob. If the error rate is higher than expected, Alice and Bob conclude there was an eavesdropper. The message contains errors, but fortunately Eve cannot know its content. Otherwise Bob can extract the secret message from the remaining bits.

2.3 Direct Communication Protocol 2

The second QDC protocol is same as the first protocol except Alice sends her encoded qubits to the Trent. However it is not needed additional quantum link between Alice and Bob in this protocol. After making Bell measurement on his and Alice's qubits, Trent reveals the result. If $|\Phi^+\rangle$ or $|\Psi^-\rangle$, then Trent publishes 0. Otherwise he notifies 1. Bob measures his particles on the X basis. (This process of Bob can be preceded even before the Alice's operation.) Using the Trent's publication and his measurement, Bob can infer which operations were used by Alice as shown in the table [2]. If 0 is published and $|+\rangle$ is measured, Bob can discover Alice operated HX (1).

Table 2. Operations on the decrypted GHZ state(i.e. $|\psi\rangle$) and Transformation of the GHZ state

Alice's Operation	Transformation of GHZ states after Alice's operation
$H(0)$	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_B + \|\Phi^-\rangle_{AT}\|+\rangle_B + \|\Psi^+\rangle_{AT}\|+\rangle_B - \|\Psi^-\rangle_{AT}\|-\rangle_B)$
$HX(1)$	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|+\rangle_B + \|\Phi^-\rangle_{AT}\|-\rangle_B - \|\Psi^+\rangle_{AT}\|-\rangle_B + \|\Psi^-\rangle_{AT}\|+\rangle_B)$

Alice reveals the position of her check bits and compares them with Bob. If the error rate of the check bits is higher than expected, Bob throws away the message. Otherwise, Bob can get the whole secret by applying the classical ECC code used by Alice if it was used.

3 Security Analysis

The security of our protocol results from the properties of the entanglement of GHZ states. We first analyze the process of authentication. If Trent is honest,

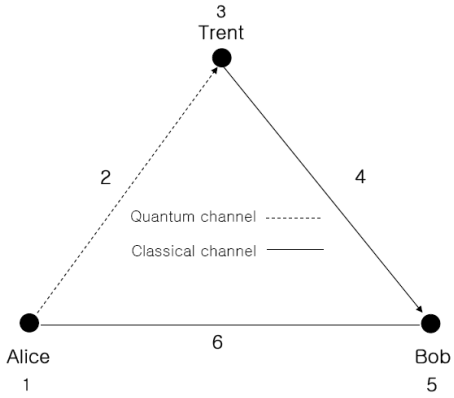

Fig. 3. Procedures of the second Direct Communication protocol 1. Alice chooses the position of check bits and a random sequence. Alice performs unitary transformation on the qubits selected for this check process following this random sequence and on the remaining qubits following the secret message. For example if the bit is 0, she makes a Hadamard operation H, otherwise a bit flip operation and a Hadamard operation HX. 2. Alice sends the encoded qubits to Trent. 3. Trent makes Bell measurements on pairs of particles consisting of his qubits and Alice's qubit. 4. Trent reveals the measurement outcomes. 5. Bob makes von Neumann measurements on his GHZ particles. 6. Alice and Bob compare the check bits.

then he will generate tripartite GHZ states, encrypt them with the right authentication keys and then distribute them to the designated users. Only the designated user can decrypt the qubits to recover the original GHZ states. This procedure can be written in the following form of a sequence of local unitary operation, the initial state:

$$|\psi_i\rangle_1 \;=\; \frac{1}{\sqrt{2}}(|000\rangle_{ATB} + |111\rangle_{ATB})$$

state after Trent's transformation

$$\begin{aligned} |\psi_i\rangle_2 \;&=\; \{[1 - f_A(ID_A, c_A)]I + [f_A(ID_A, c_A)]H\}_A \\ &\otimes \{[1 - f_B(ID_B, c_B)]I + [f_B(ID_B, c_B)]H\}_B |\psi_i\rangle_1 \end{aligned}$$

and finally the state after Alice's and Bob's local operations

$$\begin{aligned} |\psi_i\rangle_3 \;&=\; \{[1 - f_A(ID_A, c_A)]I + [f_A(ID_A c_A)]H\}_A \\ &\otimes \{[1 - f_B(ID_B, c_B)]I + [f_B(ID_B, c_B)]H\}_B |\psi_i\rangle_2 \\ &=\; |\psi_i\rangle_1 \end{aligned}$$

where $|\psi_i\rangle$ is the state of the i-th GHZ particle and the subscript 1, 2, and 3 represents the three steps of authentication. Of course, such is the situation

if there is no Eve. Suppose Eve intercepts the qubits heading to Alice or Bob and disguises her or him. Eve can be detected with probability 1/4 per check bits in this authentication process since she does not know Alice's or Bob's authentication key.

Let an attacker, Eve, use a coherent attack. She then causes errors per check bit with a probability 1/4 similarly to BB84 protocol if she uses the original bases used by Alice and Bob. It is because Eve didn't know the authentication key and she cannot decrypt the encoded qubits. For example, if the authentication key bit is 0, Eve doesn't make error in the qubit. Otherwise, an error occurs with probability 1/2. If Eve prepares $|0\rangle$ state and entangles with Alice's qubit, then the final state of the protocol qubit and Eve's qubit is after decoding by Alice and Bob as follows.

$|\psi'\rangle_{ATBE} = U_{AE}|\psi\rangle_{ATB} \otimes |0\rangle_E$
$= \frac{1}{2}\{|000\rangle_{ATB}|+\rangle_E + |100\rangle_{ATB}|-\rangle_E + |011\rangle_{ATB}|-\rangle_E + |111\rangle_{ATB}|+\rangle_E\}$

This is for a specific attack where $U_{AE}|0\rangle_A|0\rangle_E \rightarrow |0\rangle_A|0\rangle_E$ and $U_{AE}|1\rangle_A|0\rangle_E \rightarrow |1\rangle_A|1\rangle_E$. Eve can be detected with higher probability 1/2 per check bit in this case. Hence, if $m(\ll N)$ GHZ states are checked in the authentication process, Alice and Bob can confirm that the GHZ states are distributed to the legitimate users with probability $1 - (\frac{3}{4})^m$. We expect more advanced attack can be detected when m is increased.

After authentication process, only Alice's qubits are transmitted. Eve will make operations on these qubits in our quantum direct communication protocols. In both protocols, Eve must not be disclosed during the authentication process to obtain any information of secret message. Suppose Eve use the following unitary operation U_{AE} on Alice's and her qubit $|E\rangle$.

$$U_{AE}|0E\rangle_{AE} = \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E$$

$$U_{AE}|1E\rangle_{AE} = \beta'|0\rangle_A|e_{10}\rangle_E + \alpha'|1\rangle_A|e_{11}\rangle_E$$

where $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha'|^2 + |\beta'|^2 = 1$ and $\alpha\beta^* + \alpha'^*\beta' = 0$.

Then the state of the protocol is changed as follows.

1 The states after Alice made a unitary operation
$|\psi_1\rangle_{ATBE} = U_A|\psi\rangle_{ATB} \otimes |E\rangle_E$
$= \frac{1}{2}\big(|000\rangle_{ATB} \mp |100\rangle_{ATB} + |011\rangle_{ATB} \pm |111\rangle_{ATB}\big) \otimes |E\rangle_E$

2 The states after Eve made a unitary operation on her qubit and Alice's qubit heading to Bob or Trent
$|\psi_2\rangle_{ATBE} = U_{AE}|\psi_1\rangle_{ATBE}$
$= \frac{1}{2}\Big\{|000\rangle_{ATB}\big(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle\big)_E + |100\rangle_{ATB}\big(\beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle\big)_E$
$+ |011\rangle_{ATB}\big(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle\big)_E + |111\rangle_{ATB}\big(\beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle\big)_E\Big\}$
$= \frac{1}{2\sqrt{2}}\Big[\Phi^+_{AB}\Big\{|+\rangle_T\big(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle\big)_E$
$+ |-\rangle_T\big(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle\big)_E\Big\}$
$+ \Phi^-_{AB}\Big\{|+\rangle_T\big(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle\big)_E$

$$
\begin{aligned}
&\quad + |-\rangle_T \big(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle\big)_E \Big\} \\
&+ \Psi^+_{AB} \Big\{ |+\rangle_T \big(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle\big)_E \\
&\quad - |-\rangle_T \big(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle\big)_E \Big\} \\
&+ \Psi^-_{AB} \Big\{ |+\rangle_T \big(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle\big)_E \\
&\quad - |-\rangle_T \big(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle\big)_E \Big\} \Big]
\end{aligned}
$$

As shown in the above equations, Eve will introduce errors in the check bits with the probability of $1/2$ regardless of the order of measurement by Bob, Trent and Eve. Moreover, Eve cannot get any information from this attack since Eve cannot distinguish the two cases which Alice made operation H or HX. For example, suppose Alice makes operation $H(0)$, Bob measures $|\Psi^+\rangle$, and Eve measures $|e_{00}\rangle$. Then Trent will reveal $|+\rangle$ or $|-\rangle$ with equal probability. If Trent reveals $|+\rangle$ then Bob can revoke correct information. Otherwise Bob can find an error. Hence if the length of the check sequence is long enough, then we can find the existence of Eve in the transmission of message and confirm Eve does not intercept the message.

4 Conclusions

We have proposed two Authenticated Quantum Direct Communication protocols. After identifying the other user in the communication channel, Alice can directly send a secret message to Bob without a previously shared secret key. According to the existence of a quantum link between Alice and Bob, they can choose a QDC protocol between two. If there exists eavesdropping during transmission, the message will be broken and Alice and Bob can ascertain the existence of Eve by the check-bits. Though the message was broken, Eve cannot get any information of the secret message. We expect our schemes can be applied well to quantum networks even in a transition period.

Acknowledgement We thank Marek Zukowski, Andreas Poppe and Anton Zeilinger for useful discussions and comments. This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF-2005-213-D00090).

References

1. C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York , 1984), p.175-179
2. P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441-444 (2000).
3. D. Mayers, quant-ph/9802025 (1998).
4. H.-K. Lo and H.F. Chau, Science 283, 2050-2056 (1999); also quant-ph/9803006.
5. A. Beige, B. G. Englert, Ch. Kurstsiefer, and H. Weinfurter, Acta Physica Polonica A 101(3), 357-368 (2002), also available at quant-ph/0111106.

6. Fu-Guo Deng , Gui Lu Long, and Xiao-Shu Liu, Phys. Rev. A 68, 042317 (2003)
7. Fu-Guo Deng, and Gui Lu Long, Phys. Rev. A 69, 052319 (2004)
8. Marco Lucamarini and Stefano Mancini, Phys. Rev. Lett. 94, 140501 (2005)
9. Kim Bostroem and Timo Felbinger, Phys. Rev. Lett. vol 89, 187902 (2002)
10. Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long, PHYS. REV. A 71, 044305 (2005)
11. H. Lee, S. Lee, D. Lee, J. Lim, and H. Yang, arXiv:quant-ph/0510144 (2005)
12. D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, American Journal of Physics 58,1131(1990)

arXiv:quant-ph/0601194 v2 10 Feb 2006

Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping

Changho Hong[a], Jiin Kim[b], Hwayean Lee[a], and Hyungjin Yang[c,d]

[a]Center for Information Security Technologies(CIST),
Korea University, Seoul, South Korea
[b]Department of physics, Korea University, Seoul, South Korea
[c]Department of physics, Korea University, Chochiwon, Choongnam, South Korea
[d]Graduate School of Information Security(GSIS),
Korea University, 1, 5-ka, Anam-dong Sungbuk-ku, Seoul, South Korea
hchc@korea.ac.kr, jiinny@korea.ac.kr, hylee@cist.korea.ac.kr,
yangh@korea.ac.kr

Abstract. We present an Authenticated Multiuser Quantum Direct Communication(MQDC) protocol using entanglement swapping. Quantum direct communication is believed to be a safe way to send a secret message without quantum key distribution. The authentication process in our protocol allows only proper users to participate in communication. In this communication stage after the authentication, any two authorized users among n users can communicate each other even though there is no quantum communication channels between them. In the protocol, we need only n quantum communication channels between the authenticator and n users. It is similar to the present telephone system in which there are n communication channels between telephone company and users and any two designated users can communicate each other using telephone line through the telephone company. The securities of our protocols are analysed to be the same as those of other quantum key distribution protocols.

Introduction-One of the objects of quantum cryptography is to allow two distant parties to share a random bit sequence without any reveals to the eavesdropper. The Quantum Key Distribution(QKD) protocols are regarded as unconditionally secure cryptography schemes. The first Quantum key distribution was proposed by Bennett and Brassard. It is known as the BB84 protocol[1], and it uses four different non-orthogonal states of single photon. QKD establishes a common random key between two remote parties of communication. Afterwards these two parties can safely exchange a secret message over the public channel by encoding and decoding them with the distributed key. If the length of the keys is the same as the length of the messages, the communication is unconditional secure. It is because that one-time pad scheme with the enough length of secret key is proved to be unconditionally secure. QKD has progressed quickly since the first QKD protocol was designed[2,3,4,5]. QKD based on quantum mechanics is usually non-deterministic[1,2,3,4,5]. But it is sometimes deterministic[13,14,15], in which two remote parties get the same keys determinately.

A novel concept of quantum direct communication (QDC) has been proposed and pursued recently. Unlike QKD, QDC can directly send secret messages without creating the key to encrypt them. In 2002, Beige et al. presented the first QDC scheme,[6] in which messages can be read after the transmission of classical informations. Bostrom and Felbinger put forward a ping-ping scheme using entangled pair of qubits in 2002[7]. This protocol can be used for QKD as well as QDC. It is secure for key distribution, but is only quasisecure for QDC even if perfect quantum channel is used. Cai modified the ping-pong protocol by replacing the entanglement states with single photons in mixed state[16]. However it is unsafe in a noisy channel and disadvantaged to the opaque attack.

QDC may have wide application due to its fastness and unconditional security. Our QDC protocol uses entangled states and the entanglement swapping effect. It is well known that quantum entanglement swapping[8] can entangle two quantum systems which did not interact with each other before. But these QDC protocols have a common serious problem. If we don't check whether only proper users communicate each other, secret messages can be exposed to the eavesdropper. It is, thus, important to certify the identifies of the legitimate users in communication line so that no third party monitoring their identification can impersonate either of them. In our protocol, Alice (or Bob) can confirm the identification of her (or his) counterpart through the trusted third party, Trent, who acts a role of present telephone company. When one of them wants to communicate with the other, Trent guarantees the identification of each person to his(her) counterpart. Afterwards they directly communicate each other using quantum communication channels linking them and Trent.

Our authenticated multiuser QDC scheme using entanglement swapping consists of two parts; quantum authentication mode and quantum communication mode. After finishing authentication mode to identify each other, the messages are transmitted secretly and directly in communication mode.

Entanglement swapping-Let us first describe the quantum entanglement swapping. Let $|0\rangle$ and $|1\rangle$ be the horizontal and vertical polarization states of a photon, respectively. The four Bell states, $|\Phi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are maximally entangled states in two-photon Hilbert space. Let the initial state is $|\Phi_{12}^{+}\rangle \otimes |\Phi_{34}^{+}\rangle$. We can see that after the Bell measurements on the pair of photon 1 and 3 and the pair of photon 2 and 4, there is an explicit correspondence between the known initial state of the pair of two qubits and its swapped measurement outcomes. The state $|\Phi_{12}^{+}\rangle \otimes |\Phi_{34}^{+}\rangle$ can be rearranged as the linear combinations of the terms, $|\Phi_{13}^{+}\rangle \otimes |\Phi_{24}^{+}\rangle$, $|\Phi_{13}^{-}\rangle \otimes |\Phi_{24}^{-}\rangle$, $|\Psi_{13}^{+}\rangle \otimes |\Psi_{24}^{+}\rangle$ and $|\Psi_{13}^{-}\rangle \otimes |\Psi_{24}^{-}\rangle$. When the outcome of Bell measurement on the pair of photon 1 and 3 is $|\Phi_{13}^{-}\rangle$, the Bell state of the pair of photon 2 and 4 must be $|\Phi_{24}^{-}\rangle$. The outcome of entanglement swapping is summarized in Table 1.

In our protocol, every user sends Trent the secret identity sequence of N-bits. We call the Alice's(Bob's) secret identity as $ID(A)(ID(B))$. It must be kept safely between the user and Trent. Let us introduce the explicit algorithm for the protocol.

Quantum Authentication

Table 1. The outcomes of the swapped Bell measurement on the initially different combinations of four Bell states The abbreviation ID++ represents the set of four possible outcomes of Bell measurement,$(|\Phi_{14}^+\rangle, |\Phi_{23}^+\rangle)$,$(|\Phi_{14}^-\rangle, |\Phi_{23}^-\rangle)$,$(|\Psi_{14}^+\rangle, |\Psi_{23}^+\rangle)$, and $(|\Psi_{14}^-\rangle, |\Psi_{23}^-\rangle)$ with equal probability of 1/4. Similarly, the following cases can be obtained. $ID + - \Rightarrow \{(|\Psi_{14}^+\rangle, |\Psi_{23}^-\rangle)$,$(|\Phi_{14}^-\rangle, |\Phi_{23}^+\rangle)$,$(|\Phi_{14}^+\rangle, |\Phi_{23}^-\rangle)$,$(|\Psi_{14}^-\rangle, |\Psi_{23}^+\rangle)\}$, $Rev + + \Rightarrow \{(|\Phi_{14}^+\rangle, |\Psi_{23}^+\rangle)$,$(|\Phi_{14}^-\rangle, |\Psi_{23}^-\rangle)$,$(|\Psi_{14}^+\rangle, |\Phi_{23}^+\rangle)$,$(|\Psi_{14}^-\rangle, |\Phi_{23}^-\rangle)\}$, and $Rev + - \Rightarrow \{(|\Phi_{14}^+\rangle, |\Psi_{23}^-\rangle)$,$(|\Phi_{14}^-\rangle, |\Psi_{23}^+\rangle)$,$(|\Psi_{14}^+\rangle, |\Phi_{23}^-\rangle)$,$(|\Psi_{14}^-\rangle, |\Phi_{23}^+\rangle)\}$.

	$\|\Phi_{34}^+\rangle$	$\|\Phi_{34}^-\rangle$	$\|\Psi_{34}^+\rangle$	$\|\Psi_{34}^-\rangle$
$\|\Phi_{12}^+\rangle$	$ID++$	$ID+-$	$Rev++$	$Rev+-$
$\|\Phi_{12}^-\rangle$	$ID+-$	$ID++$	$Rev+-$	$Rev++$
$\|\Psi_{12}^+\rangle$	$Rev++$	$Rev+-$	$ID++$	$ID+-$
$\|\Psi_{12}^-\rangle$	$Rev+-$	$Rev++$	$ID+-$	$ID++$

(A.0) Authentication process begins when Alice asks Trent that she wants to communicate with Bob.

(A.1) Trent prepares an ordered set of $2N$ pairs of Bell state of $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We denote the $2N$ ordered EPR pairs as $[(P_1(T), P_1(A)), (P_2(T), P_2(A)),$ $...., (P_N(T), P_N(A))]$ and $[(P_{N+1}(T), P_{N+1}(B)), (P_{N+2}(T), P_{N+2}(B)), ..., (P_{2N}(T), P_{2N}(B$ Here the subscript indicates the ordering number of pairs, and T, A, and B represent the qubits of Trent, Alice and Bob, respectively.

(A.2) Trent takes one qubit from each EPR pair, say,$[P_1(T), P_2(T), ..., P_N(T)]$ $([P_{N+1}(T), P_{N+2}(T), ..., P_{2N}(T)])$ which is called the $A(B)$-checking sequence, and keep it safely. The remaining sequence of qubits $[P_1(A), P_2(A), ..., P_N(A)]$ $([P_{N+1}(B), P_{N+2}(B), ..., P_{2N}(B)])$ is called the $A(B)$-authentication sequence.

(A.3) Trent encodes $A(B)$-authentication sequence with Alice's(Bpb's) identification numbers $ID(A)$ $(ID(B))$. If the i-th value of $ID(A)$ is 1, Trent makes an Hadamard operation H to i-th qubit of $A(B)$-authentication sequence. If it is 0, identity operation I is applied. The results of the operation on $P_i(A)$ is $\{(1 - ID_i(A))I + ID_i(A)H\}P_i(A)$.

(A.4) Trent sends the $A(B)$-authentication sequences $[P_1(A), P_2(A), ..., P_N(A)]$, $([P_{N+1}(B), P_{N+2}(B), ..., P_{2N}(B)])$ to Alice(Bob).

(A.5) The legitimate user, Alice(Bob) knows her(his) ID sequence. She(he) decodes the $A(B)$-authentication sequence with her(his) ID sequence. The decoding method is the same as the Trent's encoding method. According to the ID sequence, Alice(Bob) makes an Hadamard operation H or does nothing to the qubits of $A(B)$-authentication sequence. By this decoding operation, the qubits are restored to their original state. Then she(he) measures her(his) sequence in the σ_z basis, and announces the outcomes.

(A.6) Trent measures the ordered $A(B)$-checking sequence and compare the results with the Alice's(Bob's) results. If Alice's(Bob's) result is the same as Trent's, then authentication succeeded. Otherwise, authentication failed and abort communication.

(C.1) Alice prepares a random sequence of $M+n+q$ Bell states from two states, $|\Phi^+\rangle_{T_A\,A} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\Psi^+\rangle_{T_A\,A} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.. This random choice is Alice's secret information. Bob prepares $M+n+q$ Bell states of $|\Phi^+\rangle_{T_B\,B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.. The subscripts of the states represents who is going to keep them after the process of (C.2).

(C.2) Alice(Bob) takes one qubit from each pair and sends Trent the ordered string of $M+n+q$ qubits which is named as the A-sequence(B-sequence) hereafter. Alice(Bob) stores the remaining ordered sequence of qubits in a safe place, which is named as *the encoding sequence* (*the decoding sequence*) hereafter.

(C.3) Alice randomly chooses n checking positions of the ordered encoding sequence and publicly announces it. Trent measures the n checking qubits of the ordered A-sequence by using σ_z basis and tells the outcomes to Alice. Alice measures the corresponding qubits of the encoding sequence by using σ_z basis and compares it with Trent's outcomes. She estimates error rate and can detect a eavesdropper. Bob's checking method is the same as that of Alice and Trent. They can detect eavesdropper on the channel of Alice-Trent or Bob-Trent.

(C.4) Trent performs Bell measurements on the qubits of the ordered A and B sequences. In this Bell measurement, Trent does not have to distinguish all of four different Bell states, but only needs to distinguish $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ states. After the Trent's measurement, the encoding sequence possessed by Alice and the decoding sequence possessed by Bob became to be entangled(Entanglement Swapping). Trent sends his measurement outcomes to Alice.

(C.5) Alice receives the Trent's outcome and measures the encoding sequence with σ_z basis. She randomly chooses q checking positions of the ordered encoding sequence and publicly announces the positions. Bob performs measurement on the corresponding q checking positions of the decoding sequence with σ_z basis and tells the outcome to Alice. Alice can infer Bob's measurement outcome from the effect of entanglement swapping, the information of Trent's measurement outcome, her initial Bell state and her measurement outcome. Alice compares her inference with Bob's corresponding announcements. If there is no eavesdropper on the line, their corresponding results should be correlated. If there is no correlation, the communication is aborted. Table 2 shows the correlations.

(C.6) According to Alice's bit strings, she publicly announces the positions that Bob needs to flip his measurement outcome on his decoding sequence. As she knows Bob's measurement outcome by using entanglement swapping effect, she can send decoding information to Bob. Bob flips the value of his measurement outcome of the position that Alice informed. Then he can decode the her secret message.

For example, let's suppose that Alice prepares the ordered set of Bell states $\{|\Phi^+\rangle, |\Phi^+\rangle, |\Psi^+\rangle\}$, and Trent's Bell measurement outcomes are $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Psi^+\rangle\}$.

Table 2. The correlation of entanglement swapping

Bob's initial state	Alice's initial state	Trent's Bell measurement outcome	Alice's outcome	Bob's outcome
$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	$\|\Phi^\pm\rangle$	0	0
			1	1
		$\|\Psi^\pm\rangle$	0	1
			1	0
	$\|\Psi^+\rangle$	$\|\Phi^\pm\rangle$	0	1
			1	0
		$\|\Psi^\pm\rangle$	0	0
			1	1

When Alice's measurement outcomes of the encoding sequence are {0, 0, 1}, Alice knows that Bob's outcomes must be {0, 1, 1}. Suppose that Alice's secret message bit is 101. According to the message, Alice publicly announces 110 which designates the positions Bob needs to flip his measurement outcome. After the flipping, Alice's message is transferred to Bob.

Security analysis - The proof of the security of our QDC protocol is based on the security of the transmission of the A- and B-sequence. The state of the transmitted qubits does not contain any information of the secret message because they are completely random and mixed. The exposed information is just random like that of coin flipping. In our protocol, even Trent can not know Alice's secret message since he doesn't know Alice's initial state.

The qubit transmission and the checking method in our protocol is similar to the procedure in BBM92 QKD protocol[10]. Alice stores the encoding-sequence in her safe place, and Eve cannot access it at all. Therefore, the security of our protocol is the same as that of the BBM92 QKD protocol. The proof of security for BBM92 protocol in ideal and practical conditions has been given [11,12]. So our protocol is also unconditionally secure.

Conclusion - We have established the authenticated quantum multiuser direct communication using entanglement swapping. Its security is the same as that of BBM92 protocol, which is unconditionally secure. The encoding of the message is processed only after the authentication of the users and the confirmation of the security of the quantum channel. Our protocol, therefore, is not in danger of exposure of information to Eve. Furthermore the leaked information to Eve is totally random, and does not contain any information.

In this protocol we need only EPR paris. It can be advantage in an experiment. The great feature of our protocol is that any two users among n subscribers can communicate each other. We don't need any quantum channel linking two users, because the center, Trent, connects two users Alice and Bob, and authenticates them. This structure is the same as that of nowadays telephone system, but its security is much better than present technology. It is unconditionally secure. Our scheme may be used for the safe communication system.

References

1. C.H.Bennett and G.Brassard, *in Proceedings of IEEE international Conference on Computers*, System and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175-179.
2. A.K.Ekert, Phys. Rev. Lett. 67, 661, (1991).
3. C.H.Bennett, Phys. Rev. Lett. 68, 3121 (1992).
4. L.Goldenberg and L.Vaidman, Phys. Rev. Lett. 75, 1239 (1995).
5. M.Ardehali, H.F.Chau, and H.-K.Lo, e-print quant-ph/9803007.
6. A.Beige, B.-G.Englert, Ch.Kurtsiefer, and H.Weinfurter, Acta Phys. Pol. A 101, 357(2002).
7. K.Bostrom and T.Felbinger, Phys. Rev. Lett. 89, 187902 (2002).
8. M.Zukowski, A.Zeilinger, M.A.Horne, and A.K.Ekert, *Event-ready-detectors Bell experiment via entanglement swapping*,Phys. Rev. Lett. 71, 4287 (1993).
9. Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu, Phys. Rev. A , 68, 04231 (2003).
10. C.H.Bennett, G,Brassard, and N.D.Mermin, Phys. Rev. Lett. 557 (1992).
11. H.Inamori, L.Rallan, and V.Vedral, J.Phys. A 34, 6913 (2001).
12. E.Waks, A.Zeevi, and Y.Yamamoto, Phys. Rev. A 65 052310 (2002).
13. M.Koashi and N.Imoto, Phys. Rev. Lett. 79, 2383 (1997).
14. C.H.Bennett and S.J. Wisner, Phys. Rev. Lett. 69, 2881 (1992).
15. W.Y.Hwang, I.G.Koh, and Y.D, Han, Phys. Lett. A 244, 489 (1998).
16. Q.Y.Cai, quant-ph/0304033.

Appendix C

Derivation of Tables

C.1 Authenticated MQKD

C.1.1 Protocol 1 (tab. 4.1, p. 28)

The original state of the system is $|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$. After her and Bob's transformations Alice measures her and Bob's qubit in the Bell basis. Trent measures his particle in the x basis.

1st row of tab. 4.1: Alice and Bob both perform an identity transformations (I) on their respective qubit.

$$
\begin{aligned}
I_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{\sqrt{2}}\left(|00\rangle_{AB}|0\rangle_T + |11\rangle_{AB}|1\rangle_T\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{AB}|+\rangle_T + |\Phi^-\rangle_{AB}|-\rangle_T\right)
\end{aligned}
$$

2nd row of tab. 4.1: Alice performs an identity operation (I) and Bob a Hadamard transformation (H) on their respective qubit.

$$
\begin{aligned}
I_A H_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|00\rangle_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + |11\rangle_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2}\left(|000\rangle + |001\rangle + |110\rangle - |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2}\left((|00\rangle + |01\rangle)_{AB}|0\rangle_T + (|10\rangle - |11\rangle)_{AB}|1\rangle_T\right) \\
= \quad & \frac{1}{4}\left((|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{AB}(|0\rangle + |1\rangle)_T + (|00\rangle + |01\rangle - |10\rangle + |11\rangle)_{AB}(|0\rangle - |1\rangle)_T\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \\
& \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T\Bigg) \\
= \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AB}|-\rangle_T + |\Phi^-\rangle_{AB}|+\rangle_T + |\Psi^+\rangle_{AB}|+\rangle_T + |\Psi^-\rangle_{AB}|-\rangle_T\right)
\end{aligned}
$$

3rd row of tab. 4.1: Alice performs a Hadamard operation (H) and Bob an identity transformation (I) on their respective qubit.

$$
\begin{aligned}
H_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|00\rangle_{TB} + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|11\rangle_{TB}\right) \\
= \quad & \frac{1}{2}\left(|000\rangle + |100\rangle + |011\rangle - |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2}\left((|00\rangle + |10\rangle)_{AB}|0\rangle_T + (|01\rangle - |11\rangle)_{AB}|1\rangle_T\right) \\
= \quad & \frac{1}{4}\left((|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{AB}(|0\rangle + |1\rangle)_T + (|00\rangle + |10\rangle - |01\rangle + |11\rangle)_{AB}(|0\rangle - |1\rangle)_T\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \\
& \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T - \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T\Bigg) \\
= \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AB}|-\rangle_T + |\Phi^-\rangle_{AB}|+\rangle_T + |\Psi^+\rangle_{AB}|+\rangle_T - |\Psi^-\rangle_{AB}|-\rangle_T\right)
\end{aligned}
$$

4th row of tab. 4.1: Alice and Bob both perform a Hadamard transformation (H) on their respective qubit.

$$
\begin{aligned}
H_A H_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|0\rangle_T\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|1\rangle_T\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2\sqrt{2}}\left(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2\sqrt{2}}\left((|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{AB}|0\rangle_T + (|00\rangle - |01\rangle - |10\rangle + |11\rangle)_{AB}|1\rangle_T\right) \\
= \quad & \frac{1}{4\sqrt{2}}\left(\,2\,(|00\rangle + |11\rangle)_{AB}(|0\rangle + |1\rangle)_T + 2\,(|01\rangle + |10\rangle)_{AB}(|0\rangle - |1\rangle)_T\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{AB}|+\rangle_T + |\Psi^+\rangle_{AB}|-\rangle_T\right)
\end{aligned}
$$

C.1.2 Improved Proposal 1 (tab. 4.6, p. 41)

The original state of the system is $|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$.

1st subset in tab. 4.6: Trent measures his and Bob's particle in the Bell basis. Alice measures her (untransformed) particle in the x basis.

a) Bob performs an identity operation on his B-qubit.

$$
\begin{aligned}
I_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{\sqrt{2}}\left(|00\rangle_{TB}|0\rangle_A + |11\rangle_{TB}|1\rangle_A\right) \\
= \quad & \frac{1}{2\sqrt{2}}\left((|00\rangle + |11\rangle)_{TB}(|0\rangle + |1\rangle)_A + (|00\rangle - |11\rangle)_{TB}(|0\rangle - |1\rangle)_A\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{TB}|+\rangle_A + |\Phi^-\rangle_{TB}|-\rangle_A\right)
\end{aligned}
$$

b) Bob performs a Hadamard operation on his B-qubit.

$$
\begin{aligned}
I_A H_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|00\rangle_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + |11\rangle_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2}\left(|000\rangle + |001\rangle + |110\rangle - |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2}\left((|00\rangle + |01\rangle)_{TB}|0\rangle_A + (|10\rangle - |11\rangle)_{TB}|1\rangle_A\right) \\
= \quad & \frac{1}{4}\left((|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{TB}(|0\rangle + |1\rangle)_A + (|00\rangle + |01\rangle - |10\rangle + |11\rangle)_{TB}(|0\rangle - |1\rangle)_A\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A + \\
& \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{TB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A\Bigg) \\
= \quad & \frac{1}{2}\left(|\Phi^+\rangle_{TB}|-\rangle_A + |\Phi^-\rangle_{TB}|+\rangle_A + |\Psi^+\rangle_{TB}|+\rangle_A + |\Psi^-\rangle_{TB}|-\rangle_A\right)
\end{aligned}
$$

2nd subset in tab. 4.6: Trent measures Alice's and his particle in the Bell basis. Bob measures his (untransformed) particle in the x basis.

c) Alice performs an identity operation on her A-qubit.

$$
\begin{aligned}
I_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{\sqrt{2}}\left(|00\rangle_{AT}|0\rangle_B + |11\rangle_{AT}|1\rangle_B\right) \\
= \quad & \frac{1}{2\sqrt{2}}\left((|00\rangle + |11\rangle)_{AT}(|0\rangle + |1\rangle)_B + (|00\rangle - |11\rangle)_{AT}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{AT}|+\rangle_B + |\Phi^-\rangle_{AT}|-\rangle_B\right)
\end{aligned}
$$

d) Alice performs a Hadamard operation on her A-qubit.

$$
\begin{aligned}
H_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|00\rangle_{TB} + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|11\rangle_{TB}\right) \\
= \quad & \frac{1}{2}\left(|000\rangle + |100\rangle + |011\rangle - |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2}\left((|00\rangle + |10\rangle)_{AT}|0\rangle_B + (|01\rangle - |11\rangle)_{AT}|1\rangle_B\right) \\
= \quad & \frac{1}{4}\left((|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{AT}(|0\rangle + |1\rangle)_B + (|00\rangle + |10\rangle - |01\rangle + |11\rangle)_{AT}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B) + \\
& \qquad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B - \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\Bigg) \\
= \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AT}|-\rangle_B + |\Phi^-\rangle_{AT}|+\rangle_B + |\Psi^+\rangle_{AT}|+\rangle_B - |\Psi^-\rangle_{AT}|-\rangle_B\right)
\end{aligned}
$$

C.2 Authenticated MQDC

C.2.1 Protocol 2 (tab. 5.1, p. 47)

The original state of the system is $|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$. After Alice's transformation, Trent measures her and his qubit in the Bell basis. Bob measures his particle in the x basis.

1st row of tab. 5.1: Alice performs a Hadamard transformation (H) on her qubit.

$$
\begin{aligned}
H_A \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|00\rangle_{TB} + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|11\rangle_{TB}\right) \\
= \quad & \frac{1}{2}\left(|000\rangle + |100\rangle + |011\rangle - |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2}\left((|00\rangle + |10\rangle)_{AT}|0\rangle_B + (|01\rangle - |11\rangle)_{AT}|1\rangle_B\right) \\
= \quad & \frac{1}{4}\left((|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{AT}(|0\rangle + |1\rangle_B) + (|00\rangle + |10\rangle - |01\rangle + |11\rangle)_{AT}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \\
& \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B - \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\Bigg) \\
= \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AT}|-\rangle_B + |\Phi^-\rangle_{AT}|+\rangle_B + |\Psi^+\rangle_{AT}|+\rangle_B - |\Psi^-\rangle_{AT}|-\rangle_B\right)
\end{aligned}
$$

2nd row of tab. 5.1: Alice flips her qubit before performing a Hadamard transformation on it (HX).

$$
\begin{aligned}
H_A X_A \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\
= \quad & H_A \left(\frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{ATB}\right) \\
= \quad & \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A |00\rangle_{TB} + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A |11\rangle_{TB}\right) \\
= \quad & \frac{1}{2} \left(|000\rangle - |100\rangle + |011\rangle + |111\rangle\right)_{ATB} \\
= \quad & \frac{1}{2} \left((|00\rangle - |10\rangle)_{AT} |0\rangle_B + (|01\rangle + |11\rangle)_{AT} |1\rangle_B\right) \\
= \quad & \frac{1}{4} \left((|00\rangle - |10\rangle + |01\rangle + |11\rangle)_{AT}(|0\rangle + |1\rangle_B) + (|00\rangle - |10\rangle - |01\rangle - |11\rangle)_{AT}(|0\rangle - |1\rangle)_B\right) \\
= \quad & \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B + \\
& \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B - \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AT}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_B\Bigg) \\
= \quad & \frac{1}{2} \left(|\Phi^+\rangle_{AT} |+\rangle_B + |\Phi^-\rangle_{AT} |-\rangle_B - |\Psi^+\rangle_{AT} |-\rangle_B + |\Psi^-\rangle_{AT} |+\rangle_B\right)
\end{aligned}
$$

C.2.2 Improved Proposal 2 (tab. 5.4, p. 56)

The original state of the system is $|\theta_i\rangle_{ATB} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$. After Alice's transformation, Trent measures her and his qubit in the Bell basis. Bob measures his particle in the x basis.

1st row of tab. 5.4: Alice performs a Hadamard transformation (H) on her qubit (see C.2.1 for details).

$$\begin{aligned} & H_A \quad \left(\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ATB}\right) \\ = \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AT}|-\rangle_B + |\Phi^-\rangle_{AT}|+\rangle_B + |\Psi^+\rangle_{AT}|+\rangle_B - |\Psi^-\rangle_{AT}|-\rangle_B\right) \end{aligned}$$

2nd row of tab. 5.4: Alice makes a Pauli-Z operation before performing Hadamard transformation ($H\sigma_z$).

$$\begin{aligned} & H_A\sigma_{zA} \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\ = \quad & H_A\left(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ATB}\right) \\ = \quad & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A|00\rangle_{TB} - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_A|11\rangle_{TB}\right) \\ = \quad & \frac{1}{2}\left(|000\rangle + |100\rangle - |011\rangle + |111\rangle\right)_{ATB} \\ = \quad & \frac{1}{2}\left((|00\rangle + |10\rangle)_{AT}|0\rangle_B + (-|01\rangle + |11\rangle)_{AT}|1\rangle_B\right) \\ = \quad & \frac{1}{4}\left((|00\rangle + |10\rangle - |01\rangle + |11\rangle)_{AT}(|0\rangle + |1\rangle_B) + (|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{AT}(|0\rangle - |1\rangle)_B\right) \\ = \quad & \frac{1}{2}\left(|\Phi^+\rangle_{AT}|+\rangle_B + |\Phi^-\rangle_{AT}|-\rangle_B + |\Psi^+\rangle_{AT}|-\rangle_B - |\Psi^-\rangle_{AT}|+\rangle_B\right) \end{aligned}$$

C.3 Authenticated MQDC with ES

C.3.1 Protocol 3 (tab. 6.1, p. 60)

Alice's initial Bell states are $|\phi^+\rangle_{T_AA}$ and $|\psi^+\rangle_{T_AA}$. Bob's initial state is $|\phi^+\rangle_{T_BB}$. Trent performs entanglement swapping from entanglement of the T_A- and A-particles and the T_B- and B-particles to the A- and B-qubits by projecting the T_A- and T_B-particles onto the Bell basis. Subsequently, Alice and Bob measure the A- and B-qubits in the z basis.

1st – 4th row of tab. 6.1: Alice's initial Bell state is $|\phi^+\rangle_{T_AA}$.

$$
\begin{aligned}
&|\phi^+\rangle_{T_AA} \otimes |\phi^+\rangle_{T_BB} \\
&= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{T_AA} \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{T_BB} \\
&= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)_{T_AAT_BB} \\
&= \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right)_{T_AT_BAB} \\
&= \frac{1}{4}\big(|00\rangle_{T_AT_B}|0\rangle_A|0\rangle_B + |01\rangle_{T_AT_B}|0\rangle_A|1\rangle_B + |10\rangle_{T_AT_B}|1\rangle_A|0\rangle_B + |11\rangle_{T_AT_B}|1\rangle_A|1\rangle_B + \\
&\qquad |00\rangle_{T_AT_B}|0\rangle_A|0\rangle_B + |01\rangle_{T_AT_B}|0\rangle_A|1\rangle_B + |10\rangle_{T_AT_B}|1\rangle_A|0\rangle_B + |11\rangle_{T_AT_B}|1\rangle_A|1\rangle_B\big) \\
&= \frac{1}{2\sqrt{2}}\big(|\Phi^+\rangle_{T_AT_B}|00\rangle_{AB} + |\Phi^+\rangle_{T_AT_B}|11\rangle_{AB} + |\Phi^-\rangle_{T_AT_B}|00\rangle_{AB} - |\Phi^-\rangle_{T_AT_B}|11\rangle_{AB} + \\
&\qquad |\Psi^+\rangle_{T_AT_B}|01\rangle_{AB} + |\Psi^+\rangle_{T_AT_B}|10\rangle_{AB} + |\Psi^-\rangle_{T_AT_B}|01\rangle_{AB} - |\Psi^-\rangle_{T_AT_B}|10\rangle_{AB}\big) \\
&= \frac{1}{2\sqrt{2}}\left(|\Phi^\pm\rangle_{T_AT_B}|00\rangle_{AB} \mp |\Phi^\pm\rangle_{T_AT_B}|11\rangle_{AB} + |\Psi^\pm\rangle_{T_AT_B}|01\rangle_{AB} \mp |\Psi^\pm\rangle_{T_AT_B}|10\rangle_{AB}\right)
\end{aligned}
$$

5th – 8th row of tab. 6.1: Alice's initial Bell state is $|\psi^+\rangle_{T_AA}$.

$$
\begin{aligned}
&|\psi^+\rangle_{T_AA} \otimes |\phi^+\rangle_{T_BB} \\
&= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_AA} \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \\
&= \frac{1}{2}\left(|0100\rangle + |0111\rangle + |1000\rangle + |1011\rangle\right)_{T_AAT_BB} \\
&= \frac{1}{2}\left(|0010\rangle + |0111\rangle + |1000\rangle + |1101\rangle\right)_{T_AT_BAB} \\
&= \frac{1}{4}\big(|00\rangle_{T_AT_B}|1\rangle_A|0\rangle_B + |01\rangle_{T_AT_B}|1\rangle_A|1\rangle_B + |10\rangle_{T_AT_B}|0\rangle_A|0\rangle_B + |11\rangle_{T_AT_B}|0\rangle_A|1\rangle_B + \\
&\qquad |00\rangle_{T_AT_B}|1\rangle_A|0\rangle_B + |01\rangle_{T_AT_B}|1\rangle_A|1\rangle_B + |10\rangle_{T_AT_B}|0\rangle_A|0\rangle_B + |11\rangle_{T_AT_B}|0\rangle_A|1\rangle_B\big) \\
&= \frac{1}{2\sqrt{2}}\big(|\Phi^+\rangle_{T_AT_B}|01\rangle_{AB} + |\Phi^+\rangle_{T_AT_B}|10\rangle_{AB} - |\Phi^-\rangle_{T_AT_B}|01\rangle_{AB} + |\Phi^-\rangle_{T_AT_B}|10\rangle_{AB} + \\
&\qquad |\Psi^+\rangle_{T_AT_B}|00\rangle_{AB} + |\Psi^+\rangle_{T_AT_B}|11\rangle_{AB} - |\Psi^-\rangle_{T_AT_B}|00\rangle_{AB} + |\Psi^-\rangle_{T_AT_B}|11\rangle_{AB}\big) \\
&= \frac{1}{2\sqrt{2}}\left(\mp|\Phi^\pm\rangle_{T_AT_B}|01\rangle_{AB} + |\Phi^\pm\rangle_{T_AT_B}|10\rangle_{AB} \mp |\Psi^\pm\rangle_{T_AT_B}|00\rangle_{AB} + |\Psi^\pm\rangle_{T_AT_B}|11\rangle_{AB}\right)
\end{aligned}
$$

C.3.2 Improved Proposal 4 (tab. 6.3, p. 76)

$$
\begin{aligned}
&|\Phi^+\rangle_{T_AA} \otimes |\Phi^+\rangle_{T_BB} \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \\
&= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)_{T_AAT_BB} \\
&= \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right)_{T_AT_BAB} \\
&= \frac{1}{4}\Big((|000\rangle + |101\rangle + |010\rangle + |111\rangle)_{T_AT_BA}(|0\rangle + |1\rangle)_B \\
&\qquad (|000\rangle + |101\rangle - |010\rangle - |111\rangle)_{T_AT_B}(|0\rangle - |1\rangle)_B \Big) \\
&= \frac{1}{8}\Big((|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{T_AT_B}(|0\rangle + |1\rangle)_A(|0\rangle + |1\rangle)_B \\
&\qquad (|00\rangle + |01\rangle - |10\rangle - |11\rangle)_{T_AT_B}(|0\rangle - |1\rangle)_A(|0\rangle + |1\rangle)_B \\
&\qquad (|00\rangle - |01\rangle + |10\rangle - |11\rangle)_{T_AT_B}(|0\rangle + |1\rangle)_A(|0\rangle - |1\rangle)_B \\
&\qquad (|00\rangle - |01\rangle - |10\rangle + |11\rangle)_{T_AT_B}(|0\rangle - |1\rangle)_A(|0\rangle - |1\rangle)_B \Big) \\
&= \frac{1}{2\sqrt{2}}\Big((|\Phi^+\rangle_{T_AT_B} + |\Psi^+\rangle_{T_AT_B})|+\rangle_A|+\rangle_B + \\
&\qquad (|\Phi^-\rangle_{T_AT_B} + |\Psi^-\rangle_{T_AT_B})|-\rangle_A|+\rangle_B + \\
&\qquad (|\Phi^-\rangle_{T_AT_B} - |\Psi^-\rangle_{T_AT_B})|+\rangle_A|-\rangle_B + \\
&\qquad (|\Phi^+\rangle_{T_AT_B} - |\Psi^+\rangle_{T_AT_B})|-\rangle_A|-\rangle_B \Big)
\end{aligned}
$$

Appendix D

Security Results: Protocol 1

All derivations refer to the security analysis of protocol 1 (s. 4.3, pp. 29).

D.1 Eavesdropping of Trent (s. 4.3.1, p. 29)

After Alice's and Bob's transformations, the original state $|\theta_i\rangle_{ATB}$ changes to one of the states (1) – (4). Assuming that Alice and Bob perform the operations perfectly random, each state occurs with probability $\rho_O = \frac{1}{4}$.

$$I_A I_B(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \quad (1)$$

$$I_A H_B(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATB} \quad (2)$$

$$H_A I_B(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \quad (3)$$

$$H_A H_B(|\theta_i\rangle_{ATB}) = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{ATB} \quad (4)$$

With states (1) and (3) Trent always receives the same measurement outcomes for his and Bob's qubit, that is with the probability of 1. For each state (2) and (4) he obtains the same results with the probability of $\frac{1}{2}$.

$$\rho_O\ (same\ results) = \frac{1}{4} * \left(1 + \frac{1}{2} + 1 + \frac{1}{2}\right) = \frac{3}{4} \quad (5)$$

$$\rho_O\ (different\ results) = \frac{1}{4} * \left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{4} \quad (6)$$

Different results only occur in case of H_B. With same outcomes Trent can be sure that Bob's operation was I_B with the probability of $\frac{2}{3}$.

$$\rho_O(I_B) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \quad (eqs.\ (1)\ and\ (3)) \tag{7}$$

$$\rho_O(same\ results) = \frac{3}{4} \to 1\ or\ 100\% \quad (eq.\ (5)) \tag{8}$$

$$\rho(I_B) = \frac{2}{4} \to \frac{2}{3}\ or\ 66,\overline{6}\% \quad (eqs.\ (7)\ and\ (8)) \tag{9}$$

Trent's intermediate step causes errors. For instance, if the system is in state (1) and Trent measures $|0\rangle_T|0\rangle_B$, he resends a new prepared state $|0\rangle_b$ to Alice. Alice's own particle collapses to the fixed state $|0\rangle_A$ due to Trent's measurement. Thus, Alice following Bell basis measurement may not get a valid input (eq. (10)). Additionally, Trent can neither infer nor measure a correct x basis measurement result anymore and his outcome is random.

$$|0\rangle_A \otimes |0\rangle_b = |00\rangle_{Ab} \tag{10}$$

D.2 Eavesdropping on Authentication (s. 4.3.2, p. 30)

Impersonation Attack

After Eve's encoding and Alice's decoding operations on the A-qubit the system changes to one of the states (11) – (14) with Eve guessing Alice's authentication key (option 2). If Eve leaves Alice's particles unencoded (option 1), only states (11) and (12) must be considered. The system transformations for Bob's B-qubit can equally be derived.

$$I_{E(T)}I_A(|\theta_i\rangle_{AE(T)B}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{11}$$

$$I_{E(T)}H_A(|\theta_i\rangle_{AE(T)B}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{12}$$

$$H_{E(T)}I_A(|\theta_i\rangle_{AE(T)B}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{13}$$

$$H_{E(T)}H_A(|\theta_i\rangle_{AE(T)B}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{14}$$

An error is introduced with probability $\frac{1}{4}$ for both options 1 and 2.

$$\rho_{opt1}(error) = \frac{1}{2} * (2 * \frac{1}{4}) = \frac{1}{4} \tag{15}$$

$$\rho_{opt2}(error) = \frac{1}{4} * (2 * \frac{1}{4} + 2 * \frac{1}{4}) = \frac{1}{4} \tag{16}$$

In case of option 2, table D.1 (p. D3) shows the possible cases of system changes according to eqs. (17) – (20) after the entire coding process. To analyse option 1 only the first four rows of the table must be considered.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{17}$$

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{18}$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{19}$$

$$\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - 011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{20}$$

Only eq. (17) represents the system correctly, whereas the detection probability is $\frac{1}{2}$ in each eq. (18) – (20). That leads to an overall detection probability of $\frac{3}{8}$ per check qubit.

$$\rho_D(option\ 1) \;=\; 3\ (false\ cases)\ *\frac{1}{4}\ (\rho_O\ each\ case)\ *\frac{1}{2}\ (\rho_D\ per\ case) = \frac{3}{8} \tag{21}$$

$$\rho_D(option\ 2) \;=\; 12\ (false\ cases)\ *\frac{1}{16}\ (\rho_O\ each\ case)\ *\frac{1}{2}\ (\rho_D\ per\ case) = \frac{3}{8} \tag{22}$$

Eve's operation on Alice's qubit	Eve's operation on Bob's qubit	Alice's operation	Bob's operation	System changes to equation
$I_{E(T)}$	$I_{E(T)}$	I_A	I_B	(17)
		I_A	H_B	(18)
		H_A	I_B	(19)
		H_A	H_B	(20)
$I_{E(T)}$	$H_{E(T)}$	I_A	I_B	(18)
		I_A	H_B	(17)
		H_A	I_B	(20)
		H_A	H_B	(19)
$H_{E(T)}$	$I_{E(T)}$	I_A	I_B	(19)
		I_A	H_B	(20)
		H_A	I_B	(17)
		H_A	H_B	(18)
$H_{E(T)}$	$H_{E(T)}$	I_A	I_B	(20)
		I_A	H_B	(19)
		H_A	I_B	(18)
		H_A	H_B	(17)

Table D.1: Cases of System Changes

Table D.2 (p. D4) presents Eve's chances to gain the key value. Eve derives Alice's operation H_A with the probability of $\rho_S(H_A) = \frac{3}{16}$. The probability $\rho_S(H_B)$, with which Eve deduces H_B, has the same value. If Eve's result differs from Alice's and Bob's outcomes, Eve can deduce both operations. That occurs for Eve's wrong guess of both authentication key values with the probability $\rho_S(H_AH_B) = \frac{1}{16}$.

$$\rho_S(H_A) = 2 * \frac{3}{32} = \frac{3}{16} \quad (23)$$

$$\rho_S(H_B) = 2 * \frac{3}{32} = \frac{3}{16} \quad (24)$$

$$\rho_S(H_A H_B) = 2 * \frac{1}{32} = \frac{1}{16} \quad (25)$$

$$\rho_{\overline{S}} = 2 * \frac{9}{32} = \frac{9}{16} \quad (26)$$

Measurement result of Alice	Eve	Bob	Possible operations	Eve's derivation	ρ_O	Eq.
0	0	0	all	-	9/32	(17) - (20)
0	0	1	$I_A H_B$ or $H_A H_B$	H_B	3/32	(18),(20)
0	1	0	$H_A H_B$	H_A and H_B	1/32	(20)
0	1	1	$H_A I_B$ or $H_A H_B$	H_A	3/32	(19),(20)
1	0	0	$H_A I_B$ or $H_A H_B$	H_A	3/32	(19),(20)
1	0	1	$H_A H_B$	H_A and H_B	1/32	(20)
1	1	0	$I_A H_B$ or $H_A H_B$	H_B	3/32	(18),(20)
1	1	1	all	-	9/32	(17) - (20)

Table D.2: Eve's Possible Derivations

Intercept-resend Attack on Alice's qubits

The system is changed by Trent depending on Alice's authentication key value of 0 (eq. (27)) or 1 (eq. (28)).

$$I_T(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \quad (27)$$

$$H_T(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \quad (28)$$

When resending a particle to Alice prepared according to Eve's measurement result, there is no error and no detection in case of eq. (27). In case of eq. (28) the probability of introducing an error and being detected amounts to $\frac{1}{2}$. The overall detection probability is $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \quad (29)$$

Translucent Attack on Alice's qubits

The two following unitary operations to entangle ancilla $|E\rangle_E$ or $|0\rangle_E$ are considered.

$$\begin{aligned} U_E(|0E\rangle_{AE}) &= \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E \\ U_E(|1E\rangle_{AE}) &= \alpha'|1\rangle_A|e_{11}\rangle_E + \beta'|0\rangle_A|e_{10}\rangle_E \ , \end{aligned} \quad (A)$$

where $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha'|^2 + |\beta'|^2 = 1$ and $|\alpha\beta^*|^2 + |\alpha'^*\beta'|^2 = 0$
and

$$\begin{aligned} U_E(|00\rangle_{AE}) &= |00\rangle_{AE} \\ U_E(|10\rangle_{AE}) &= |11\rangle_{AE} \ . \end{aligned} \tag{B}$$

With transformation (A) the total system changes to states $|\xi_{A0}\rangle$ or $|\xi_{A1}\rangle$, where subscripts $A0$ and $A1$ denote the unitary transformation (A) followed by the authentication key value $id_{iA} = 0$ or $id_{iA} = 1$, respectively. Accordingly, the unitary operation (B) transforms the system to states $|\xi_{B0}\rangle$ or $|\xi_{B1}\rangle$. The first operation is performed by Trent on Alice's qubit (subscripted with T), the second transforms Alice's and Eve's particle (E), and the last is executed by Alice (A).

$$\begin{aligned} |\xi_{A0}\rangle &= I_A U_E \left(I_T \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \right) \otimes |E\rangle_E \right) \\ &= \frac{1}{\sqrt{2}} (\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|100\rangle_{ATB}|e_{01}\rangle_E + \alpha'|111\rangle_{ATB}|e_{11}\rangle_E + \beta'|011\rangle_{ATB}|e_{10}\rangle_E) \end{aligned} \tag{30}$$

$$\begin{aligned} |\xi_{A1}\rangle &= H_A U_E \left(H_T \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \right) \otimes |E\rangle_E \right) \\ &= H_A U_E \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \otimes |E\rangle_E \right) \\ &= H_A \Big(\frac{1}{2}(\alpha|000\rangle|e_{00}\rangle_E + \beta|100\rangle|e_{01}\rangle_E + \alpha'|100\rangle|e_{11}\rangle_E + \beta'|000\rangle|e_{10}\rangle_E \\ &\qquad + \alpha|011\rangle|e_{00}\rangle_E + \beta|111\rangle|e_{01}\rangle_E - \alpha'|111\rangle|e_{11}\rangle_E - \beta'|011\rangle|e_{10}\rangle_E) \Big) \\ &= \frac{1}{2} H_A \Big(|000\rangle_{ATB}(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle)_E \\ &\qquad + |100\rangle_{ATB}(\beta|e_{01}\rangle + \alpha'|e_{11}\rangle)_E \\ &\qquad + |011\rangle_{ATB}(\alpha|e_{00}\rangle - \beta'|e_{10}\rangle)_E \\ &\qquad + |111\rangle_{ATB}(\beta|e_{01}\rangle - \alpha'|e_{11}\rangle)_E \Big) \\ &= \frac{1}{2\sqrt{2}} \Big(|000\rangle_{ATB}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E \\ &\qquad + |100\rangle_{ATB}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E \\ &\qquad + |011\rangle_{ATB}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E \\ &\qquad + |111\rangle_{ATB}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E \Big) \end{aligned} \tag{31}$$

The detection probabilities are calculated as follows.

$$\rho_D(|\xi_{A0}\rangle) = \left(\frac{|\beta|}{\sqrt{2}}\right)^2 + \left(\frac{|\beta'|}{\sqrt{2}}\right)^2 = \frac{\beta^2+\beta'^2}{2} \tag{32}$$

$$\rho_D(|\xi_{A1}\rangle) = \left(\frac{1}{2\sqrt{2}}\right)^2 * 2\left(|\alpha|^2+|\beta|^2+|\alpha'|^2+|\beta'|^2\right) = \frac{1}{2} \tag{33}$$

$$\rho_D = \frac{1}{2} * \left(\frac{\beta^2+\beta'^2}{2} + \frac{1}{2}\right) = \frac{\beta^2+\beta'^2+1}{4} \tag{34}$$

With the unitary transformation (B) the total system changes to states $|\xi_{B0}\rangle$ or $|\xi_{B1}\rangle$ after all operations of Trent, Eve and Alice.

$$\begin{aligned}
|\xi_{B0}\rangle &= I_A U_E \left(I_T \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|0000\rangle + |1111\rangle\right)_{ATBE}
\end{aligned} \tag{35}$$

$$\begin{aligned}
|\xi_{B1}\rangle &= H_A U_E \left(H_T \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \otimes |0\rangle_E\right) \\
&= H_A U_E \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= H_A \left(\frac{1}{2}(|0000\rangle + |1001\rangle + |0110\rangle - |1111\rangle)_{ATBE}\right) \\
&= \frac{1}{2\sqrt{2}}\left(|0000\rangle + |1000\rangle + |0001\rangle - |1001\rangle + |0110\rangle + |1110\rangle - |0111\rangle + |1111\rangle\right)_{ATBE} \\
&= \frac{1}{2}\Big(|000\rangle_{ATB}|+\rangle_E + |100\rangle_{ATB}|-\rangle_E + |011\rangle_{ATB}|-\rangle_E + |111\rangle_{ATB}|+\rangle_E\Big)
\end{aligned} \tag{36}$$

In case of $id_{iA} = 0$ (eq. (35)), Eve is not detected. There's only detection possible, if $id_{iA} = 1$ (eq. (36)).

$$\rho_D(|\xi_{B0}\rangle) = 0 \tag{37}$$

$$\rho_D(|\xi_{B1}\rangle) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \tag{38}$$

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{39}$$

D.3 Eavesdropping on QKD (s. 4.3.3, p. 31)

Translucent Attack (A) on Bob's particles

After Alice's, Bob's, and Eve's operations the system changes to one of the following states (40) – (43).

Eq. (40): Alice and Bob both perform an identity transformation (I) on their respective qubit before Eve entangles her ancilla.

$$
\begin{aligned}
|\xi_A\rangle_1 &= U_E\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \otimes |E\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \alpha'|111\rangle_{ATB}|e_{11}\rangle_E + \beta'|110\rangle_{ATB}|e_{10}\rangle_E\right) \\
&= \frac{1}{4\sqrt{2}} * 4\Bigg(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \\
&\qquad \alpha'|111\rangle_{ATB}|e_{11}\rangle_E + \beta'|110\rangle_{ATB}|e_{10}\rangle_E\Bigg) \\
&= \frac{1}{2\sqrt{2}}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E + \\
&\qquad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E\Bigg) \\
&= \frac{1}{2\sqrt{2}}\Bigg(|\Phi^+\rangle_{AB}(|+\rangle_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + |-\rangle_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E) + \\
&\qquad |\Phi^-\rangle_{AB}(|+\rangle_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E + |-\rangle_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E) + \\
&\qquad |\Psi^+\rangle_{AB}(|+\rangle_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E + |-\rangle_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E) + \\
&\qquad |\Psi^-\rangle_{AB}(|+\rangle_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E + |-\rangle_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E)\Bigg) \qquad (40)
\end{aligned}
$$

Eq. (41): Alice performs an identity operation (I_A) and Bob a Hadamard transformation (H_B) on their respective qubit before Eve entangles her ancilla.

$$
\begin{aligned}
|\xi_A\rangle_2 &= U_E(\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATB} \otimes |E\rangle_E) \\
&= \frac{1}{2}(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \alpha'|001\rangle_{ATB}|e_{11}\rangle_E + \beta'|000\rangle_{ATB}|e_{10}\rangle_E + \\
&\quad \alpha|110\rangle_{ATB}|e_{00}\rangle_E + \beta|111\rangle_{ATB}|e_{01}\rangle_E - \alpha'|111\rangle_{ATB}|e_{11}\rangle_E - \beta'|110\rangle_{ATB}|e_{10}\rangle_E) \\
&= \frac{1}{8} * 4(|000\rangle_{ATB}(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle)_E + |001\rangle_{ATB}(\beta|e_{01}\rangle + \alpha'|e_{11}\rangle)_E + \\
&\quad |110\rangle_{ATB}(\alpha|e_{00}\rangle - \beta'|e_{10}\rangle)_E + |111\rangle_{ATB}(\beta|e_{01}\rangle - \alpha'|e_{11}\rangle)_E) \\
&= \frac{1}{4}(|\Phi^+\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^+\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AB}|-\rangle_T(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AB}|+\rangle_T(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E \ ) \qquad (41)
\end{aligned}
$$

Eq. (42): Alice performs a Hadamard operation (H_A) and Bob an identity transformation (I_B) on their respective qubit before Eve entangles her ancilla.

$$
\begin{aligned}
|\xi_A\rangle_3 &= U_E(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \otimes |E\rangle_E) \\
&= \frac{1}{2}(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \alpha|100\rangle_{ATB}|e_{00}\rangle_E + \beta|101\rangle_{ATB}|e_{01}\rangle_E) + \\
&\quad \alpha'|011\rangle_{ATB}|e_{11}\rangle_E + \beta'|010\rangle_{ATB}|e_{10}\rangle_E - \alpha'|111\rangle_{ATB}|e_{11}\rangle_E - \beta'|110\rangle_{ATB}|e_{10}\rangle_E \\
&= \frac{1}{8} * 4(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \alpha|100\rangle_{ATB}|e_{00}\rangle_E + \beta|101\rangle_{ATB}|e_{01}\rangle_E) + \\
&\quad \alpha'|011\rangle_{ATB}|e_{11}\rangle_E + \beta'|010\rangle_{ATB}|e_{10}\rangle_E - \alpha'|111\rangle_{ATB}|e_{11}\rangle_E - \beta'|110\rangle_{ATB}|e_{10}\rangle_E \\
&= \frac{1}{4}(|\Phi^+\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^+\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AB}|+\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AB}|-\rangle_T(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AB}|+\rangle_T(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AB}|-\rangle_T(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E \ ) \qquad (42)
\end{aligned}
$$

Eq. (43): Alice and Bob both perform a Hadamard transformation (H) on their respective qubit before Eve entangles her ancilla.

$$
\begin{aligned}
|\xi_A\rangle_4 &= U_E(\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{ATB} \otimes |E\rangle_E) \\
&= \frac{1}{8\sqrt{2}} * 4(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|001\rangle_{ATB}|e_{01}\rangle_E + \alpha'|001\rangle_{ATB}|e_{11}\rangle_E + \beta'|000\rangle_{ATB}|e_{10}\rangle_E \\
&\quad + \alpha|100\rangle_{ATB}|e_{00}\rangle_E + \beta|101\rangle_{ATB}|e_{01}\rangle_E + \alpha'|101\rangle_{ATB}|e_{11}\rangle_E + \beta'|100\rangle_{ATB}|e_{10}\rangle_E \\
&\quad + \alpha|010\rangle_{ATB}|e_{00}\rangle_E + \beta|011\rangle_{ATB}|e_{01}\rangle_E - \alpha'|011\rangle_{ATB}|e_{11}\rangle_E - \beta'|010\rangle_{ATB}|e_{10}\rangle_E \\
&\quad + \alpha|110\rangle_{ATB}|e_{00}\rangle_E - \beta|111\rangle_{ATB}|e_{01}\rangle_E + \alpha'|111\rangle_{ATB}|e_{11}\rangle_E + \beta'|110\rangle_{ATB}|e_{10}\rangle_E) \\
&= \frac{1}{4\sqrt{2}}(|\Phi^+\rangle_{AB}(|+\rangle_T\ 2(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + |-\rangle_T 2(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E) + \\
&\quad |\Phi^-\rangle_{AB}(|+\rangle_T\ 2(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E - |-\rangle_T 2(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E) + \\
&\quad |\Psi^+\rangle_{AB}(|+\rangle_T\ 2(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E + |-\rangle_T 2(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E) + \\
&\quad |\Psi^-\rangle_{AB}(|+\rangle_T\ 2(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E - |-\rangle_T 2(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E)\ ) \\
&= \frac{1}{2\sqrt{2}}(|\Phi^+\rangle_{AB}(|+\rangle_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + |-\rangle_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E) + \\
&\quad |\Phi^-\rangle_{AB}(|+\rangle_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E - |-\rangle_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E) + \\
&\quad |\Psi^+\rangle_{AB}(|+\rangle_T(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E + |-\rangle_T(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E) + \\
&\quad |\Psi^-\rangle_{AB}(|+\rangle_T(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E - |-\rangle_T(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E)\ ) \qquad (43)
\end{aligned}
$$

The detection probabilities can be calculated by comparing the results of (40) – (43) with the expected results given in table 4.1 (p. 28).

$$
\begin{aligned}
\rho_D(|\xi_A\rangle_1) &= \left(\frac{1}{2\sqrt{2}}\right)^2 \left(2\alpha^2 + 4\beta^2 + 2\alpha'^2 + 4\beta'^2\right) \\
&= \frac{1}{4}\left(1 - \beta^2 + 2\beta^2 + 1 - \beta'^2 + 2\beta'^2\right) \\
&= \frac{1}{4}\left(2 + \beta^2 + 2\beta'^2\right) \\
&= \frac{2 + \beta^2 + \beta'^2}{4} \qquad (44) \\
\rho_D(|\xi_A\rangle_2) &= \left(\frac{1}{4}\right)^2 \left(4\alpha^2 + 4\beta^2 + 4\alpha'^2 + 4\beta'^2\right) \\
&= \frac{1}{4}\left(1 - \beta^2 + \beta^2 + 1 - \beta'^2 + \beta'^2\right) \\
&= \frac{1}{2} \qquad (45) \\
\rho_D(|\xi_A\rangle_3) &= \left(\frac{1}{4}\right)^2 \left(4\alpha^2 + 4\beta^2 + 4\alpha'^2 + 4\beta'^2\right) \\
&= \frac{1}{2} \qquad (46) \\
\rho_D(|\xi_A\rangle_4) &= \left(\frac{1}{2\sqrt{2}}\right)^2 \left(2\alpha^2 + 4\beta^2 + 2\alpha'^2 + 4\beta'^2\right) \\
&= \frac{2 + \beta^2 + \beta'^2}{4} \qquad (47)
\end{aligned}
$$

$$\begin{aligned}\rho_D &= \frac{1}{4}\left(2*\left(\frac{1}{2}+\frac{\beta^2+\beta'2}{4}\right)+2*\frac{1}{2}\right)\\ &= \frac{1}{4}\left(1+\frac{\beta^2+\beta'^2}{2}+1\right)\\ &= \frac{1}{2}+\frac{\beta^2+\beta'^2}{8}\end{aligned} \tag{48}$$

Translucent Attack (B) on Bob's particles

After Alice's, Bob's, and Eve's operations the system changes to one of the following states (49) – (52).

Eq. (49): Alice and Bob both perform an identity transformation (I) on their respective qubit before Eve entangles her ancilla.

$$\begin{aligned}|\xi_B\rangle_1 &= U_E\left(\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ATB}\otimes|0\rangle_E\right)\\ &= \frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)_{ATBE}\\ &= \frac{1}{4\sqrt{2}}*4(|0000\rangle+|1111\rangle)_{ATBE}\\ &= \frac{1}{2}\Bigg(\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_T\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_E\\ &+ \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_T\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_E\\ &+ \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_T\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_E\\ &+ \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_T\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_E\Bigg)\\ &= \frac{1}{2}\left(|\Phi^+\rangle_{AB}|+\rangle_T|+\rangle_E+|\Phi^+\rangle_{AB}|-\rangle_T|-\rangle_E+|\Phi^-\rangle_{AB}|+\rangle_T|-\rangle_E+|\Phi^-\rangle_{AB}|-\rangle_T|+\rangle_E\right)\end{aligned} \tag{49}$$

Eq. (50): Alice performs an identity operation (I) and Bob a Hadamard transformation (H) on their respective qubit before Eve entangles her ancilla.

$$\begin{aligned}|\xi_B\rangle_2 &= U_E\left(\frac{1}{2}(|000\rangle+|001\rangle+|110\rangle-|111\rangle)_{ATB}\otimes|0\rangle_E\right)\\ &= \frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{ATBE}\\ &= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{AB}|+\rangle_T|-\rangle_E+|\Phi^+\rangle_{AB}|-\rangle_T|+\rangle_E+|\Phi^-\rangle_{AB}|+\rangle_T|+\rangle_E+|\Phi^-\rangle_{AB}|-\rangle_T|-\rangle_E+\\ &\qquad |\Psi^+\rangle_{AB}|+\rangle_T|+\rangle_E-|\Psi^+\rangle_{AB}|-\rangle_T|-\rangle_E-|\Psi^-\rangle_{AB}|+\rangle_T|-\rangle_E+|\Psi^-\rangle_{AB}|-\rangle_T|+\rangle_E\big)\end{aligned} \tag{50}$$

Eq. (51): Alice performs a Hadamard transformation (H_A) and Bob an identity operation (I_B) on their respective qubit before Eve entangles her ancilla.

$$\begin{aligned}
|\xi_B\rangle_3 &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle + |001\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |1000\rangle + |0111\rangle - |1111\rangle)_{ATBE} \\
&= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{AB}|+\rangle_T|-\rangle_E + |\Phi^+\rangle_{AB}|-\rangle_T|+\rangle_E + |\Phi^-\rangle_{AB}|+\rangle_T|+\rangle_E + |\Phi^-\rangle_{AB}|-\rangle_T|-\rangle_E + \\
&\qquad |\Psi^+\rangle_{AB}|+\rangle_T|+\rangle_E + |\Psi^+\rangle_{AB}|-\rangle_T|-\rangle_E - |\Psi^-\rangle_{AB}|+\rangle_T|-\rangle_E - |\Psi^-\rangle_{AB}|-\rangle_T|+\rangle_E\big)
\end{aligned} \tag{51}$$

Eq. (52): Alice and Bob both perform a Hadamard transformation (H) on their respective qubit before Eve entangles her ancilla.

$$\begin{aligned}
|\xi_B\rangle_4 &= U_E\left(\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2\sqrt{2}}\left(|0000\rangle + |0011\rangle + |1000\rangle + |1011\rangle + |0100\rangle - |0111\rangle - |1100\rangle + |1111\rangle\right)_{ATBE} \\
&= \frac{1}{2}\big(|\Phi^+\rangle_{AB}|+\rangle_T|+\rangle_E + |\Phi^-\rangle_{AB}|+\rangle_T|-\rangle_E + |\Psi^+\rangle_{AB}|-\rangle_T|+\rangle_E - |\Psi^-\rangle_{AB}|-\rangle_T|-\rangle_E\big)
\end{aligned} \tag{52}$$

Again, detection probabilities can be calculated by comparing the results of (49) – (52) with the expected outcomes.

$$\rho_D(|\xi_B\rangle_1) = 2 * \left(\frac{1}{2}\right)^2 = \frac{1}{2} \tag{53}$$

$$\rho_D(|\xi_B\rangle_2) = 4 * \left(\frac{1}{2\sqrt{2}}\right)^2 = \frac{1}{2} \tag{54}$$

$$\rho_D(|\xi_B\rangle_3) = 4 * \left(\frac{1}{2\sqrt{2}}\right)^2 = \frac{1}{2} \tag{55}$$

$$\rho_D(|\xi_B\rangle_4) = 2 * \left(\frac{1}{2}\right)^2 = \frac{1}{2} \tag{56}$$

The overall detection probability sums up to $\frac{1}{2}$.

$$\rho_D = \frac{1}{4}\left(4 * \frac{1}{2}\right) = \frac{1}{2} \tag{57}$$

D.4 Simple Impersonation Attacks (s. 4.3.4, p. 31)

Sender or Receiver Impersonation in Authentication

The impersonation of Alice and Bob are equivalent during authentication. In the analysis the impersonation of Alice is discussed.

Both authentication key values ($id_{iA} = 0$ and $id_{iA} = 1$) occur with the same probability of $\frac{1}{2}$. The detection probability amounts to $\frac{1}{4}$ in both cases, Eve guessing the authentication key value (eq. (58)) or Eve measuring the undecoded particle (eq. (59)).

$$\frac{1}{2}\ (\rho\ of\ \ guessing\ \ false)\ * \frac{1}{2}\ (\rho_D\ in\ \ false\ \ case) = \frac{1}{4} \tag{58}$$

If $id_{iA} = 0$, Eve always measures the right result in the system

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB}$$

If $id_{iA} = 1$, Eve can be detected with probability for

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB}$$

The detection probability can be calculated as follows.

$$\frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{59}$$

Sender or Receiver Impersonation in QKD

In Eve's impersonation of Alice (1st impersonation attack) the system changes to one of the following states while Eve attempts to restore the A-qubits without any knowledge of the authentication key. States (60) and (63) are correctly restored, whereas states (61) and (62) are not.

In case of $id_{iA} = 0$:

$$\begin{aligned} I_{E(A)} \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \end{aligned} \tag{60}$$

$$\begin{aligned} H_{E(A)} \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \end{aligned} \tag{61}$$

In case of $id_{iA} = 1$:

$$\begin{aligned} I_{E(A)} \quad & \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (62) \\ H_{E(A)} \quad & \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (63) \end{aligned}$$

In QKD Eve performs $I_{E(A)}$ or $H_{E(A)}$ on her restored states (60) – (63). Operations on states (60) and (63) results in correct states without any detection probability, whereas there are errors in all other cases:

$$I_{E(A)}\ on\ (60): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (64)$$

$$I_{E(A)}\ on\ (61): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (65)$$

$$I_{E(A)}\ on\ (62): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (66)$$

$$I_{E(A)}\ on\ (63): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (67)$$

$$H_{E(A)}\ on\ (60): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (68)$$

$$H_{E(A)}\ on\ (61): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (69)$$

$$H_{E(A)}\ on\ (62): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (70)$$

$$H_{E(A)}\ on\ (63): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (71)$$

Eve's alternative is the performance of her operations for QKD on the received states without trying to restore them first. According to D.2, this option is a simplification of guessing the key in terms of the analysis. Only states (72) and (73) and states (74) – (77) must be considered. However, the simplification leads to the same results.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (72)$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (73)$$

$$I_{E(A)}\ on\ (72): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (74)$$

$$I_{E(A)}\ on\ (73): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (75)$$

$$H_{E(A)}\ on\ (72): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \qquad (76)$$

$$H_{E(A)}\ on\ (73): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \qquad (77)$$

The state transformations can be equally derived for Eve's impersonation of Bob (2nd impersonation attack). Eve then works on the B-particles of the system $|\theta_i\rangle_{ATE(B)}$. That means the incorrect states (61) and (62) or (73) must be replaced with (78) in the following calculations.

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATE(B)} \tag{78}$$

Table D.3 lists the possible transformed states of the system after Eve's and Bob's operations, and Eve's and Trent's measurements during Eve's impersonation of Alice (1st impersonation attack). Eve's possible derivations on Bob's operations (i.e. the key) are shown in table D.4 (p. D15) in case of an identity operation by Eve ($I_{E(A)}$). Exactly the same can be applied to a Hadamard transformation of Eve (replace $I_{E(A)}$ with $H_{E(A)}$ in column *Eve's operation* and (80), (81), (82) and (83) with (85), (84), (87) and (86) in column *Eq*, respectively).

The success and detection probabilities in the sender impersonation can be derived according to tables D.3 and D.4. Eve can only derive Bob's transformation in case of the entire results $|\Phi^-\rangle_{E(A)B}|-\rangle_T$ and $|\Psi^+\rangle_{E(A)B}|-\rangle_T$, that is with a success probability of $\frac{1}{4}$.

$$\begin{aligned}\rho_S &= \frac{1}{8}\,(\rho_O\ of\ transformed\ term)\ *4\ (n^o\ of\ results)\ *\frac{1}{2}\,(\rho_O\ of\ each\ result)\\ &= \frac{1}{4}\end{aligned} \tag{79}$$

Eq.	Operation of Eve	Bob	Transformation of GHZ states
(80)	$I_{E(A)}$	I_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Phi^-\rangle_{E(A)B}\|-\rangle_T)$
(81)			$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T - \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$
(82)	$I_{E(A)}$	H_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$
(83)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|-\rangle_T)$
(84)	$H_{E(A)}$	I_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T - \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$
(85)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Phi^-\rangle_{E(A)B}\|-\rangle_T)$
(86)	$H_{E(A)}$	H_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|-\rangle_T)$
(87)			$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$

Table D.3: Results of QKD (1st Impersonation Attack)

There's no detection in eqs. (80), (82), (84) and (86), as these equations are correct system transformations. In case of eqs. (81) and (87), Bob detects Eve for any of her turns to announce her operation and her Bell state. For $|\Psi^+\rangle_{E(A)B}|-\rangle_T$ in eq. (83) or $|\Phi^-\rangle_{E(A)B}|-\rangle_T$ in eq. (85) Eve is in the position to recognise a restoring error, since these results are not supposed to occur. Simultaneously, she knows Bob's operation. To avoid detection Eve must announce an expected result of eqs. (82) or (84), respectively. Hence, the detection probability in these cases is $\frac{1}{2}$. The overall detection probability totals $\frac{3}{8}$ per any second check qubit.

$$\rho_D = \frac{1}{8} * \left(4 * 0 + 2 * 1 + 2 * \frac{1}{2}\right) = \frac{3}{8} \tag{88}$$

Eve's operation	Eve's entire result	Bob's operation	Eq.
$I_{E(A)}$	$\|\Phi^+\rangle_{E(A)B}\|+\rangle_T$	I_B or H_B	(80),(83)
	$\|\Phi^+\rangle_{E(A)B}\|-\rangle_T$	I_B or H_B	(81),(82)
	$\|\Phi^-\rangle_{E(A)B}\|+\rangle_T$	I_B or H_B	(81),(82)
	$\|\Phi^-\rangle_{E(A)B}\|-\rangle_T$	I_B	(80)
	$\|\Psi^+\rangle_{E(A)B}\|+\rangle_T$	I_B or H_B	(81),(82)
	$\|\Psi^+\rangle_{E(A)B}\|-\rangle_T$	H_B	(83)
	$\|\Psi^-\rangle_{E(A)B}\|+\rangle_T$	-	-
	$\|\Psi^-\rangle_{E(A)B}\|-\rangle_T$	I_B or H_B	(81),(82)

Table D.4: Eve's Derivations (1st Impersonation Attack)

Eq.	Operation of Alice	Operation of Eve	Transformation of GHZ states
(89)	I_A	$I_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Phi^-\rangle_{AE(B)}\|-\rangle_T)$
(90)			$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$
(91)	I_A	$H_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$
(92)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Phi^-\rangle_{AE(B)}\|-\rangle_T)$
(93)	H_A	$I_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T - \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$
(94)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|-\rangle_T)$
(95)	H_A	$H_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|-\rangle_T)$
(96)			$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T - \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$

Table D.5: Results of QKD (2nd Impersonation Attack)

Table D.5 represents the possible transformed states of the system after Alice's and Eve's operations, and Alice's and Trent's measurements during Eve's impersonation of Bob (2nd impersonation attack). The detection and success probabilities can be derived as follows. In eqs. (89), (91), (93) and (95) there is no detection. In contrast to the first impersonation attack, Eve does not know the Bell measurement result. Thus, she cannot observe her own restoring errors and is detected by Alice for all other terms (eqs. (90), (92), (94) and (96)) when she announces her results.

$$\rho_D = \frac{1}{8} * (4 * 0 + 4 * 1) = \frac{1}{2} \tag{97}$$

With the knowledge of her own operations Alice precisely deduces one operation. But Eve does not know Alice's operation, nor her resultant Bell state. All entire results are received by both of Eve's operations, so Eve cannot deduce Alice's derivation (tab. D.6, p. D16). Thus, ρ_S is 0.

Entire state	Alice's derivation with		Eve's operations	Eq.
	I_A	H_A		
$\|\Phi^+\rangle_{AE(B)}\|+\rangle_T$	I_B	H_B	$I_{E(B)}$ or $H_{E(B)}$	(89),(92)/(94),(95)
$\|\Phi^+\rangle_{AE(B)}\|-\rangle_T$	H_B	I_B	$I_{E(B)}$ or $H_{E(B)}$	(90),(91)/(93),(96)
$\|\Phi^-\rangle_{AE(B)}\|+\rangle_T$	H_B	I_B	$I_{E(B)}$ or $H_{E(B)}$	(90),(91)/(93),(96)
$\|\Phi^-\rangle_{AE(B)}\|-\rangle_T$	I_B	-	$I_{E(B)}$ or $H_{E(B)}$	(89),(92)
$\|\Psi^+\rangle_{AE(B)}\|+\rangle_T$	H_B	I_B	$I_{E(B)}$ or $H_{E(B)}$	(90),(91)/(93),(96)
$\|\Psi^+\rangle_{AE(B)}\|-\rangle_T$	-	H_B	$I_{E(B)}$ or $H_{E(B)}$	(94),(95)
$\|\Psi^-\rangle_{AE(B)}\|-\rangle_T$	H_B	I_B	$I_{E(B)}$ or $H_{E(B)}$	(90),(91)/(93),(96)

Table D.6: Alice's Derivations (2nd Impersonation Attack)

D.5 Advanced Impersonation Attacks (s. 4.3.5, p. 34)

Impersonation of Sender ans Authority

Bob correctly decodes the non-encoded B-particles.
In case of $id_{iB} = 0$:

$$\begin{aligned} & I_B \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \end{aligned} \tag{98}$$

In case of $id_{iB} = 1$:

$$\begin{aligned} & H_B \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \end{aligned} \tag{99}$$

The detection probability during authentication remains $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{100}$$

Bob's operation for QDK on states (98) and (99) transforms the system to one of the following states (101) – (104).

$$I_B \text{ on } (98): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \tag{101}$$

$$I_B \text{ on } (99): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \tag{102}$$

$$H_B \text{ on } (98): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \tag{103}$$

$$H_B \text{ on } (99): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \tag{104}$$

By measuring the B-particle and her own $E(A)$- or $E(T)$-particle Eve does not gain any

knowledge of Bob's operation. The same results can be measured for all states (101) – (104). Different measurement outcomes occur for I_B on the falsely restored state (102) or for H_B on the correctly restored state (103).

Following the protocol Eve's operation on her $E(A)$-particle transforms the system to one of the following states (105) – (112).

$$I_{E(A)}\ on\ (101): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \tag{105}$$

$$I_{E(A)}\ on\ (102): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \tag{106}$$

$$I_{E(A)}\ on\ (103): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \tag{107}$$

$$I_{E(A)}\ on\ (104): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \tag{108}$$

$$H_{E(A)}\ on\ (101): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{109}$$

$$H_{E(A)}\ on\ (102): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{E(A)E(T)B} \tag{110}$$

$$H_{E(A)}\ on\ (103): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{E(A)E(T)B} \tag{111}$$

$$H_{E(A)}\ on\ (104): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{112}$$

Again, Eve cannot gain any knowledge of Bob's operation. By separate measurements of all particles of the system she measures all combinations $|000\rangle, |001\rangle, ..., |111\rangle$ for both of Bob's operations. By projecting the $E(A)$- and the B-particle onto the Bell basis and measuring the $E(T)$-particle in the x basis all entire results occur for both of Bob's operations (tab. D.7).

Eq.	Operation of Eve	Operation of Bob	Transformation of GHZ states	Case
(113)	$I_{E(A)}$	I_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Phi^-\rangle_{E(A)B}\|-\rangle_T)$	(105)
(114)			$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$	(106)
(115)	$I_{E(A)}$	H_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$	(107)
(116)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Phi^-\rangle_{E(A)B}\|-\rangle_T)$	(108)
(117)	$H_{E(A)}$	I_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T - \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$	(109)
(118)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|-\rangle_T)$	(110)
(119)	$H_{E(A)}$	H_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|-\rangle_T)$	(111)
(120)			$\frac{1}{2}(\|\Phi^+\rangle_{E(A)B}\|-\rangle_T + \|\Phi^-\rangle_{E(A)B}\|+\rangle_T + \|\Psi^+\rangle_{E(A)B}\|+\rangle_T - \|\Psi^-\rangle_{E(A)B}\|-\rangle_T)$	(112)

Table D.7: Results of QKD (1st Advanced Impersonation Attack)

The detection probability can be derived according to table D.7. The correct transformations (113), (115), (117), and (119) exclude any detection. Eve cannot observe any restoring errors, since all entire results occur in correct and wrong cases. That leads to a detection probability of 1 in cases (114), (116), (118), and (120) and to an overall detection probability of 50 %.

$$\rho_D = \frac{1}{8} * (4 * 0 + 4 * 1) = \frac{1}{2} \tag{121}$$

Impersonation of Receiver and Authority

Alice correctly decodes her non-encoded A-particles.
In case of $id_i = 0$:

$$\begin{aligned} & I_B \quad \left(\frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \right) \\ = \quad & \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{E(T)E(B)} \end{aligned} \tag{122}$$

In case of $id_i = 1$:

$$\begin{aligned} & H_A \quad \left(\frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \right) \\ = \quad & \frac{1}{2} (|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \end{aligned} \tag{123}$$

The detection probability during authentication remains $\frac{1}{4}$ (see eq. (100)).

Alice's operation for QDK on states (122) and (123) transforms the system to one of the following states (124) – (127).

$$I_A \; on \; (122): \quad \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{124}$$

$$I_A \; on \; (123): \quad \frac{1}{2} (|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{125}$$

$$H_A \; on \; (122): \quad \frac{1}{2} (|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{126}$$

$$H_A \; on \; (123): \quad \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{127}$$

Eve's operation on the $E(B)$-particle changes the system to one of the following states (128) – (135).

$$I_{E(B)} \; on \; (124): \quad \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{128}$$

$$I_{E(B)} \; on \; (125): \quad \frac{1}{2} (|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{129}$$

$$I_{E(B)} \; on \; (126): \quad \frac{1}{2} (|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{130}$$

$$I_{E(B)} \; on \; (127): \quad \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{131}$$

$$H_{E(B)}\ on\ (124): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)E(B)} \tag{132}$$

$$H_{E(B)}\ on\ (125): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)E(B)} \tag{133}$$

$$H_{E(B)}\ on\ (126): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)E(B)} \tag{134}$$

$$H_{E(B)}\ on\ (127): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)E(B)} \tag{135}$$

Table D.8 presents the transformed states after Alice's and Eve's operations. Eve cannot gain any information of Alice's derivation. Hence, she cannot know which key Alice infers. According to table D.8, the detection probability amounts to $\frac{1}{2}$ with $\rho_{D1} = 0$ for the first, third, fifth, and seventh row and $\rho_{D2} = 1$ for the other rows.

$$\rho_D = \frac{1}{8} * (4 * 0 + 4 * 1) = \frac{1}{2} \tag{136}$$

An additional detection probability for $|\Psi^+\rangle_{AE(B)}|-\rangle_{E(T)}$ in eq. (141) and $|\Phi^-\rangle_{AE(B)}|-\rangle_{E(T)}$ in eq. (143) amounts to $\frac{1}{8}$. These states are not supposed to occur.

$$\rho_{D_{add}} = \frac{1}{8} * \left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{8} \tag{137}$$

Eq.	Operation of Alice	Operation of Eve	Transformation of GHZ states	Case
(138)	I_A	$I_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Phi^-\rangle_{AE(B)}\|-\rangle_T)$	(128)
(139)			$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T - \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$	(129)
(140)	I_A	$H_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$	(132)
(141)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|-\rangle_T)$	(133)
(142)	H_A	$I_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T - \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$	(130)
(143)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Phi^-\rangle_{AE(B)}\|-\rangle_T)$	(131)
(144)	H_A	$H_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|-\rangle_T)$	(134)
(145)			$\frac{1}{2}(\|\Phi^+\rangle_{AE(B)}\|-\rangle_T + \|\Phi^-\rangle_{AE(B)}\|+\rangle_T + \|\Psi^+\rangle_{AE(B)}\|+\rangle_T + \|\Psi^-\rangle_{AE(B)}\|-\rangle_T)$	(135)

Table D.8: Results of QKD (2nd Advanced Impersonation Attack)

Impersonation of the Authority

The system changes to one of the following states (146) – (149) after Alice's and Bob's decoding.

$$\begin{aligned} I_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \end{aligned} \tag{146}$$

$$\begin{aligned} I_A H_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \end{aligned} \tag{147}$$

$$\begin{aligned} H_A I_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \end{aligned} \tag{148}$$

$$\begin{aligned} H_A H_B \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right) \\ = \quad & \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \end{aligned} \tag{149}$$

In the first eavesdropping test during authentication the detection probability sums up to $\frac{3}{8}$.

$$\rho_D = \frac{1}{4} * \left(0 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}\right) = \frac{3}{8} \tag{150}$$

The restoring errors are maintained in all transformations of the system, e.g. the state of the system changes after $I_A I_B$ to one of the following states (151) – (154) or to one of the states (155) – (158) after $I_A H_B$.

$$I_A I_B \text{ on } (146): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{151}$$

$$I_A I_B \text{ on } (147): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{152}$$

$$I_A I_B \text{ on } (148): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{153}$$

$$I_A I_B \text{ on } (149): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{154}$$

$$I_A H_B \text{ on } (146): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{155}$$

$$I_A H_B \text{ on } (147): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{156}$$

$$I_A H_B \text{ on } (148): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{157}$$

$$I_A H_B \text{ on } (149): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{158}$$

The detection probabilities can be calculated according to table D.9. For $I_A I_B$ there is no detection probability in eq. (162), full detection probability in eqs. (163) and (164), and a detection probability of $\frac{1}{2}$ in eq. (162). The same probabilities apply to $H_A H_B$.

$$\rho_D(I_A I_B) = \rho_D(H_A H_B) = \frac{1}{4} * \left(0 + 1 + 1 + \frac{1}{2}\right) = \frac{5}{8} \tag{159}$$

For $I_A H_B$ and $H_A I_B$ the detection probability totals $\frac{1}{2}$ with full detection probability in eqs. (167) and (168). There is no detection in eqs. (166) and (169), because the first case represents a correct transformation and the second equation equals it.

$$\rho_D(I_A H_B) = \rho_D(H_A I_B) = \frac{1}{4} * (0 + 1 + 1 + 0) = \frac{1}{2} \tag{160}$$

The overall detection probability amounts to 56.25 %.

$$\rho_D = \frac{1}{4} * \left(2 * \frac{5}{8} + 2 * \frac{1}{2}\right) = \frac{9}{16} \tag{161}$$

Eq.	Operation of Alice	Operation of Bob	Transformation of GHZ states	Case
(162)	I	I	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|-\rangle_{E(T)})$	(151)
(163)			$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^-\rangle_{AB}\|-\rangle_{E(T)})$	(152)
(164)			$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|+\rangle_{E(T)} - \|\Psi^-\rangle_{AB}\|-\rangle_{E(T)})$	(153)
(165)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|-\rangle_{E(T)})$	(154)
(166)	I	H	$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^-\rangle_{AB}\|-\rangle_{E(T)})$	(155)
(167)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|-\rangle_{E(T)})$	(156)
(168)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|-\rangle_{E(T)})$	(157)
(169)			$\frac{1}{2}(\|\Phi^+\rangle_{AB}\|-\rangle_{E(T)} + \|\Phi^-\rangle_{AB}\|+\rangle_{E(T)} + \|\Psi^+\rangle_{AB}\|+\rangle_{E(T)} - \|\Psi^-\rangle_{AB}\|-\rangle_{E(T)})$	(158)
⋮	⋮	⋮	⋮	⋮

Table D.9: Results of QKD (3rd Advanced Impersonation Attack)

Appendix E

Security Results: Improved Proposal 1

All derivations refer to the security analysis of the improved proposal of protocol 1 (s. 4.5.2, pp. 42).

E.1 Eavesdropping of Trent

After Bob's transformations the original state $|\theta_i\rangle_{ATB}$ of the first subset changes to one of the following states (170) – (171).

$$I_A I_B(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \quad (170)$$

$$I_A H_B(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATB} \quad (171)$$

With state (170) Trent always receives the same measurement outcomes of his and Bob's qubit. For state (171) he obtains the same result with the probability of $\frac{1}{2}$.

$$\rho(same\ results) = \frac{1}{2} * (1 + \frac{1}{2}) = \frac{3}{4} \quad (172)$$

$$\rho(different\ results) = \frac{1}{2} * \frac{1}{2} = \frac{1}{4} \quad (173)$$

Different results only occur in case of H_B. With same outcomes Trent can be sure that Bob's operation was I_B with the probability of $\frac{2}{3}$.

$$\rho_O(I_B) = \frac{1}{2} \ \ (eq.\ (170)) \quad (174)$$

$$\rho(same\ results) = \frac{3}{4} \rightarrow 1\ or\ 100\% \ \ (eq.\ (172)) \quad (175)$$

$$\rho(I_B) = \frac{2}{4} \rightarrow \frac{2}{3}\ or\ 66,\overline{6}\% \ \ (eqs.\ (174)\ and\ (175)) \quad (176)$$

Exactly the same results are calculated for Alice's operations of the second subset leading to states (177) and (178).

$$I_A I_B(|\theta_i\rangle_{ATB}) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \quad (177)$$

$$H_A I_B(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \quad (178)$$

E.2 Eavesdropping on Authentication

As authentication exactly proceeds as in the original protocol 1, see D.2 (p. D2) for detailed calculations.

E.3 Eavesdropping on QKD

Translucent Attack (A)

Eq. (179): Alice and Bob both perform an identity transformation (I) on their respective qubit of the first/second subset. Eve entangles her ancilla with Bob's/Alice's particle.

$$\begin{aligned}
|\xi_A\rangle_1 &= U_E(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \otimes |E\rangle_E) \\
&= \frac{1}{2\sqrt{2}}\big(|\Phi^+\rangle_{TB/AT}(|+\rangle_{A/B}(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E + |-\rangle_{A/B}(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E) + \\
&\quad |\Phi^-\rangle_{TB/AT}(|+\rangle_{A/B}(\alpha|e_{00}\rangle - \alpha'|e_{11}\rangle)_E + |-\rangle_{A/B}(\alpha|e_{00}\rangle + \alpha'|e_{11}\rangle)_E) + \\
&\quad |\Psi^+\rangle_{TB/AT}(|+\rangle_{A/B}(\beta|e_{01}\rangle + \beta'|e_{10}\rangle)_E + |-\rangle_{A/B}(\beta|e_{01}\rangle - \beta'|e_{10}\rangle)_E) + \\
&\quad |\Psi^-\rangle_{TB/AT}(|+\rangle_{A/B}(\pm\beta|e_{01}\rangle \mp \beta'|e_{10}\rangle)_E + |-\rangle_{A/B}(\pm\beta|e_{01}\rangle \pm \beta'|e_{10}\rangle)_E\big)
\end{aligned} \quad (179)$$

Eq. (180): Alice performs an identity operation (I_A) and Bob a Hadamard transformation (H_B) on their respective qubit of the first subset. Eve entangles her ancilla with Bob's particle.

$$\begin{aligned}
|\xi_A\rangle_2 &= U_E(\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATB} \otimes |E\rangle_E) \\
&= \frac{1}{4}\big(|\Phi^+\rangle_{BT}|+\rangle_A(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^+\rangle_{BT}|-\rangle_A(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{BT}|+\rangle_A(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{BT}|-\rangle_A(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{BT}|+\rangle_A(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{BT}|-\rangle_A(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{BT}|+\rangle_A(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{BT}|-\rangle_A(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E\big)
\end{aligned} \quad (180)$$

Eq. (181): Alice performs a Hadamard transformation (H_A) and Bob an identity operation (I_B) on their respective qubit of the second subset. Eve entangles her ancilla with Alice's particle.

$$\begin{aligned}
|\xi_A\rangle_3 &= U_E(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB}) \otimes |E\rangle_E) \\
&= \frac{1}{4}\big(|\Phi^+\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^+\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Phi^-\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^+\rangle_{AT}|-\rangle_B(-\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\quad |\Psi^-\rangle_{AT}|-\rangle_B(-\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E\big)
\end{aligned} \tag{181}$$

The detection probabilities can be calculated as follows.

$$\rho_D(|\xi_A\rangle_1) = \left(\frac{1}{2\sqrt{2}}\right)^2 (2\alpha^2 + 4\beta^2 + 2\alpha'^2 + 4\beta'^2) = \frac{2 + \beta^2 + \beta'^2}{4} \tag{182}$$

$$\rho_D(|\xi_A\rangle_2) = \left(\frac{1}{4}\right)^2 (4\alpha^2 + 4\beta^2 + 4\alpha'^2 + 4\beta'^2) = \frac{1}{2} \tag{183}$$

$$\rho_D(|\xi_A\rangle_3) = \left(\frac{1}{4}\right)^2 (4\alpha^2 + 4\beta^2 + 4\alpha'^2 + 4\beta'^2) = \frac{1}{2} \tag{184}$$

The overall detection probability totals $\frac{1}{2} + \frac{\beta^2+\beta'^2}{8}$.

$$\begin{aligned}
\rho_D &= \frac{1}{4}\left(2 * \frac{1}{2} + 2 * \frac{2 + \beta^2 + \beta' 2}{4}\right) \\
&= \frac{1}{4}\left(1 + 1 + \frac{\beta^2 + \beta'^2}{2}\right) \\
&= \frac{1}{2} + \frac{\beta^2 + \beta'^2}{8}
\end{aligned} \tag{185}$$

Translucent Attack (B)

Eq. (186): Alice and Bob both perform identity transformation (I) on their respective qubit of the first/second subset. Eve entangles her ancilla with Bob's/Alice's particle.

$$\begin{aligned}
|\xi_B\rangle_1 &= U_E\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |1111\rangle)_{ATBE} \\
&= \frac{1}{2}\big(|\Phi^+\rangle_{TB}|+\rangle_A|+\rangle_E + |\Phi^+\rangle_{TB}|-\rangle_A|-\rangle_E + |\Phi^-\rangle_{TB}|+\rangle_A|-\rangle_E + |\Phi^-\rangle_{TB}|-\rangle_A|+\rangle_E\big)
\end{aligned} \tag{186}$$

Eq. (187): Alice performs an identity operation (I_A) and Bob a Hadamard transformation (H_B) on their respective qubit of the first subset. Eve entangles her ancilla with Bob's particle.

$$\begin{aligned}
|\xi_B\rangle_2 &= U_E\left(\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)_{ATBE} \\
&= \frac{1}{2\sqrt{2}}\big(|\Phi^+\rangle_{TB}|-\rangle_A|+\rangle_E + |\Phi^+\rangle_{TB}|-\rangle_A|-\rangle_E + |\Phi^-\rangle_{TB}|+\rangle_A|+\rangle_E + |\Phi^-\rangle_{TB}|+\rangle_A|-\rangle_E + \\
&\qquad |\Psi^+\rangle_{TB}|+\rangle_A|+\rangle_E + |\Psi^+\rangle_{TB}|+\rangle_A|-\rangle_E + |\Psi^-\rangle_{TB}|-\rangle_A|+\rangle_E + |\Psi^-\rangle_{TB}|-\rangle_A|-\rangle_E\big)
\end{aligned} \tag{187}$$

Eq. (188): Alice performs a Hadamard transformation (H_A) and Bob an identity operation (I_B) on their respective qubit of the second subset. Eve entangles her ancilla with Alice's particle.

$$\begin{aligned}
|\xi_B\rangle_3 &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle + |001\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |1001\rangle + |0110\rangle - |1111\rangle)_{ATBE} \\
&= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{AT}|-\rangle_B|+\rangle_E + |\Phi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|+\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|-\rangle_E + \\
&\qquad |\Psi^+\rangle_{AT}|+\rangle_B|+\rangle_E - |\Psi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Psi^-\rangle_{AT}|+\rangle_B|-\rangle_E - |\Psi^-\rangle_{AT}|-\rangle_B|+\rangle_E\big)
\end{aligned} \tag{188}$$

The detection probabilities are calculated as follows.

$$\rho_D(|\xi_B\rangle_1) = 2 * \left(\frac{1}{2}\right)^2 = \frac{1}{2} \tag{189}$$

$$\rho_D(|\xi_B\rangle_2) = 0 \tag{190}$$

$$\rho_D(|\xi_B\rangle_3) = 2 * \left(\frac{1}{2\sqrt{2}}\right)^2 = \frac{1}{4} \tag{191}$$

The overall detection probability ρ_D sums up to $\frac{5}{16}$.

$$\rho_D = \frac{1}{4} * \left(2 * \frac{1}{2} + \frac{1}{4}\right) = \frac{5}{16} \tag{192}$$

E.4 Simple Impersonation Attacks

Sender or Receiver Impersonation in Authentication

During authentication the detection probability of 25 % is maintained (see D.4, p. D12).

Sender Impersonation in QKD

For simplicity, it is assumed here that Eve leaves the $E(A)$-qubit unrestored.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{193}$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{194}$$

Table E.1 shows the results of Eve's impersonation of the sender during QKD. In the first subset (row 1 - 4) Bob performs I_B on his particles of the (unrestored) system (193) or (194), which results in eq. (195) or (196), respectively. Bob's H_B on (193) and (194) leads to eqs. (197) and (198). In the second subset (row 5 - 8) Eve performs an identity or a Hadamard transformations on the $E(A)$-qubit of the system (193) or (194) resulting in transformations (199) – (202).

Eq.	Operation of Eve	Operation of Bob	Transformation of GHZ states
(195)	$I_{E(A)}$	I_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{TB}\|+\rangle_{E(A)} + \|\Phi^-\rangle_{TB}\|-\rangle_{E(A)})$
(196)			$\frac{1}{2}(\|\Phi^+\rangle_{TB}\|+\rangle_{E(A)} + \|\Phi^+\rangle_{TB}\|-\rangle_{E(A)} + \|\Phi^-\rangle_{TB}\|+\rangle_{E(A)} - \|\Phi^-\rangle_{TB}\|-\rangle_{E(A)})$
(197)	$I_{E(A)}$	H_B	$\frac{1}{2}(\|\Phi^+\rangle_{TB}\|-\rangle_{E(A)} + \|\Phi^-\rangle_{TB}\|+\rangle_{E(A)} + \|\Psi^+\rangle_{TB}\|+\rangle_{E(A)} + \|\Psi^-\rangle_{TB}\|-\rangle_{E(A)})$
(198)			$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{TB}\|+\rangle_{E(A)} - \|\Phi^+\rangle_{TB}\|-\rangle_{E(A)} + \|\Phi^-\rangle_{TB}\|+\rangle_{E(A)} + \|\Phi^-\rangle_{TB}\|-\rangle_{E(A)}$ $+\|\Psi^+\rangle_{TB}\|+\rangle_{E(A)} + \|\Psi^+\rangle_{TB}\|-\rangle_{E(A)} + \|\Psi^-\rangle_{TB}\|+\rangle_{E(A)} - \|\Psi^-\rangle_{TB}\|-\rangle_{E(A)})$
(199)	$I_{E(A)}$	I_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B)$
(200)			$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|-\rangle_B + \|\Phi^-\rangle_{E(A)T}\|+\rangle_B + \|\Psi^+\rangle_{E(A)T}\|+\rangle_B - \|\Psi^-\rangle_{E(A)T}\|-\rangle_B)$
(201)	$H_{E(A)}$	I_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|-\rangle_B + \|\Phi^-\rangle_{E(A)T}\|+\rangle_B + \|\Psi^+\rangle_{E(A)T}\|+\rangle_B - \|\Psi^-\rangle_{E(A)T}\|-\rangle_B)$
(202)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B)$

Table E.1: Results of QKD (1st Impersonation Attack)

Every first row (eqs. (195), (197), (199), and (201)) represents correct system transformations with no detection. Every second row (eqs. (196), (198), (200), and (202)) includes detection. Only in eq. (198) Eve is able to recognise a restoring error on her side, as $|\Psi^+\rangle_{TB}$ and $|\Psi^-\rangle_{TB}$ are not supposed to occur with $|-\rangle_E$ and $|+\rangle_E$, respectively. The overall detection probability for any of Eve's first turns can be calculated like follows.

$$\begin{aligned} \rho_D &= \frac{1}{8} * \left(4 * 0 + \frac{1}{2} + 2 * \left(\frac{1}{2\sqrt{2}}\right)^2 + 1 + 1\right) \\ &= \frac{11}{32} \end{aligned} \tag{203}$$

Table E.2 shows Eve's derivations of Bob's operations of the first subset. Eve can only derive Bob's operation in row 5 and 8 for states without consideration in the key arrangement, and in row 6 and 7 for states which are not supposed to occur. Table E.3, valid for the second subset, represents Bob's derivations of Alice's (Eve's) operations. Bob always deduces exactly one operation, but Eve cannot know which. Only in row 5 and 6 Eve is able to derive that Bob deduces H_A, but these states are not considered in the key arrangement.

Entire state	Eve's derivations	Remarks	Eq.
$\|\Phi^+\rangle_{TB}\|+\rangle_{E(A)}$	I_B or H_B	-	(195),(196),(198)
$\|\Phi^+\rangle_{TB}\|-\rangle_{E(A)}$	I_B or H_B	-	(196),(197),(198)
$\|\Phi^-\rangle_{TB}\|+\rangle_{E(A)}$	I_B or H_B	-	(196),(197),(198)
$\|\Phi^-\rangle_{TB}\|-\rangle_{E(A)}$	I_B or H_B	-	(195),(196),(198)
$\|\Psi^+\rangle_{TB}\|+\rangle_{E(A)}$	H_B	not considered	(197),(198)
$\|\Psi^+\rangle_{TB}\|-\rangle_{E(A)}$	H_B	not considered	(198)
$\|\Psi^-\rangle_{TB}\|+\rangle_{E(A)}$	H_B	not considered	(198)
$\|\Psi^-\rangle_{TB}\|-\rangle_{E(A)}$	H_B	not considered	(197),(198)

Table E.2: Eve's Derivations (1st Impersonation Attack)

Entire state	Bob's derivation	Eve's operations	Remarks	Eq.
$\|\Phi^+\rangle_{E(A)T}\|+\rangle_B$	I_A	$I_{E(A)}$ or $H_{E(A)}$	-	(199),(202)
$\|\Phi^+\rangle_{E(A)T}\|-\rangle_B$	H_A	$I_{E(A)}$ or $H_{E(A)}$	-	(200),(201)
$\|\Phi^-\rangle_{E(A)T}\|+\rangle_B$	H_A	$I_{E(A)}$ or $H_{E(A)}$	-	(200),(201)
$\|\Phi^-\rangle_{E(A)T}\|-\rangle_B$	I_A	$I_{E(A)}$ or $H_{E(A)}$	-	(199),(202)
$\|\Psi^+\rangle_{E(A)T}\|+\rangle_B$	H_A	$I_{E(A)}$ or $H_{E(A)}$	not considered	(200),(201)
$\|\Psi^-\rangle_{E(A)T}\|-\rangle_B$	H_A	$I_{E(A)}$ or $H_{E(A)}$	not considered	(200),(201)

Table E.3: Bob's Derivations (1st Impersonation Attack)

Receiver Impersonation in QKD

For simplicity, it is assumed that Eve leaves the $E(B)$-qubit unrestored.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)} \tag{204}$$

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATE(B)} \tag{205}$$

The results of Eve's receiver impersonation are shown in table E.4 (p. E7). In the first subset (row 1 - 4) Eve performs $I_{E(B)}$ and $H_{E(B)}$ on her $E(B)$-particle of the (unrestored) system (204) or (205) resulting in eqs. (207) and (209) or (208) and (210), respectively. In the second subset (row 5 - 8) Alice performs the operations. Again, every second row is obtained, due to

the restoring error in eq. (205).

The overall detection probability for any of Eve's first announcements is calculated as follows.

$$\rho_D = \frac{1}{8} * \left(4 * 0 + 1 + 1\frac{1}{2} + 2 * \left(\frac{1}{2\sqrt{2}} \right)^2 \right) = \frac{11}{32} \tag{206}$$

Eq.	Operation of Alice	Operation of Eve	Transformation of GHZ states
(207)	I_A	$I_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{TE(B)}\|+\rangle_A + \|\Phi^-\rangle_{TE(B)}\|-\rangle_A)$
(208)			$\frac{1}{2}(\|\Phi^+\rangle_{TE(B)}\|-\rangle_A + \|\Phi^-\rangle_{TE(B)}\|+\rangle_A + \|\Psi^+\rangle_{TE(B)}\|+\rangle_A + \|\Psi^-\rangle_{TE(B)}\|-\rangle_A)$
(209)	I_A	$H_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{TE(B)}\|-\rangle_A + \|\Phi^-\rangle_{TE(B)}\|+\rangle_A + \|\Psi^+\rangle_{TE(B)}\|+\rangle_A + \|\Psi^-\rangle_{TE(B)}\|-\rangle_A)$
(210)			$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{TE(B)}\|+\rangle_A + \|\Phi^-\rangle_{TE(B)}\|-\rangle_A)$
(211)	I_A	$I_{E(B)}$	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)})$
(212)			$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} - \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)})$
(213)	H_A	$I_{E(B)}$	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$
(214)			$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)}$ $+\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$

Table E.4: Results of QKD (2nd Impersonation Attack)

Table E.5 shows Alice's possible derivations of Eve's operations of the first subset. Eve's derivation of Alice operations of the second subset are listed in table E.6 (p. E8). Again, Eve can only derive Alice's operation for states $|\Psi^+\rangle_{AT}|+\rangle_{E(B)}$ and $|\Psi^-\rangle_{AT}|-\rangle_{E(B)}$, which are not taken for the key arrangement, and for states $|\Psi^+\rangle_{AT}|-\rangle_{E(B)}$ and $|\Psi^-\rangle_{AT}|+\rangle_{E(B)}$, which are not supposed to occur nor considered.

Entire state	Alice's derivation	Eve's operations	Remarks	Eq.
$\|\Phi^+\rangle_{TE(B)}\|+\rangle_A$	I_B	$I_{E(B)}$ or $H_{E(B)}$	-	(207),(210)
$\|\Phi^+\rangle_{TE(B)}\|-\rangle_A$	H_B	$I_{E(B)}$ or $H_{E(B)}$	-	(208),(209)
$\|\Phi^-\rangle_{TE(B)}\|+\rangle_A$	H_B	$I_{E(B)}$ or $H_{E(B)}$	-	(208),(209)
$\|\Phi^-\rangle_{TE(B)}\|-\rangle_A$	I_B	$I_{E(B)}$ or $H_{E(B)}$	-	(207),(210)
$\|\Psi^+\rangle_{TE(B)}\|+\rangle_A$	H_B	$I_{E(B)}$ or $H_{E(B)}$	not considered	(208),(209)
$\|\Psi^-\rangle_{TE(B)}\|-\rangle_A$	H_B	$I_{E(B)}$ or $H_{E(B)}$	not considered	(208),(209)

Table E.5: Alice's Derivations (2nd Impersonation Attack)

Entire state	Eve's derivation	Remarks	Eq.
$\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)}$	I_A or H_A	-	(211),(212),(214)
$\|\Phi^+\rangle_{AT}\|-\rangle_{E(B)}$	I_A or H_A	-	(212),(213),(214)
$\|\Phi^-\rangle_{AT}\|+\rangle_{E(B)}$	I_A or H_A	-	(212),(213),(214)
$\|\Phi^-\rangle_{AT}\|-\rangle_{E(B)}$	I_A or H_A	-	(211),(212),(214)
$\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)}$	H_A	not considered	(213),(214)
$\|\Psi^+\rangle_{AT}\|-\rangle_{E(B)}$	H_A	not considered	(214)
$\|\Psi^-\rangle_{AT}\|+\rangle_{E(B)}$	H_A	not considered	(214)
$\|\Psi^-\rangle_{AT}\|-\rangle_{E(B)}$	H_A	not considered	(213),(214)

Table E.6: Eve's Derivations (2nd Impersonation Attack)

E.5 Advanced Impersonation Attacks

During authentication the detection probabilities of all advanced impersonation attack of the original protocol 1 are maintained (see D.5, p. D16).

Impersonation of Sender and Authority

The restoring errors occur on the side of the second communication party, as Bob decodes his unencoded particles. Therefore, the consequences in the system are equal to the transformations described in the receiver impersonation of the improved proposal (see tab. E.4, p. E7). States of type $|\Omega^{\pm}\rangle_{TE(B)}|\pm\rangle_A$ of the first and $|\Omega^{\pm}\rangle_{AT}|\pm\rangle_{E(B)}$ of the second subset must be replaced here with states of type $|\Omega^{\pm}\rangle_{E(T)B}|\pm\rangle_{E(A)}$ and $|\Omega^{\pm}\rangle_{E(A)E(T)}|\pm\rangle_B$, respectively, with $|\Omega\rangle$ representing $|\Phi\rangle$ or $|\Psi\rangle$.

As Eve cannot know if Bob changes his particle knowingly or unintentionally, she is not able to deduce his operations of the first subset. For the second subset Eve additionally needs to know Bob's measurement result to correctly deduce his derivation. The difference here is that Bob can detect an attack beyond any eavesdropping test in case of $|\Psi^+\rangle_{E(A)E(T)}|-\rangle_B$ and $|\Psi^-\rangle_{E(A)E(T)}|+\rangle_B$ with the probability of $\rho_{D_{add}} = \frac{1}{32}$, since he knows the entire state of the second subset. Hence, this probability is no longer an advantage but a disadvantage for Eve, as it now may lead to her detection.

The overall detection probability for any of Eve's first announcements can be calculated like follows with the probabilities ordered according to the rows of tab. E.4.

$$\rho_D = \frac{1}{8} * \left(0 + 1 + 0 + 1 + 0 + \frac{1}{2} + 0 + \frac{1}{2}\right) = \frac{3}{8} \tag{215}$$

Impersonation of Receiver and Authority

The restoring errors occur on the side of the first communication party, due to Alice's decoding of her unencoded particles. Hence, the consequences in the system are similar to the

transformations of GHZ states in the sender impersonation of the improved proposal (see tab. E.1, p. E5). Now states of type $|\Omega^{\pm}\rangle_{TB}|\pm\rangle_{E(A)}$ of the first and $|\Omega^{\pm}\rangle_{E(A)T}|\pm\rangle_{B}$ of the second subset must be replaced by types $|\Omega^{\pm}\rangle_{E(T)E(B)}|\pm\rangle_{A}$ and $|\Omega^{\pm}\rangle_{AE(T)}|\pm\rangle_{E(B)}$, respectively, with $|\Omega\rangle$ representing $|\Phi\rangle$ or $|\Psi\rangle$.

For the first subset Alice derives exactly one operation, due to her knowledge of the x basis measurement result. Since Alice changes the system also by restoring, Eve cannot deduce Alice's operations of the second subset.

The detection probability for any of Eve's first announcements remains as in the first advanced impersonation attack of the proposal. The probabilities are ordered according to table E.1.

$$\rho_D = \frac{1}{8} * \left(0 + \frac{1}{2} + 0 + \frac{1}{2} + 0 + 1 + 0 + 1\right) = \frac{3}{8} \tag{216}$$

Alice can detect Eve beyond any test in case of $|\Psi^{+}\rangle_{E(T)E(B)}|-\rangle_{A}$ and $|\Psi^{-}\rangle_{E(T)E(B)}|+\rangle_{A}$, that is with the probability of $\rho_{D_{add}} = \frac{1}{32}$, since Alice knows the entire state of the first subset.

Impersonation of the Authority

As shown in the first and second advanced impersonation, the restoring problem on one side leads to a total failure of the attack. In an impersonation of Trent the restoring problem occurs on both sides. Hence, Eve cannot be successful in this attack. For simplicity, the results in table E.7 (p. E10) and the detection probability are derived only for the first subset. The results for the second subset can be calculated accordingly. The detection probability of the second subset is approximately on the same scale as the probability of the first subset. According to the rows of table E.7, the detection probability of the first subset is derived as follows.

$$\rho_D = \frac{1}{8} * \left(0 + 1 + \frac{1}{2} + \frac{3}{4} + 0 + 1 + \frac{1}{2} + \frac{1}{2}\right) = \frac{17}{32} \tag{217}$$

Operation of Alice	Operation of Bob	Transformation of GHZ states
I_A	I_B	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(T)B}\|+\rangle_A + \|\Phi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{2}(\|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Psi^+\rangle_{E(T)B}\|+\rangle_A + \|\Psi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{2}(\|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Phi^+\rangle_{E(T)B}\|+\rangle_A - \|\Phi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{E(T)B}\|+\rangle_A - \|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Phi^-\rangle_{E(T)B}\|-\rangle_A$ $+ \|\Psi^+\rangle_{E(T)B}\|+\rangle_A + \|\Psi^+\rangle_{E(T)B}\|-\rangle_A + \|\Psi^-\rangle_{E(T)B}\|+\rangle_A - \|\Psi^-\rangle_{E(T)B}\|-\rangle_A)$
I_A	H_B	$\frac{1}{2}(\|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Psi^+\rangle_{E(T)B}\|+\rangle_A + \|\Psi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(T)B}\|+\rangle_A + \|\Phi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{2}(\|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Phi^+\rangle_{E(T)B}\|+\rangle_A - \|\Phi^-\rangle_{E(T)B}\|-\rangle_A)$
		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{E(T)B}\|+\rangle_A - \|\Phi^+\rangle_{E(T)B}\|-\rangle_A + \|\Phi^-\rangle_{E(T)B}\|+\rangle_A + \|\Phi^-\rangle_{E(T)B}\|-\rangle_A$ $+ \|\Psi^+\rangle_{E(T)B}\|+\rangle_A + \|\Psi^+\rangle_{E(T)B}\|-\rangle_A + \|\Psi^-\rangle_{E(T)B}\|+\rangle_A - \|\Psi^-\rangle_{E(T)B}\|-\rangle_A)$

Table E.7: Results of QKD in the first Subset (3rd Advanced Impersonation Attack)

Appendix F

Security Results: Protocol 2

All derivations refer to the security analysis of protocol 2 (s. 5.3, pp. 47).

F.1 Eavesdropping of Trent (s. 5.3.1, p. 47)

Depending on Alice's operations the original state $|\theta_i\rangle_{ATB}$ is transformed to one of the following states (218) or (219).

$$\begin{aligned} H_A \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \end{aligned} \tag{218}$$

$$\begin{aligned} H_A X_A \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}\right) \\ = \quad & H_A\left(\frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{ATB}\right) \\ = \quad & \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATB} \end{aligned} \tag{219}$$

If Trent performs an additional Hadamard operation on the A-qubit after he receives it from Alice ($H_{T(A)}$), only Alice's bit flip operation is preserved.

$$\begin{aligned} H_{T(A)} \quad & \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \end{aligned} \tag{220}$$

$$\begin{aligned} H_{T(A)} \quad & \left(\frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATB}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{ATB} \end{aligned} \tag{221}$$

With a measurement of the transformed A-particle and his own T-qubit in the z basis Trent is able to derive Alice's operations and the message bits. If both qubits have the same result (eq. (220)), Alice has performed a Hadamard operation. Thus, her message bit is 0. In case of different outcomes (eq. (221)), Alice has first flipped her bit before performing a Hadamard

operation. Hence, her message bit is 1.

Trent's intermediate step certainly increases the error rate, because the resulting system (220) or (221) leaves Trent no choice but to announce a random Bell state. Additionally, Bob's qubit collapses into a fixed state by Trent's measurements. Thus, his x basis measurement result is random. Unfortunately, the higher error rate is observed at the time the message already leaked out to Trent.

F.2 Eavesdropping on Authentication (s. 5.3.2, p. 48)

As authentication exactly proceeds as in protocol 1, see D.2 (p. D2) for detailed calculations.

F.3 Eavesdropping on QDC (s. 5.3.3, p. 48)

Translucent Attack (A) on Alice's particles

After Alice's and Eve's operations the system changes like follows. The upper sign line represent the state after H_A, whereas the lower line denotes $H_A X_A$.

$$
\begin{aligned}
|\xi_A\rangle &= U_E\left(\frac{1}{2}(|000\rangle \pm |100\rangle + |011\rangle \mp |111\rangle)_{ATB} \otimes |E\rangle_E\right) \\
&= \frac{1}{2}\Big(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|100\rangle_{ATB}|e_{01}\rangle_E \pm \alpha'|100\rangle_{ATB}|e_{11}\rangle_E \pm \beta'|000\rangle_{ATB}|e_{10}\rangle_E + \\
&\qquad \alpha|011\rangle_{ATB}|e_{00}\rangle_E + \beta|111\rangle_{ATB}|e_{01}\rangle_E \mp \alpha'|111\rangle_{ATB}|e_{11}\rangle_E \mp \beta'|011\rangle_{ATB}|e_{10}\rangle_E\Big) \\
&= \frac{1}{8} * 4\Big(|000\rangle_{ATB}(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle)_E + |100\rangle_{ATB}(\beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + \\
&\qquad |011\rangle_{ATB}(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle)_E + |111\rangle_{ATB}(\beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E\Big) \\
&= \frac{1}{4}\Big(|\Phi^+\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + && \text{(i)} \\
&\qquad |\Phi^+\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + && \text{(ii)} \\
&\qquad |\Phi^-\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle - \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + && \text{(iii)} \\
&\qquad |\Phi^-\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle \pm \beta'|e_{10}\rangle + \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + && \text{(iv)} \\
&\qquad |\Psi^+\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E - && \text{(v)} \\
&\qquad |\Psi^+\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + && \text{(vi)} \\
&\qquad |\Psi^-\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E - && \text{(vii)} \\
&\qquad |\Psi^-\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E\Big) && \text{(viii)}
\end{aligned}
\tag{222}
$$

The detection probability can be derived by comparing this outcome with the expected results according to table 5.1 (p. 47).

1. ρ_D for H_A (states (i), (iv), (vi), and (vii) differ from the 1st row of tab. 5.1):

$$\begin{aligned}\rho_D(H_A) &= \left(\frac{1}{4}\right)^2 * 4 * (\alpha^2 + \beta^2 + \alpha'^2 + \beta'^2) \\ &= \frac{1}{4} * (1 - \beta^2 + \beta'^2 + \beta^2 + 1 - \beta'^2) \\ &= \frac{1}{2}\end{aligned} \tag{223}$$

2. ρ_D for $H_A X_A$ (states (ii), (iii), (v), and (viii) differ from the 2nd row of tab. 5.1):

$$\begin{aligned}\rho_D(H_A X_A) &= \left(\frac{1}{4}\right)^2 * 4 * (\alpha^2 + \beta^2 + \alpha'^2 + \beta'^2) \\ &= \frac{1}{2}\end{aligned} \tag{224}$$

The overall detection probability amounts to $\frac{1}{2}$.

$$\rho_D = \frac{1}{2} * \left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{2} \tag{225}$$

Translucent Attack (B) on Alice's particles

After Alice's and Eve's operations the system changes to one of the following states (226) or (227).

$$\begin{aligned}|\xi_B\rangle_1 &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\ &= \frac{1}{2}(|0000\rangle + |1001\rangle + |0110\rangle - |1111\rangle)_{ATBE} \\ &= \frac{1}{2\sqrt{2}}\Big(|\Phi^+\rangle_{AT}|+\rangle_B|-\rangle_E + |\Phi^+\rangle_{AT}|-\rangle_B|+\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|+\rangle_E + |\Phi^-\rangle_{AT}|-\rangle_B|-\rangle_E + \\ &\qquad |\Psi^+\rangle_{AT}|+\rangle_B|+\rangle_E - |\Psi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Psi^-\rangle_{AT}|+\rangle_B|-\rangle_E - |\Psi^-\rangle_{AT}|-\rangle_B|+\rangle_E\Big)\end{aligned} \tag{226}$$

$$\begin{aligned}|\xi_B\rangle_2 &= U_E\left(\frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\ &= \frac{1}{2}(|0000\rangle - |1001\rangle + |0110\rangle + |1111\rangle)_{ATBE} \\ &= \frac{1}{2\sqrt{2}}\Big(|\Phi^+\rangle_{AT}|+\rangle_B|+\rangle_E + |\Phi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|-\rangle_E + |\Phi^-\rangle_{AT}|-\rangle_B|+\rangle_E + \\ &\qquad |\Psi^+\rangle_{AT}|+\rangle_B|-\rangle_E - |\Psi^+\rangle_{AT}|-\rangle_B|+\rangle_E + |\Psi^-\rangle_{AT}|+\rangle_B|+\rangle_E - |\Psi^-\rangle_{AT}|-\rangle_B|-\rangle_E\Big)\end{aligned} \tag{227}$$

Again, the detection probability can be calculated by comparing the result of eqs. (226) and (227) with the first and second row in table 5.1 (p. 47), respectively.

$$\rho_D(|\xi_B\rangle_1) = \left(\frac{1}{2\sqrt{2}}\right)^2 * 4 = \frac{1}{2} \tag{228}$$

$$\rho_D(|\xi_B\rangle_2) = \left(\frac{1}{2\sqrt{2}}\right)^2 * 4 = \frac{1}{2} \tag{229}$$

The overall detection probability sums up to $\frac{1}{2}$.

$$\rho_D = \frac{1}{2} * \left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{2} \tag{230}$$

Intercept-resend Attack

After Alice's operations the system is in the following state. The upper sign line denotes H_A and the lower one represents $H_A X_A$.

$$\frac{1}{2}(|000\rangle \pm |100\rangle + |011\rangle \mp |111\rangle)_{ATB} \tag{231}$$

Eve measures 0 and 1 with the same probability for both operations.

F.4 Simple Impersonation Attacks (s. 5.3.4, p. 49)

Sender or Receiver Impersonation in Authentication

In an impersonation of Alice or Bob the detection probability during the first eavesdropping test totals $\frac{1}{4}$ with both of Eve's options – guessing the authentication key or measuring the undecoded particle (see D.4, p. D12 for details).

Sender Impersonation in QDC

The following states eqs. (232) – (235) occur while restoring the A-qubit in an impersonation of Alice.

In case of $id_{iA} = 0$:

$$I_{E(A)} \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB}\right) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{232}$$

$$H_{E(A)} \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB}\right) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{233}$$

In case of $id_{iA} = 1$:

$$I_{E(A)} \quad \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB}\right)$$
$$= \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{234}$$
$$H_{E(A)} \quad \left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB}\right)$$
$$= \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{235}$$

In QDC the operations $H_{E(A)}$ and $H_{E(A)}X_{E(A)}$ on states (232) and (235) result in correct transformations, whereas Eve's restoring errors is maintained in the other states.

$$H_{E(A)}\ on\ (232): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{236}$$
$$H_{E(A)}\ on\ (233): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{237}$$
$$H_{E(A)}\ on\ (234): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{238}$$
$$H_{E(A)}\ on\ (235): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{239}$$
$$H_{E(A)}X_{E(A)}\ on\ (232): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{E(A)TB} \tag{240}$$
$$H_{E(A)}X_{E(A)}\ on\ (233): \quad \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{E(A)TB} \tag{241}$$
$$H_{E(A)}X_{E(A)}\ on\ (234): \quad \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{E(A)TB} \tag{242}$$
$$H_{E(A)}X_{E(A)}\ on\ (235): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{E(A)TB} \tag{243}$$

If Eve does not decode the A-qubit, the analysis is simplified, since only eqs. (232) and (234), and (236), (238), (240), and (242) must be considered. The simplification leads to the same results.

Table F.1 lists all transformations after Eve's operations and Trent's and Bob's measurements during the sender impersonation.

Eq.	Eve's operation	Transformation of GHZ states
(244)	$H_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|-\rangle_B + \|\Phi^-\rangle_{E(A)T}\|+\rangle_B + \|\Psi^+\rangle_{E(A)T}\|+\rangle_B - \|\Psi^-\rangle_{E(A)T}\|-\rangle_B)$
(245)		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B)$
(246)	$H_{E(A)}X_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B - \|\Psi^+\rangle_{E(A)T}\|-\rangle_B + \|\Psi^-\rangle_{E(A)T}\|+\rangle_B)$
(247)		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)T}\|-\rangle_B + \|\Phi^-\rangle_{E(A)T}\|+\rangle_B)$

Table F.1: Results of QDC (1st Impersonation Attack)

If Eve announces her result, the wrong transformations (245) and (247) include full detection probability. Hence, the overall detection probability amounts to $\frac{1}{2}$.

$$\rho_D = \frac{1}{4} * (0 + 1 + 0 + 1) = \frac{1}{2} \tag{248}$$

Table F.2 shows Bob's derivations of Alice's (Eve's) operations. Eve cannot control the message bit for any occurrence of $|\Phi^{\pm}\rangle_{E(A)T}$. In fact, Bob deduces exactly one outcome according to his x basis measurement result. But Eve cannot know which, since she receives the states with both of her operations. Hence, her success probability totals $\frac{1}{4}$.

$$\rho_S = \frac{1}{4} * (\frac{1}{2} + 0 + \frac{1}{2} + 0) = \frac{1}{4} \tag{249}$$

Entire state	Bob's derivation	Eve's operation	Eq.
$\|\Phi^+\rangle_{E(A)T}\|+\rangle_B$	$H_A X_A$	$H_{E(A)}$ or $H_{E(A)}X_{E(A)}$	(245),(246)
$\|\Phi^+\rangle_{E(A)T}\|-\rangle_B$	H_A	$H_{E(A)}$ or $H_{E(A)}X_{E(A)}$	(244),(247)
$\|\Phi^-\rangle_{E(A)T}\|+\rangle_B$	H_A	$H_{E(A)}$ or $H_{E(A)}X_{E(A)}$	(244),(247)
$\|\Phi^-\rangle_{E(A)T}\|-\rangle_B$	$H_A X_A$	$H_{E(A)}$ or $H_{E(A)}X_{E(A)}$	(245),(246)
$\|\Psi^+\rangle_{E(A)T}\|+\rangle_B$	H_A	$H_{E(A)}$	(244)
$\|\Psi^+\rangle_{E(A)T}\|-\rangle_B$	$H_A X_A$	$H_{E(A)}X_{E(A)}$	(246)
$\|\Psi^-\rangle_{E(A)T}\|+\rangle_B$	$H_A X_A$	$H_{E(A)}X_{E(A)}$	(246)
$\|\Psi^-\rangle_{E(A)T}\|-\rangle_B$	H_A	$H_{E(A)}$	(244)

Table F.2: Bob's Derivations (1st Impersonation Attack)

Receiver Impersonation in QDC

While restoring the B-qubit in an impersonation of Bob (2nd impersonation attack), two right system transformations (eqs. (250) and (253)) and two wrong states (eqs. (251) and (252)) can occur.

In case of $id_{iB} = 0$:

$$\begin{aligned} I_{E(B)} & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)}\right) \\ = & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)} \end{aligned} \tag{250}$$

$$\begin{aligned} H_{E(B)} & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)}\right) \\ = & \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATE(B)} \end{aligned} \tag{251}$$

In case of $id_{iB} = 1$:

$$\begin{aligned} I_{E(B)} \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATE(B)} \end{aligned} \tag{252}$$

$$\begin{aligned} H_{E(B)} \quad & \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)} \end{aligned} \tag{253}$$

Alice's operations H_A and $H_A X_A$ on states (250) and (253) lead to correct states. In the other cases Eve's errors are maintained.

$$H_A \; on \; (250): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATE(B)} \tag{254}$$

$$H_A \; on \; (251): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |001\rangle + |101\rangle + |010\rangle - |110\rangle - |011\rangle + |111\rangle)_{ATE(B)} \tag{255}$$

$$H_A \; on \; (252): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |001\rangle + |101\rangle + |010\rangle - |110\rangle - |011\rangle + |111\rangle)_{ATE(B)} \tag{256}$$

$$H_A \; on \; (253): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATE(B)} \tag{257}$$

$$H_A X_A \; on \; (250): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATE(B)} \tag{258}$$

$$H_A X_A \; on \; (251): \quad \frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle + |001\rangle - |101\rangle + |010\rangle + |110\rangle - |011\rangle - |111\rangle)_{ATE(B)} \tag{259}$$

$$H_A X_A \; on \; (252): \quad \frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle + |001\rangle - |101\rangle + |010\rangle + |110\rangle - |011\rangle - |111\rangle)_{ATE(B)} \tag{260}$$

$$H_A X_A \; on \; (253): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{ATE(B)} \tag{261}$$

Table F.3 (p. F8) lists all transformations after Alice's operations and Trent's and Eve's measurements. It shows that Alice can detect Eve with the probability of $\frac{1}{2}$ in eqs. (264) and (266). Hence, the overall detection probability totals $\frac{1}{4}$.

$$\rho_D \quad = \quad \frac{1}{4} * (0 + \frac{1}{2} + 0 + \frac{1}{2}) = \frac{1}{4} \tag{262}$$

Table F.4 (p. F8) presents Eve's possible derivations of Alice's operation. Eve receives all entire results by both of Alice's operations. Hence, Eve cannot deduce any operation nor any message bit in the receiver impersonation.

Eq.	Alice's operation	Transformation of GHZ states
(263)	H_A	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$
(264)		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} +$ $\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$
(265)	$H_A X_A$	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} - \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)})$
(266)		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} - \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} -$ $\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$

Table F.3: Results of QDC (2nd Impersonation Attack)

Entire state	Alice's operation	Eq.
$\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)}$	H_A or $H_A X_A$	(264),(265),(266)
$\|\Phi^+\rangle_{AT}\|-\rangle_{E(B)}$	H_A or $H_A X_A$	(263),(264),(266)
$\|\Phi^-\rangle_{AT}\|+\rangle_{E(B)}$	H_A or $H_A X_A$	(263),(264),(266)
$\|\Phi^-\rangle_{AT}\|-\rangle_{E(B)}$	H_A or $H_A X_A$	(264),(265),(266)
$\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)}$	H_A or $H_A X_A$	(263),(264),(266)
$\|\Psi^+\rangle_{AT}\|-\rangle_{E(B)}$	H_A or $H_A X_A$	(264),(265),(264)
$\|\Psi^-\rangle_{AT}\|+\rangle_{E(B)}$	H_A or $H_A X_A$	(264),(265),(264)
$\|\Psi^-\rangle_{AT}\|-\rangle_{E(B)}$	H_A or $H_A X_A$	(263),(264),(266)

Table F.4: Eve's Derivation (2nd Impersonation Attack)

F.5 Advanced Impersonation Attacks (s. 5.3.5, p. 51)

During authentication the results of the advanced impersonation attack of protocol 1 are maintained (see D.5, p. D16), i.e. a detection probability of $\frac{1}{4}$ in the first and second attack and a detection probability of $\frac{3}{8}$ in the third attack.

Impersonation of Sender and Authority

Bob correctly decodes the non-encoded B-particles.

In case of $id_{iB} = 0$:

$$\begin{aligned} & I_B \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \end{aligned} \tag{267}$$

In case of $id_{iB} = 1$:

$$\begin{aligned} & H_B \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \end{aligned} \tag{268}$$

In QDC the system changes to one of the following states (269) – (272) when following the protocol.

$$H_{E(A)} \text{ on } (267): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{269}$$

$$H_{E(A)} \text{ on } (268): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |001\rangle + |101\rangle + |010\rangle - |110\rangle - |011\rangle + |111\rangle)_{E(A)E(T)B} \tag{270}$$

$$H_{E(A)}X_{E(A)} \text{ on } (267): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{E(A)E(T)B} \tag{271}$$

$$H_{E(A)}X_{E(A)} \text{ on } (268): \quad \frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle + |001\rangle - |101\rangle + |010\rangle + |110\rangle - |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{272}$$

In the case that Eve measures her $E(A)$- and $E(T)$-particles in the Bell basis without performing any operation for QDC on the $E(A)$-qubit, the system is in the state

$$\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{E(A)E(T)}|+\rangle_B + |\Phi^-\rangle_{E(A)E(T)}|-\rangle_B\right) \tag{273}$$

with eq. (267) and in

$$\frac{1}{2}\left(|\Phi^+\rangle_{E(A)E(T)}|+\rangle_B + |\Phi^+\rangle_{E(A)E(T)}|-\rangle_B + |\Phi^-\rangle_{E(A)E(T)}|+\rangle_B - |\Phi^-\rangle_{E(A)E(T)}|-\rangle_B\right) \tag{274}$$

with eq. (268). That way Eve cannot be successful.

Eve can also not be successful when following the protocol (see tab. F.5). Furthermore, the detection probability totals 25 % for every second check qubit.

$$\rho_D = \frac{1}{4} * \left(0 + \frac{1}{2} + 0 + \frac{1}{2}\right) = \frac{1}{4} \tag{275}$$

Eve's operation	Transformation of GHZ states
$H_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)E(T)}\|-\rangle_B + \|\Phi^-\rangle_{E(A)E(T)}\|+\rangle_B + \|\Psi^+\rangle_{E(A)E(T)}\|+\rangle_B - \|\Psi^-\rangle_{E(A)E(T)}\|-\rangle_B)$
	$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{E(A)E(T)}\|+\rangle_B - \|\Phi^+\rangle_{E(A)E(T)}\|-\rangle_B + \|\Phi^-\rangle_{E(A)E(T)}\|+\rangle_B + \|\Phi^-\rangle_{E(A)E(T)}\|-\rangle_B + \|\Psi^+\rangle_{E(A)E(T)}\|+\rangle_B + \|\Psi^+\rangle_{E(A)E(T)}\|-\rangle_B - \|\Psi^-\rangle_{E(A)E(T)}\|+\rangle_B + \|\Psi^-\rangle_{E(A)E(T)}\|-\rangle_B)$
$H_{E(A)}X_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)E(T)}\|+\rangle_B + \|\Phi^-\rangle_{E(A)E(T)}\|-\rangle_B - \|\Psi^+\rangle_{E(A)E(T)}\|-\rangle_B + \|\Psi^-\rangle_{E(A)E(T)}\|+\rangle_B)$
	$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{E(A)E(T)}\|+\rangle_B + \|\Phi^+\rangle_{E(A)E(T)}\|-\rangle_B + \|\Phi^-\rangle_{E(A)E(T)}\|+\rangle_B - \|\Phi^-\rangle_{E(A)E(T)}\|-\rangle_B - \|\Psi^+\rangle_{E(A)E(T)}\|+\rangle_B + \|\Psi^+\rangle_{E(A)E(T)}\|-\rangle_B + \|\Psi^-\rangle_{E(A)E(T)}\|+\rangle_B + \|\Psi^-\rangle_{E(A)E(T)}\|-\rangle_B)$

Table F.5: Results of QDC (1st Advanced Impersonation Attack)

Impersonation of Receiver and Authority

After Alice's decoding of the unencoded particles the state of the system changes to one of the states (276) or (277).

In case of $id_{iA} = 0$:

$$\begin{aligned} & I_A \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)}\right) \\ = \quad & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)} \end{aligned} \tag{276}$$

In case of $id_{iA} = 1$:

$$\begin{aligned} & H_A \quad \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)}\right) \\ = \quad & \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \end{aligned} \tag{277}$$

Alice's operations transform the system in QDC to one of the following states (278) – (281).

$$H_A \; on \; (276): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{278}$$

$$H_A \; on \; (277): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{279}$$

$$H_A X_A \; on \; (276): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{AE(T)E(B)} \tag{280}$$

$$H_A X_A \; on \; (277): \quad \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{AE(T)E(B)} \tag{281}$$

Table F.6 lists the transformations of the system after all operations and measurements. Although Eve is in possession of all particles of the system, she can only successfully deduce Alice's operation with the states $|\Psi^{\pm}\rangle_{AE(T)}$, that is with a probability of 25 % per GHZ state. The detection probability totals 50 % for every second check qubit.

$$\rho_S = \frac{1}{4} * \left(4 * \frac{1}{4}\right) = \frac{1}{4} \tag{282}$$

$$\rho_D = \frac{1}{4} * (0 + 1 + 0 + 1) = \frac{1}{2} \tag{283}$$

Alice's operation	Transformation of GHZ states
H_A	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AE(T)}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AE(T)}\|+\rangle_{E(B)} - \|\Psi^-\rangle_{AE(T)}\|-\rangle_{E(B)})$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AE(T)}\|-\rangle_{E(B)})$
$H_A X_A$	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AE(T)}\|-\rangle_{E(B)} - \|\Psi^+\rangle_{AE(T)}\|-\rangle_{E(B)} + \|\Psi^-\rangle_{AE(T)}\|+\rangle_{E(B)})$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AE(T)}\|+\rangle_{E(B)})$

Table F.6: Results of QDC (2nd Advanced Impersonation Attack)

An additional Hadamard operation ($H_{E(A)}$) does not improve Eve's result, because not only I_A and $X_A I_A$ are preserved but also H_A and $X_A H_A$ (see eqs. (284) – (287)). Hence, Eve cannot reach Trent's position in eavesdropping.

$H_{E(A)}$ *on* (278) :

$$H_{E(A)}H_A I_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = I_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{284}$$

$H_{E(A)}$ *on* (279) :

$$H_{E(A)}H_A H_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = H_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{285}$$

$H_{E(A)}$ *on* (280) :

$$H_{E(A)}H_A X_A I_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = X_A I_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{AE(T)E(B)} \tag{286}$$

$H_{E(A)}$ *on* (281) :

$$H_{E(A)}H_A X_A H_A\left(|\theta_i\rangle_{AE(T)E(B)}\right) = X_A H_A\left(|\theta_i\rangle_{AE(T)E(B)}\right)$$
$$= \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{AE(T)E(B)} \tag{287}$$

Impersonation of the Authority

After Alice's and Bob's decoding the system changes to one of the states (288) – (291).

$$I_A I_B\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right)$$
$$= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{288}$$

$$I_A H_B\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right)$$
$$= \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{289}$$

$$H_A I_B\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right)$$
$$= \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{290}$$

$$H_A H_B\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B}\right)$$
$$= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{291}$$

The restoring problems go through all of Alice's transformations of the system leading to eqs. (292) – (299) and table F.7.

$$H_A \text{ on } (288): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{292}$$

$$H_A \text{ on } (289): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{293}$$

$$H_A \text{ on } (290): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{294}$$

$$H_A \text{ on } (291): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{295}$$

$$H_AX_A \text{ on } (288): \quad \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle + |111\rangle)_{AE(T)B} \tag{296}$$

$$H_AX_A \text{ on } (289): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle - |100\rangle - |101\rangle + |010\rangle - |011\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{297}$$

$$H_AX_A \text{ on } (290): \quad \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{AE(T)B} \tag{298}$$

$$H_AX_A \text{ on } (291): \quad \frac{1}{2}(|000\rangle + |001\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{299}$$

Eq.	Alice's operation	Transformation of GHZ states
(300)	H_A	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|+\rangle_B - \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
(301)		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B - \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B +$ $\|\Psi^+\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|-\rangle_B - \|\Psi^-\rangle_{AE(T)}\|+\rangle_B + \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
(302)		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$
(303)		$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B - \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$
(304)	H_AX_A	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B - \|\Psi^+\rangle_{AE(T)}\|-\rangle_B + \|\Psi^-\rangle_{AE(T)}\|+\rangle_B)$
(305)		$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B - \|\Phi^-\rangle_{AE(T)}\|-\rangle_B -$ $\|\Psi^+\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|-\rangle_B + \|\Psi^-\rangle_{AE(T)}\|+\rangle_B + \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
(306)		$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B)$
(307)		$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B - \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$

Table F.7: Results of QDC (3rd Advanced Impersonation Attack)

Eqs. (300) and (304) do not include detection probability, but there is full detection probability in eqs. (302) and (306), and a detection probability of $\frac{1}{2}$ in eqs. (301), (303), (305), and (307). Hence, the overall detection probability can be calculated as follows.

$$\rho_D = \frac{1}{8} * \left(2 * 0 + 2 * 1 + 4 * \frac{1}{2}\right) = \frac{1}{2} \tag{308}$$

After an additional Hadamard operation on the A-qubit ($H_{E(A)}$), Eve restores states (288) – (291) for a previous H_A, since $H_{E(A)}H_AO_AO_B = O_AO_B$ with O representing any operation I or H (eqs. (309) – (312)). For a previous H_AX_A only Alice's bit flip is preserved, i.e. $H_{E(A)}H_AX_AO_AO_B = X_AO_AO_B$ (eqs. (313) – (316)). However, Eve cannot distinguish between

H_A and $H_A X_A$ when measuring the A- and the T-qubit. Hence, Eve cannot reach Trent's superior position.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{309}$$

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{310}$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{311}$$

$$\frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{312}$$

$$\frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{AE(T)B} \tag{313}$$

$$\frac{1}{2}(|100\rangle + |101\rangle + |010\rangle - |011\rangle)_{AE(T)B} \tag{314}$$

$$\frac{1}{2}(|100\rangle + |000\rangle + |111\rangle - |011\rangle)_{AE(T)B} \tag{315}$$

$$\frac{1}{2\sqrt{2}}(|100\rangle + |101\rangle + |000\rangle + |001\rangle + |110\rangle - |111\rangle - |010\rangle + |011\rangle)_{AE(T)B} \tag{316}$$

Appendix G

Security Results: Improved Proposal 2

All derivations refer to the security analysis of the improved proposal of protocol 2 (s. 5.5.2, pp. 56).

G.1 Eavesdropping of Trent

After Alice's transformations the original state $|\theta_i\rangle_{ATB}$ changes to one of the following states (317) – (318).

$$H_A(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \quad (317)$$

$$H_A\sigma_{zA}(|\theta_i\rangle_{ATB}) = \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{ATB} \quad (318)$$

With a measurement of Alice's and his qubit in the z basis Trent cannot distinguish between Alice's operations. He measures the results $|0\rangle_A|0\rangle_T$, $|1\rangle_A|0\rangle_T$, $|0\rangle_A|1\rangle_T$, and $|1\rangle_A|1\rangle_T$ with the same probability of $\frac{1}{4}$ for both of her operations.

In case of applying an additional Hadamard operation before measurement, Trent receives the results $|0\rangle_A|0\rangle_T$ or $|1\rangle_A|1\rangle_T$ with the same probability of $\frac{1}{2}$ for both of Alice's operations (eqs. (319) and (320)).

$$H_{T(A)}H_A\left(|\theta_i\rangle_{ATB}\right) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB} \quad (319)$$

$$H_{T(A)}H_A\sigma_{zA}\left(|\theta_i\rangle_{ATB}\right) = \sigma_{zA}\left(|\theta_i\rangle_{ATB}\right) = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ATB} \quad (320)$$

Hence, Trent's success probability is $\rho_S = 0$. Moreover, Trent's intermediate step increases the error rate, because Trent must announce a random Bell state and Bob's qubit collapses into a fixed state.

G.2 Eavesdropping on Authentication

As authentication exactly proceeds as in protocol 1, see D.2 (p. D2) for detailed calculations.

G.3 Eavesdropping on QKD

Translucent Attack (A) on Alice's particles

After Alice's and Eve's operations the system changes as follows, with the upper sign line representing the state after H_A and the lower line denoting it after $H_A\sigma_{zA}$.

$$\begin{aligned}
|\xi_A\rangle &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle \pm |011\rangle \mp |111\rangle)_{ATB} \otimes |E\rangle_E\right) \\
&= \frac{1}{2}\Big(\alpha|000\rangle_{ATB}|e_{00}\rangle_E + \beta|100\rangle_{ATB}|e_{01}\rangle_E + \alpha'|100\rangle_{ATB}|e_{11}\rangle_E + \beta'|000\rangle_{ATB}|e_{10}\rangle_E \pm \\
&\qquad \alpha|011\rangle_{ATB}|e_{00}\rangle_E \pm \beta|111\rangle_{ATB}|e_{01}\rangle_E \mp \alpha'|111\rangle_{ATB}|e_{11}\rangle_E \mp \beta'|011\rangle_{ATB}|e_{10}\rangle_E\Big) \\
&= \frac{1}{4}\Big(|\Phi^+\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle \pm \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + \\
&\qquad |\Phi^+\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle \mp \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + \\
&\qquad |\Phi^-\rangle_{AT}|+\rangle_B(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle \mp \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E + \\
&\qquad |\Phi^-\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle + \beta'|e_{10}\rangle \pm \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + \\
&\qquad |\Psi^+\rangle_{AT}|+\rangle_B(\pm\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle)_E - \\
&\qquad |\Psi^+\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle - \beta'|e_{10}\rangle \mp \beta|e_{01}\rangle \mp \alpha'|e_{11}\rangle)_E + \\
&\qquad |\Psi^-\rangle_{AT}|+\rangle_B(\pm\alpha|e_{00}\rangle \mp \beta'|e_{10}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle)_E - \\
&\qquad |\Psi^-\rangle_{AT}|-\rangle_B(\alpha|e_{00}\rangle - \beta'|e_{10}\rangle \pm \beta|e_{01}\rangle \pm \alpha'|e_{11}\rangle)_E\Big)
\end{aligned} \tag{321}$$

The overall detection probability ρ_D remains $\frac{1}{2}$.

Translucent Attack (B) on Alice's particles

After Alice's and Eve's operations the system changes as follows.

$$\begin{aligned}
|\xi_B\rangle_1 &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |1001\rangle + |0110\rangle - |1111\rangle)_{ATBE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^+\rangle_{AT}|+\rangle_B|-\rangle_E + |\Phi^+\rangle_{AT}|-\rangle_B|+\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|+\rangle_E + |\Phi^-\rangle_{AT}|-\rangle_B|-\rangle_E + \\
&\qquad |\Psi^+\rangle_{AT}|+\rangle_B|+\rangle_E - |\Psi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Psi^-\rangle_{AT}|+\rangle_B|-\rangle_E - |\Psi^-\rangle_{AT}|-\rangle_B|+\rangle_E\Big)
\end{aligned} \tag{322}$$

$$
\begin{aligned}
|\xi_B\rangle_2 &= U_E\left(\frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{ATB} \otimes |0\rangle_E\right) \\
&= \frac{1}{2}(|0000\rangle + |1001\rangle - |0110\rangle + |1111\rangle)_{ATBE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^+\rangle_{AT}|+\rangle_B|+\rangle_E + |\Phi^+\rangle_{AT}|-\rangle_B|-\rangle_E + |\Phi^-\rangle_{AT}|+\rangle_B|-\rangle_E + |\Phi^-\rangle_{AT}|-\rangle_B|+\rangle_E - \\
&\qquad |\Psi^+\rangle_{AT}|+\rangle_B|-\rangle_E + |\Psi^+\rangle_{AT}|-\rangle_B|+\rangle_E - |\Psi^-\rangle_{AT}|+\rangle_B|+\rangle_E + |\Psi^-\rangle_{AT}|-\rangle_B|-\rangle_E\Big)
\end{aligned} \tag{323}
$$

The overall detection probability ρ_D remains $\frac{1}{2}$.

Intercept-resend Attack

After Alice's operations the system is in the following state. The upper sign line denotes H_A and the lower one represents $H_A\sigma_{zA}$.

$$\frac{1}{2}(|000\rangle + |100\rangle \pm |011\rangle \mp |111\rangle)_{ATB} \tag{324}$$

Eve measures 0 and 1 with the same probability for both operations.

G.4 Simple Impersonation Attacks

Sender or Receiver Impersonation in Authentication

The detection probability during authentication remains $\frac{1}{4}$ per check qubit (see D.4 for details).

Sender Impersonation in QDC

The system changes to one of the following states (325) or (326) while restoring the A-qubit in the sender impersonation.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{325}$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{326}$$

Eve's operations during QDC on states (325) and (326) transforms the system to one of the following states (327) – (330) resulting in table G.1 (p. G4).

$$H_{E(A)}\ on\ (325): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)TB} \tag{327}$$

$$H_{E(A)}\ on\ (326): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)TB} \tag{328}$$

$$H_{E(A)}\sigma_{zE(A)}\ on\ (325): \quad \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{E(A)TB} \tag{329}$$

$$H_{E(A)}\sigma_{zE(A)}\ on\ (326): \quad \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{E(A)TB} \tag{330}$$

Eve's operation	Transformation of GHZ states
$H_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|-\rangle_B + \|\Phi^-\rangle_{E(A)T}\|+\rangle_B + \|\Psi^+\rangle_{E(A)T}\|+\rangle_B - \|\Psi^-\rangle_{E(A)T}\|-\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B)$
$H_{E(A)}X_{E(A)}$	$\frac{1}{2}(\|\Phi^+\rangle_{E(A)T}\|+\rangle_B + \|\Phi^-\rangle_{E(A)T}\|-\rangle_B + \|\Psi^+\rangle_{E(A)T}\|-\rangle_B - \|\Psi^-\rangle_{E(A)T}\|+\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Psi^+\rangle_{E(A)T}\|+\rangle_B - \|\Psi^-\rangle_{E(A)T}\|-\rangle_B)$

Table G.1: Results of QDC (1st Impersonation Attack)

The overall detection probability remains $\frac{1}{2}$ when Eve announces her result. Her success probability of $\frac{1}{4}$ is also maintained.

$$\rho_D = \frac{1}{4} * (0 + 1 + 0 + 1) = \frac{1}{2} \tag{331}$$

$$\rho_S = \frac{1}{4} * \left(\frac{1}{2} + 0 + \frac{1}{2} + 0\right) = \frac{1}{4} \tag{332}$$

Receiver Impersonation in QDC

The system changes to one of the following states (333) – (334) while restoring the B-qubit in the receiver impersonation.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATE(B)} \tag{333}$$

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{ATE(B)} \tag{334}$$

Alice's operations during QDC on states (333) and (334) changes the system to one of the following states (335) – (338) resulting in table G.2 (p. G5).

$$H_A \text{ on } (333): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{ATE(B)} \tag{335}$$

$$H_A \text{ on } (334): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |001\rangle + |101\rangle + |010\rangle - |110\rangle - |011\rangle + |111\rangle)_{ATE(B)} \tag{336}$$

$$H_A\sigma_{zA} \text{ on } (333): \quad \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{ATE(B)} \tag{337}$$

$$H_A\sigma_{zA} \text{ on } (334): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle - |001\rangle - |101\rangle + |010\rangle - |110\rangle + |011\rangle - |111\rangle)_{ATE(B)} \tag{338}$$

Alice's operation	Transformation of GHZ states
H_A	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$
	$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} - \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} +$ $\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$
H_AX_A	$\frac{1}{2}(\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)})$
	$\frac{1}{2\sqrt{2}}(-\|\Phi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|+\rangle_{E(B)} + \|\Phi^-\rangle_{AT}\|-\rangle_{E(B)} +$ $\|\Psi^+\rangle_{AT}\|+\rangle_{E(B)} + \|\Psi^+\rangle_{AT}\|-\rangle_{E(B)} + \|\Psi^-\rangle_{AT}\|+\rangle_{E(B)} - \|\Psi^-\rangle_{AT}\|-\rangle_{E(B)})$

Table G.2: Results of QDC (2nd Impersonation Attack)

The overall detection probability remains $\frac{1}{4}$ for every second check qubit. Since Eve receives all entire results by both of Alice's operations, she cannot deduce a correct outcome.

$$\rho_D = \frac{1}{4} * (0 + \frac{1}{2} + 0 + \frac{1}{2}) = \frac{1}{4} \tag{339}$$

$$\rho_S = 0 \tag{340}$$

G.5 Advanced Impersonation Attacks

During authentication a detection probability of $\frac{1}{4}$ in the first and second attack, and a detection probability of $\frac{3}{8}$ in the third attack are maintained (see D.5, p. D16).

Impersonation of Sender and Authority

After Bob's decoding of the unencoded particles the state of the system changes as follows.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{E(A)E(T)B} \tag{341}$$

$$\frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{E(A)E(T)B} \tag{342}$$

In QDC the system changes to one of the following states (343) – (346) (see also tab. G.2, p. G5 with adapted subscripts).

$$H_{E(A)}\ on\ (341): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{343}$$

$$H_{E(A)}\ on\ (342): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |001\rangle + |101\rangle + |010\rangle - |110\rangle - |011\rangle + |111\rangle)_{E(A)E(T)B} \tag{344}$$

$$H_{E(A)}X_{E(A)}\ on\ (341): \quad \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{E(A)E(T)B} \tag{345}$$

$$H_{E(A)}X_{E(A)}\ on\ (342): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle - |001\rangle - |101\rangle + |010\rangle - |110\rangle + |011\rangle - |111\rangle)_{E(A)E(T)B} \tag{346}$$

The detection and success probabilities remain $\frac{1}{4}$ and 0, respectively.

Impersonation of Receiver and Authority

After Alice's decoding of the unencoded particles the state of the system changes as follows.

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{347}$$

$$\frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{348}$$

In QDC the system changes to one of the following states (349) – (352) (see also tab. G.1, p. G4 with adapted subscripts).

$$H_A\ on\ (347): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)E(B)} \tag{349}$$

$$H_A\ on\ (348): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)E(B)} \tag{350}$$

$$H_A\sigma_{zA}\ on\ (347): \quad \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{AE(T)E(B)} \tag{351}$$

$$H_A\sigma_{zA}\ on\ (348): \quad \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{AE(T)E(B)} \tag{352}$$

The probabilities are maintained, i.e.

$$\rho_D = \frac{1}{4} * (0 + 1 + 0 + 1) = \frac{1}{2} \tag{353}$$

$$\rho_S = \frac{1}{4} * \left(4 * \frac{1}{4}\right) = \frac{1}{4}\ . \tag{354}$$

Impersonation of the Authority

After Alice's and Bob's decoding the system changes to one of the following states (355) – (358).

$$I_A I_B \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \right)$$
$$= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{355}$$
$$I_A H_B \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \right)$$
$$= \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{356}$$
$$H_A I_B \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \right)$$
$$= \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{357}$$
$$H_A H_B \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \right)$$
$$= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{358}$$

The restoring problems lead to the transformations shown in eqs. (359) – (366) and table G.3 (p. G8).

$$H_A \text{ on } (355): \quad \frac{1}{2}(|000\rangle + |100\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{359}$$
$$H_A \text{ on } (356): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle)_{AE(T)B} \tag{360}$$
$$H_A \text{ on } (357): \quad \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{AE(T)B} \tag{361}$$
$$H_A \text{ on } (358): \quad \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)_{AE(T)B} \tag{362}$$
$$H_A\sigma_{zA} \text{ on } (355): \quad \frac{1}{2}(|000\rangle + |100\rangle - |011\rangle + |111\rangle)_{AE(T)B} \tag{363}$$
$$H_A\sigma_{zA} \text{ on } (356): \quad \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle - |001\rangle - |101\rangle + |010\rangle - |110\rangle + |011\rangle - |111\rangle)_{AE(T)B} \tag{364}$$
$$H_A\sigma_{zA} \text{ on } (357): \quad \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{AE(T)B} \tag{365}$$
$$H_A\sigma_{zA} \text{ on } (358): \quad \frac{1}{2}(|000\rangle - |001\rangle + |110\rangle + |111\rangle)_{AE(T)B} \tag{366}$$

The overall detection probability ρ_D remains $\frac{1}{2}$ with

$$\rho_D \;=\; \frac{1}{8} * \left(2*0 + 2*1 + 4*\frac{1}{2} \right) = \frac{1}{2}\ . \tag{367}$$

Alice's operation	Transformation of GHZ states
H_A	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|+\rangle_B - \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
	$\frac{1}{2\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B - \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B +$ $\|\Psi^+\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|-\rangle_B - \|\Psi^-\rangle_{AE(T)}\|+\rangle_B + \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$
	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B - \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$
H_AX_A	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B + \|\Psi^+\rangle_{AE(T)}\|-\rangle_B - \|\Psi^-\rangle_{AE(T)}\|+\rangle_B)$
	$\frac{1}{2\sqrt{2}}(-\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^+\rangle_{AE(T)}\|-\rangle_B + \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B +$ $\|\Psi^+\rangle_{AE(T)}\|+\rangle_B + \|\Psi^+\rangle_{AE(T)}\|-\rangle_B + \|\Psi^-\rangle_{AE(T)}\|+\rangle_B - \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
	$\frac{1}{\sqrt{2}}(\|\Psi^+\rangle_{AE(T)}\|+\rangle_B - \|\Psi^-\rangle_{AE(T)}\|-\rangle_B)$
	$\frac{1}{2}(\|\Phi^+\rangle_{AE(T)}\|+\rangle_B + \|\Phi^+\rangle_{AE(T)}\|-\rangle_B - \|\Phi^-\rangle_{AE(T)}\|+\rangle_B + \|\Phi^-\rangle_{AE(T)}\|-\rangle_B)$

Table G.3: Results of QDC (3rd Advanced Impersonation Attack)

Eve cannot derive any message bit ($\rho_S = 0$). An additional operation on the A-qubit does not change that.

Appendix H

Security Results: Protocol 3

All derivations refer to the security analysis of protocol 3 (s. 6.3, pp. 60).

H.1 Eavesdropping of Trent (s. 6.3.1, p. 60)

Before the entanglement swapping the entire system can be in one of the following states (368) or (369) depending on Alice initial states $|\Phi^+\rangle_{T_AA}$ or $|\Psi^+\rangle_{T_AA}$, respectively. Due to the entanglement between Trent's T_B-particle and Bob's B-qubit the T_B-qubit is in the same state as the B-particle.

$$\frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{T_AAT_BB} \tag{368}$$

$$\frac{1}{2}(|0100\rangle + |0111\rangle + |1000\rangle + |1011\rangle)_{T_AAT_BB} \tag{369}$$

According to the z basis measurement result of the T_A- and T_B-qubit, Trent announces his faked Bell state (see terms (370) – (373)).

$$|0\rangle_{T_A}|0\rangle_{T_B} \rightarrow |\Phi^{\pm}\rangle_{T_AT_B} \tag{370}$$

$$|0\rangle_{T_A}|1\rangle_{T_B} \rightarrow |\Psi^{\pm}\rangle_{T_AT_B} \tag{371}$$

$$|1\rangle_{T_A}|0\rangle_{T_B} \rightarrow |\Psi^{\pm}\rangle_{T_AT_B} \tag{372}$$

$$|1\rangle_{T_A}|1\rangle_{T_B} \rightarrow |\Phi^{\pm}\rangle_{T_AT_B} \tag{373}$$

Each combination T_AT_B occurs with the probability of $\frac{1}{4}$, which can be derived from eqs. (368) and (369). Hence, the occurrence probability for the entire result (e.g. $|0\rangle_{T_A}|0\rangle_{T_B}$ and $|0\rangle_A|0\rangle_B$) in case of a faked Bell state equals the expected probability, in which each result consists of a Bell state and the users' measurements, e.g. $|\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B$ (cf. C.3.1).

$$\rho_O(faked) = \left(\frac{1}{2}\right)^2 = \frac{1}{4} \tag{374}$$

$$\rho_O(expected) = \left(\frac{1}{2\sqrt{2}}\right)^2 * 2 = \frac{1}{4} \tag{375}$$

H.2 Eavesdropping on Authentication (s. 6.3.2, p. 61)

Impersonation Attack

Assuming that Eve leaves the particles unencoded, the system changes to one of the states (376) or (377) after Alice's decoding operations on the A-qubit.

$$I_A I_{E(T)} \left(|\Phi^+\rangle_{T_A A}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{E(T)A} \tag{376}$$

$$H_A I_{E(T)} \left(|\Phi^+\rangle_{T_A A}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{E(T)A} \tag{377}$$

There's no detection probability in eq. (376), but a detection probability of $\frac{1}{2}$ in eq. (377). Hence, the overall detection totals $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{378}$$

Eve can only deduce Alice's operation for different measurement results. Thus, the success probability ρ_S equals the detection probability.

Intercept-resend Attack

Trent transforms the system according to the identification information value.

$$I_T \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \tag{379}$$

$$H_T \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \tag{380}$$

When resending a particle to the user prepared according to Eve's measurement result, the detection probability totals $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{381}$$

Translucent Attack on Alice's qubits

With unitary transformation (A) the system changes to states $|\xi_{A0}\rangle$ or $|\xi_{A1}\rangle$ depending on the user's authentication key value $id_{iU} = 0$ or $id_{iU} = 1$, respectively. Accordingly, the unitary operation (B) transforms the system to states $|\xi_{B0}\rangle$ or $|\xi_{B1}\rangle$. The first operation is performed by Trent on the user's qubit (subscripted with T), the second transforms the user's and Eve's particle (E), and the last one is made by the user (U).

$$\begin{aligned} |\xi_{A0}\rangle &= I_U U_E I_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\ &= \frac{1}{\sqrt{2}} \left(\alpha|00\rangle_{T_U U}|e_{00}\rangle_E + \beta|01\rangle_{T_U U}|e_{01}\rangle_E + \alpha'|11\rangle_{T_U U}|e_{11}\rangle_E + \beta'|10\rangle_{T_U U}|e_{10}\rangle_E\right) \end{aligned} \tag{382}$$

$$
\begin{aligned}
|\xi_{A1}\rangle &= H_U U_E H_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\
&= H_U U_E \left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\
&= H_U \Big(\frac{1}{2}(\alpha|00\rangle|e_{00}\rangle_E + \beta|01\rangle|e_{01}\rangle_E + \alpha'|01\rangle|e_{11}\rangle_E + \beta'|00\rangle|e_{10}\rangle_E + \\
&\qquad \alpha|10\rangle|e_{00}\rangle_E + \beta|11\rangle|e_{01}\rangle_E - \alpha'|11\rangle|e_{11}\rangle_E - \beta'|10\rangle|e_{10}\rangle_E\Big) \\
&= \frac{1}{2\sqrt{2}}\Big(|00\rangle_{T_U U}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |01\rangle_{T_U U}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |10\rangle_{T_U U}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\qquad |11\rangle_{T_U U}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E\Big) \qquad (383)
\end{aligned}
$$

The detection probabilities are calculated as follows.

$$
\rho_D(|\xi_{A0}\rangle = \left(\frac{\beta}{\sqrt{2}}\right)^2 + \left(\frac{\beta'}{\sqrt{2}}\right)^2 = \frac{\beta^2 + \beta'^2}{2} \qquad (384)
$$

$$
\begin{aligned}
\rho_D(|\xi_{A1}\rangle) &= \left(\frac{1}{2\sqrt{2}}\right)^2 * 2(\alpha^2 + \beta^2 + \alpha'^2 + \beta'^2) \\
&= \frac{1}{4}(1 - \beta^2 + \beta^2 + 1 - \beta'^2 + \beta'^2) \\
&= \frac{1}{2} \qquad (385)
\end{aligned}
$$

The overall detection probability totals $\frac{1}{4} + \frac{\beta^2+\beta'^2}{4}$.

$$
\rho_D = \frac{1}{2} * \left(\frac{\beta^2 + \beta'^2}{2} + \frac{1}{2}\right) = \frac{\beta^2 + \beta'^2 + 1}{4} \qquad (386)
$$

With unitary transformation (B) the total system changes to states $|\xi_{B0}\rangle$ or $|\xi_{B1}\rangle$ after all operations of Trent, Eve, and the user.

$$
\begin{aligned}
|\xi_{B0}\rangle &= I_U U_E I_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))_{T_U U} \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{T_U UE} \qquad (387)
\end{aligned}
$$

$$
\begin{aligned}
|\xi_{B1}\rangle &= H_U U_E H_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))_{T_U U} \otimes |0\rangle_E\right) \\
&= H_U U_{UE} \left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \otimes |0\rangle_E\right) \\
&= H_U \left(\frac{1}{2}(|000\rangle + |011\rangle + |100\rangle - |111\rangle)_{T_U UE}\right) \\
&= \frac{1}{2\sqrt{2}} (|000\rangle + |010\rangle + |001\rangle - |011\rangle + |100\rangle + |110\rangle - |101\rangle + |111\rangle)_{T_U UE} \\
&= \frac{1}{2}(|00\rangle_{T_U U}|+\rangle_E + |01\rangle_{T_U U}|-\rangle_E + |10\rangle_{T_U U}|-\rangle_E + |11\rangle_{T_U U}|+\rangle_E) \qquad (388)
\end{aligned}
$$

The detection probability totals $\frac{1}{4}$.

$$
\rho_D = \frac{1}{2} * (\rho_D(|\xi_{B0}\rangle) + \rho_D(|\xi_{B1}\rangle)) = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \qquad (389)
$$

H.3 Eavesdropping on QDC (s. 6.3.3, p. 62)

Translucent Attack (A)

$|\xi_{A\Phi}\rangle_B$ denotes the system after using unitary operation (A) to entangle the ancilla with the T_B-particle of Bob's initial state $|\Phi^+\rangle_{T_B B}$.

$$
\begin{aligned}
|\xi_{A\Phi}\rangle_B &= U_{T_B E} \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B} \otimes |E\rangle_E\right) \\
&= \frac{1}{\sqrt{2}} (\alpha|00\rangle_{T_B B}|e_{00}\rangle_E + \beta|10\rangle_{T_B B}|e_{01}\rangle_E + \alpha'|11\rangle_{T_B B}|e_{11}\rangle_E + \beta'|01\rangle_{T_B B}|e_{10}\rangle_E)
\end{aligned} \qquad (390)
$$

In the eavesdropping test between Bob and Trent on the c_{TRANS} check qubits the detection probability totals $\rho_D(|\xi_{A\Phi}\rangle_B) = \frac{\beta^2+\beta'^2}{2}$ per check qubit.

After entanglement swapping is applied, the system changes to one of the following states $|\xi_{ES}\rangle_1$ or $|\xi_{ES}\rangle_2$. The upper and lower sign lines correspond to the upper and lower signs of the exponent of the Bell states.

$$
\begin{aligned}
|\xi_{ES}\rangle_1 &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{A\Phi}\rangle_B \\
&= \frac{1}{2}(\alpha|0000\rangle|e_{00}\rangle + \alpha|1010\rangle|e_{00}\rangle + \beta|0100\rangle|e_{01}\rangle + \beta|1110\rangle|e_{01}\rangle + \\
&\quad \alpha'|0101\rangle|e_{11}\rangle + \alpha'|1111\rangle|e_{11}\rangle + \beta'|0001\rangle|e_{10}\rangle + \beta'|1011\rangle|e_{10}\rangle)_{T_A T_B ABE} \\
&= \frac{1}{2\sqrt{2}}\Big(\alpha|\Phi^\pm\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|e_{00}\rangle_E \pm \alpha'|\Phi^\pm\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|e_{11}\rangle_E \pm \\
&\qquad \beta|\Phi^\pm\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|e_{01}\rangle_E + \beta'|\Phi^\pm\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|e_{10}\rangle_E \pm \\
&\qquad \alpha|\Psi^\pm\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|e_{00}\rangle_E + \alpha'|\Psi^\pm\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|e_{11}\rangle_E + \\
&\qquad \beta|\Psi^\pm\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|e_{01}\rangle_E \pm \beta'|\Psi^\pm\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|e_{10}\rangle_E\Big)
\end{aligned} \qquad (391)
$$

$$
\begin{aligned}
|\xi_{ES}\rangle_2 &= |\Psi^+\rangle_{T_AA} \otimes |\xi_{A\Phi}\rangle_B \\
&= \frac{1}{2}(\alpha|0010\rangle|e_{00}\rangle + \alpha|1000\rangle|e_{00}\rangle + \beta|0110\rangle|e_{01}\rangle + \beta|1100\rangle|e_{01}\rangle + \\
&\quad \alpha'|01111\rangle|e_{11}\rangle + \alpha'|1101\rangle|e_{11}\rangle + \beta'|0011\rangle|e_{10}\rangle + \beta'|1001\rangle|e_{10}\rangle)_{T_AT_BABE} \\
&= \frac{1}{2\sqrt{2}}\Big(\alpha|\Phi^\pm\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|e_{00}\rangle_E \pm \alpha'|\Phi^\pm\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|e_{11}\rangle_E + \\
&\qquad \beta|\Phi^\pm\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|e_{01}\rangle_E \pm \beta'|\Phi^\pm\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|e_{10}\rangle_E + \\
&\qquad \alpha|\Psi^\pm\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|e_{00}\rangle_E + \alpha'|\Psi^\pm\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|e_{11}\rangle_E \pm \\
&\qquad \beta|\Psi^\pm\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|e_{01}\rangle_E \pm \beta'|\Psi^\pm\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|e_{10}\rangle_E\Big)
\end{aligned} \tag{392}
$$

The detection probability amounts to $\frac{\beta^2+\beta'^2}{2}$ in the second eavesdropping test.

$$
\rho_D(|\xi_{ES}\rangle_{1/2}) = \left(\frac{1}{2\sqrt{2}}\right)^2 \left(4 * \beta^2 + 4 * \beta'^2\right) = \frac{\beta^2+\beta'^2}{2} \tag{393}
$$

When entangling the ancillas with the A-sequence, the detection probability also amounts to $\frac{\beta^2+\beta'^2}{2}$ preconditioned that Alice chooses $|\Phi^+\rangle_{T_AA}$ (eq. (394)) and $|\Psi^+\rangle_{T_AA}$ (eq. (394)) with probability ρ_Φ and ρ_Ψ (with $\rho_\Phi + \rho_\Psi = 1$), respectively.

$$
|\xi_{A\Phi}\rangle_A = \frac{1}{\sqrt{2}}\left(\alpha|00\rangle_{T_AA}|e_{00}\rangle_E + \beta|10\rangle_{T_AA}|e_{01}\rangle_E + \alpha'|11\rangle_{T_AA}|e_{11}\rangle_E + \beta'|01\rangle_{T_AA}|e_{10}\rangle_E\right) \tag{394}
$$

$$
|\xi_{A\Psi}\rangle_A = \frac{1}{\sqrt{2}}\left(\alpha|01\rangle_{T_AA}|e_{00}\rangle_E + \beta|11\rangle_{T_AA}|e_{01}\rangle_E + \alpha'|10\rangle_{T_AA}|e_{11}\rangle_E + \beta'|00\rangle_{T_AA}|e_{10}\rangle_E\right) \tag{395}
$$

$$
\rho_D(|\xi_{A\Omega}\rangle_A) = \rho_\Phi * \frac{\beta^2+\beta'^2}{2} + \rho_\Psi * \frac{\beta^2+\beta'^2}{2} = \frac{\beta^2+\beta'^2}{2} \tag{396}
$$

When entangling the ancillas on both sequences, the detection probability in both first eavesdropping tests, each on c_{TRANS} check qubits, totals $\beta^2 + \beta'^2$ per check qubit.

$$
\rho_D(|\xi_{A\Omega}\rangle_{AB}) = 2 * \frac{\beta^2+\beta'^2}{2} = \beta^2 + \beta'^2 \tag{397}
$$

After the entanglement swapping the system is transformed as follows.

$$
\begin{aligned}
|\xi_{ES}\rangle_3 &= |\xi_{A\Phi}\rangle_A \otimes |\xi_{A\Phi}\rangle_B \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\alpha|e_{00}\rangle_E \pm \beta|e_{01}\rangle_E\beta|e_{01}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B(\alpha|e_{00}\rangle_E\beta'|e_{10}\rangle_E \pm \beta|e_{01}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\beta'|e_{10}\rangle_E \pm \beta|e_{01}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B(\beta'|e_{10}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha'|e_{11}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\beta|e_{01}\rangle_E \pm \alpha|e_{00}\rangle_E\beta|e_{01}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B(\alpha|e_{00}\rangle_E\alpha'|e_{11}\rangle_E \pm \beta|e_{01}\rangle_E\beta'|e_{10}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B(\beta|e_{01}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha|e_{00}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B(\alpha'|e_{11}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha'|e_{11}\rangle_E\beta'|e_{10}\rangle_E)\Big)
\end{aligned} \tag{398}
$$

$$
\begin{aligned}
|\xi_{ES}\rangle_4 &= |\xi_{A\Psi}\rangle_A \otimes |\xi_{A\Phi}\rangle_B \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\beta'|e_{10}\rangle_E \pm \beta|e_{01}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B(\beta'|e_{10}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha'|e_{11}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\alpha|e_{00}\rangle_E \pm \beta|e_{01}\rangle_E\beta|e_{01}\rangle_E) + \\
&\quad |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B(\alpha|e_{00}\rangle_E\beta'|e_{10}\rangle_E \pm \beta|e_{01}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B(\beta|e_{01}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha|e_{00}\rangle_E\alpha'|e_{11}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B(\alpha'|e_{11}\rangle_E\beta'|e_{10}\rangle_E \pm \alpha'|e_{11}\rangle_E\beta'|e_{10}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B(\alpha|e_{00}\rangle_E\beta|e_{01}\rangle_E \pm \alpha|e_{00}\rangle_E\beta|e_{01}\rangle_E) + \\
&\quad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B(\alpha|e_{00}\rangle_E\alpha'|e_{11}\rangle_E \pm \beta|e_{01}\rangle_E\beta'|e_{10}\rangle_E)\Big)
\end{aligned} \tag{399}
$$

$$
\rho_D(|\xi_{ES}\rangle_3) = \frac{(\beta^2+\beta'^2)^2}{4} + \frac{1-2\beta^2-2\beta'^2}{2} \tag{400}
$$

$$
\rho_D(|\xi_{ES}\rangle_4) = \frac{-(\beta^2+\beta'^2)^2}{4} + \frac{\beta^2+\beta'^2}{2} \tag{401}
$$

$$
\rho_D(|\xi_{ES}\rangle_{3/4}) = \frac{1-\beta^2-\beta'^2}{4} \tag{402}
$$

Translucent Attack (B)

$|\xi_{B\Phi}\rangle_B$ denotes the system after entangling ancilla (B) with the B-sequence (i.e. the T_B-particles) of Bob's initial states $|\Phi^+\rangle_{T_BB}$.

$$
\begin{aligned}
|\xi_{B\Phi}\rangle_B &= U_{T_BE}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{T_BBE}
\end{aligned} \tag{403}
$$

No errors are introduced. Hence, the attack cannot be detected in the first eavesdropping test on the c_{TRANS} check qubits nor in the second eavesdropping test on the c_{ES} check qubits after the entanglement swapping (eqs. (404) and (405)). When measuring her entangled particle, Eve obtains the same result as Bob.

$$\begin{aligned}
|\xi_{ES}\rangle_1 &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \otimes |\xi_{B\Phi}\rangle_B \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_AA} \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{T_BBE} \\
&= \frac{1}{2}(|00000\rangle + |00111\rangle + |11000\rangle + |11111\rangle)_{T_AAET_BB} \\
&= \frac{1}{2}(|00000\rangle + |01011\rangle + |10100\rangle + |11111\rangle)_{T_AT_BABE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|0\rangle_E \pm |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|1\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|1\rangle_E \pm |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|0\rangle_E\Big) \qquad (404)
\end{aligned}$$

$$\begin{aligned}
|\xi_{ES}\rangle_2 &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_AA} \otimes |\xi_{B\Phi}\rangle_B \\
&= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_AA} \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{T_BBE} \\
&= \frac{1}{2}(|01000\rangle + |01111\rangle + |10000\rangle + |10111\rangle)_{T_AAET_BB} \\
&= \frac{1}{2}(|00100\rangle + |01111\rangle + |10000\rangle + |11011\rangle)_{T_AT_BABE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|0\rangle_E \pm |\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|1\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|1\rangle_E \pm |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|0\rangle_E\Big) \qquad (405)
\end{aligned}$$

The following eqs. (406) – (409) show the transformed system when attacking the A-sequence, although Eve can succeed in sufficient degree when only attacking the B-sequence.

$$|\xi_{B\Phi}\rangle_A = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{T_AAE} \qquad (406)$$

$$|\xi_{B\Psi}\rangle_A = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{T_AAE} \qquad (407)$$

$$\begin{aligned}
|\xi_{ES}\rangle_3 &= |\xi_{B\Phi}\rangle_A \otimes |\xi_{B\Phi}\rangle_B \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|00\rangle_E \pm |\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|11\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|01\rangle_E \pm |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|10\rangle_E\Big) \qquad (408)
\end{aligned}$$

$$
\begin{aligned}
|\xi_{ES}\rangle_4 &= |\xi_{B\Psi}\rangle_A \otimes |\xi_{B\Phi}\rangle_B \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|00\rangle_E \pm |\Phi^{\pm}\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|11\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|01\rangle_E \pm |\Psi^{\pm}\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|10\rangle_E \Big) \qquad (409)
\end{aligned}
$$

Appendix I

Security Results: Improved Proposal 3

All derivations refer to the security analysis of the improved proposal 3 (s. 6.5.1.2, pp. 72).

I.1 Eavesdropping of Trent

As the modifications in the improved proposal have no impact on the process of Trent's eavesdropping attack, see H.1 (p. H1) for details.

I.2 Eavesdropping on Authentication

Only the tasks are switched in the authentication process, not the core of authentication. Hence, the results of the original protocol 3 remain still valid here (see H.2, p. H2 for more details).

I.3 Eavesdropping on QDC

Translucent Attack (A) on the B-sequence

Eve attacks the T_B-qubits of the B-sequence during its transmission to Trent, that is in between Bob's encoding and Trent's decoding operations. Additionally, there're are unencoded particles, transmitted on positions, which Eve does not know yet. After entangling her ancilla the total B-system of the decoding sequence and the B-sequence is transformed to states $|\xi_{A0}\rangle_B$ or $|\xi_{A1}\rangle_B$ depending on Bob's authentication key value $id_{iB} = 0$ or $id_{iB} = 1$, respectively, or to state $|\xi_{AX}\rangle_B$ with X denoting the unencoded particles without any authentication key value.

$$\begin{aligned} |\xi_{A0}\rangle_B &= I_B U_{T_B E} I_B \left(\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{T_B B} \otimes |E\rangle_E \right) \\ &= \frac{1}{\sqrt{2}} \left(\alpha |00\rangle_{T_B B} |e_{00}\rangle_E + \beta |10\rangle_{T_B B} |e_{01}\rangle_E + \alpha' |11\rangle_{T_B B} |e_{11}\rangle_E + \beta' |01\rangle_{T_B B} |e_{10}\rangle_E \right) \end{aligned} \tag{410}$$

$$
\begin{aligned}
|\xi_{A1}\rangle_B &= H_B U_{T_B E} H_B \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B} \otimes |E\rangle_E \right) \\
&= H_B U_{T_B E} \left(\frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{T_B B} \otimes |E\rangle_E \right) \\
&= H_B \Big(\frac{1}{2}(\alpha|00\rangle|e_{00}\rangle_E + \beta|10\rangle|e_{01}\rangle_E + \alpha'|10\rangle|e_{11}\rangle_E + \beta'|00\rangle|e_{10}\rangle_E + \\
&\qquad \alpha|01\rangle|e_{00}\rangle_E + \beta|11\rangle|e_{01}\rangle_E - \alpha'|11\rangle|e_{11}\rangle_E - \beta'|01\rangle|e_{10}\rangle_E \Big) \\
&= \frac{1}{2\sqrt{2}} \Big(|00\rangle_{T_B B}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |01\rangle_{T_B B}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\qquad |10\rangle_{T_B B}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |11\rangle_{T_B B}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E \Big) \qquad (411)
\end{aligned}
$$

$$
\begin{aligned}
|\xi_{AX}\rangle_B &= U_{T_B E} \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_B B} \otimes |E\rangle_E \right) \\
&= \frac{1}{\sqrt{2}} \left(\alpha|00\rangle_{T_B B}|e_{00}\rangle_E + \beta|10\rangle_{T_B B}|e_{01}\rangle_E + \alpha'|11\rangle_{T_B B}|e_{11}\rangle_E + \beta'|01\rangle_{T_B B}|e_{10}\rangle_E \right)
\end{aligned} \qquad (412)
$$

During the authentication only states $|\xi_{A0}\rangle_B$ and $|\xi_{A1}\rangle_B$ are checked. The detection probability in the eavesdropping test totals $\frac{1}{4} + \frac{\beta^2+\beta'^2}{2}$.

$$
\rho_D(|\xi_{A0/1}\rangle_B) = \frac{1}{2} * \left(\frac{\beta^2 + \beta'^2}{2} + \frac{1}{2} \right) = \frac{1}{4} + \frac{\beta^2 + \beta'^2}{4} \qquad (413)
$$

After entanglement swapping is applied, the entire system changes to one of the following states $|\xi_{ES}\rangle_1$ or $|\xi_{ES}\rangle_2$. The upper and lower sign lines correspond to the upper and lower signs in the exponent of the Bell states.

$$
\begin{aligned}
|\xi_{ES}\rangle_1 &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{AX}\rangle_B \\
&= \frac{1}{2}(\alpha|0000\rangle|e_{00}\rangle + \alpha|1010\rangle|e_{00}\rangle + \beta|0100\rangle|e_{01}\rangle + \beta|1110\rangle|e_{01}\rangle + \\
&\quad \alpha'|0101\rangle|e_{11}\rangle + \alpha'|1111\rangle|e_{11}\rangle + \beta'|0001\rangle|e_{10}\rangle + \beta'|1011\rangle|e_{10}\rangle)_{T_A T_B ABE} \\
&= \frac{1}{2\sqrt{2}} \Big(\alpha|\Phi^\pm\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|e_{00}\rangle_E \pm \alpha'|\Phi^\pm\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|e_{11}\rangle_E \pm \\
&\qquad \beta|\Phi^\pm\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|e_{01}\rangle_E + \beta'|\Phi^\pm\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|e_{10}\rangle_E \pm \\
&\qquad \alpha|\Psi^\pm\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|e_{00}\rangle_E + \alpha'|\Psi^\pm\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|e_{11}\rangle_E + \\
&\qquad \beta|\Psi^\pm\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|e_{01}\rangle_E \pm \beta'|\Psi^\pm\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|e_{10}\rangle_E + \Big)
\end{aligned} \qquad (414)
$$

$$
\begin{aligned}
|\xi_{ES}\rangle_2 &= |\Psi^+\rangle_{T_AA} \otimes |\xi_{AX}\rangle_B \\
&= \frac{1}{2}(\alpha|0010\rangle|e_{00}\rangle + \alpha|1000\rangle|e_{00}\rangle + \beta|0110\rangle|e_{01}\rangle + \beta|1100\rangle|e_{01}\rangle + \\
&\quad \alpha'|01111\rangle|e_{11}\rangle + \alpha'|1101\rangle|e_{11}\rangle + \beta'|0011\rangle|e_{10}\rangle + \beta'|1001\rangle|e_{10}\rangle)_{T_AT_BABE} \\
&= \frac{1}{2\sqrt{2}}\Big(\alpha|\Phi^\pm\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|e_{00}\rangle_E \pm \alpha'|\Phi^\pm\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|e_{11}\rangle_E + \\
&\qquad \beta|\Phi^\pm\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|e_{01}\rangle_E \pm \beta'|\Phi^\pm\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|e_{10}\rangle_E + \\
&\qquad \alpha|\Psi^\pm\rangle_{T_AT_B}|0\rangle_A|0\rangle_B|e_{00}\rangle_E + \alpha'|\Psi^\pm\rangle_{T_AT_B}|1\rangle_A|1\rangle_B|e_{11}\rangle_E \pm \\
&\qquad \beta|\Psi^\pm\rangle_{T_AT_B}|1\rangle_A|0\rangle_B|e_{01}\rangle_E \pm \beta'|\Psi^\pm\rangle_{T_AT_B}|0\rangle_A|1\rangle_B|e_{10}\rangle_E + \Big)
\end{aligned} \tag{415}
$$

The detection probability amounts to $\beta^2 + \beta'^2$ in the second eavesdropping test.

$$
\rho_D(|\xi_{ES}\rangle_{1/2}) = \frac{1}{2} * 2 * \left(\frac{1}{2\sqrt{2}}\right)^2 \left(8 * \beta^2 + 8 * \beta'^2\right) = \beta^2 + \beta'^2 \tag{416}
$$

Translucent Attack (B) on the B-sequence

The attack is launched during the transmission of the T_B-qubits, that is in between Bob's encoding and Trent's decoding operations. Again, there're are unencoded particles transmitted at the same time. After the entanglement the total B-system of the decoding sequence and the B-sequence is transformed to states $|\xi_{B0}\rangle_B$, $|\xi_{B0}\rangle_B$, or $|\xi_{BX}\rangle_B$ depending on Bob's authentication key value 0, 1, or X (non), respectively.

$$
\begin{aligned}
|\xi_{B0}\rangle_B &= I_B U_{T_BE} I_B \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))_{T_BB} \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{T_BBE}
\end{aligned} \tag{417}
$$

$$
\begin{aligned}
|\xi_{B1}\rangle_B &= H_B U_{T_BE} H_B \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \otimes |0\rangle_E\right) \\
&= H_B U_{UT_BE} \left(\frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{T_BB} \otimes |0\rangle_E\right) \\
&= H_B \left(\frac{1}{2}(|000\rangle + |101\rangle + |010\rangle - |111\rangle)_{T_BBE}\right) \\
&= \frac{1}{2\sqrt{2}}\left(|000\rangle + |100\rangle + |001\rangle - |101\rangle + |010\rangle + |110\rangle - |011\rangle + |111\rangle\right)_{T_BBE} \\
&= \frac{1}{2}(|00\rangle_{T_BB}|+\rangle_E + |01\rangle_{T_BB}|-\rangle_E + |10\rangle_{T_BB}|-\rangle_E + |11\rangle_{T_BB}|+\rangle_E)
\end{aligned} \tag{418}
$$

$$
\begin{aligned}
|\xi_{BX}\rangle_B &= U_{T_BE} \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_BB} \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{T_BBE}
\end{aligned} \tag{419}
$$

During the authentication only $|\xi_{B0}\rangle_B$ and $|\xi_{B1}\rangle_B$ are checked. The detection probability totals $\frac{1}{4}$.

$$\rho_D(|\xi_{B0/1}\rangle_B) = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{420}$$

After Trent swapped the entanglement the total system is in one of the following states $|\xi_{ES}\rangle_1$ or $|\xi_{ES}\rangle_2$. The upper and lower sign lines correspond to the upper and lower signs in the exponent of the Bell states, respectively.

$$\begin{aligned}
|\xi_{ES}\rangle_1 &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_A A} \otimes |\xi_{BX}\rangle_B \\
&= \frac{1}{2}(|00000\rangle + |01011\rangle + |10100\rangle + |11111\rangle)_{T_A T_B ABE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|0\rangle_E \pm |\Phi^{\pm}\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|1\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|1\rangle_E \pm |\Psi^{\pm}\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|0\rangle_E\Big)
\end{aligned} \tag{421}$$

$$\begin{aligned}
|\xi_{ES}\rangle_2 &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{T_A A} \otimes |\xi_{BX}\rangle_B \\
&= \frac{1}{2}(|00100\rangle + |01111\rangle + |10000\rangle + |11011\rangle)_{T_A T_B ABE} \\
&= \frac{1}{2\sqrt{2}}\Big(|\Phi^{\pm}\rangle_{T_A T_B}|1\rangle_A|0\rangle_B|0\rangle_E \pm |\Phi^{\pm}\rangle_{T_A T_B}|0\rangle_A|1\rangle_B|1\rangle_E + \\
&\qquad |\Psi^{\pm}\rangle_{T_A T_B}|1\rangle_A|1\rangle_B|1\rangle_E \pm |\Psi^{\pm}\rangle_{T_A T_B}|0\rangle_A|0\rangle_B|0\rangle_E\Big)
\end{aligned} \tag{422}$$

There is no detection probability in the second eavesdropping test ($\rho_D(|\xi_{ES}\rangle_{1/2}) = 0$).

I.4 Simple Impersonation Attacks

Sender or Receiver Impersonation in Authentication

The impersonation of Alice and Bob are equivalent during authentication, as both parties use states $|\Phi^+\rangle_{T_U U}$. It is assumed that Eve sends the particles unencoded to Trent. While Trent attempts to restore his T_U-qubits, the U-system changes to one of the following states (423) or (424).

In case of $id_{iU} = 0$:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \tag{423}$$

In case of $id_{iU} = 1$:

$$\frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)_{T_U U} \tag{424}$$

Eve can be detected with the probability of $\frac{1}{2}$ in eq. (424). Hence, the overall detection probability amounts to $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{425}$$

Sender or Receiver Impersonation in QDC

The direct communication process in an impersonation attack proceeds according to the specification of the improved proposal 3 (see 6.5.1), since Eve does not introduce any errors.

Appendix J

Security Results: Improved Proposal 4

All derivations refer to the security analysis of the improved proposal 4 (s. 6.5.2.2, pp. 77).

J.1 Eavesdropping of Trent

Before the entanglement swapping the entire system is in the state (426). Trent can only deduce Alice's and Bob's state of particles in the z basis, but he cannot derive their x basis measurement results after his entanglement swapping (eq. (427)).

$$\frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)_{T_A A T_B B} \tag{426}$$

$$= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{T_A T_B A B}$$

$$\begin{aligned} = \frac{1}{8}\Big(& (|00\rangle + |01\rangle + |10\rangle + |11\rangle)_{T_A T_B}(|0\rangle + |1\rangle)_A(|0\rangle + |1\rangle)_B + \\ & (|00\rangle + |01\rangle - |10\rangle - |11\rangle)_{T_A T_B}(|0\rangle - |1\rangle)_A(|0\rangle + |1\rangle)_B + \\ & (|00\rangle - |01\rangle + |10\rangle - |11\rangle)_{T_A T_B}(|0\rangle + |1\rangle)_A(|0\rangle - |1\rangle)_B + \\ & (|00\rangle - |01\rangle - |10\rangle + |11\rangle)_{T_A T_B}(|0\rangle - |1\rangle)_A(|0\rangle - |1\rangle)_B \Big) \end{aligned} \tag{427}$$

$$\begin{aligned} = \frac{1}{2\sqrt{2}}\Big(& \big(|\Phi^+\rangle_{T_A T_B} + |\Psi^+\rangle_{T_A T_B}\big)|+\rangle_A|+\rangle_B \; + \\ & \big(|\Phi^-\rangle_{T_A T_B} + |\Psi^-\rangle_{T_A T_B}\big)|-\rangle_A|+\rangle_B \; + \\ & \big(|\Phi^-\rangle_{T_A T_B} - |\Psi^-\rangle_{T_A T_B}\big)|+\rangle_A|-\rangle_B \; + \\ & \big(|\Phi^+\rangle_{T_A T_B} - |\Psi^+\rangle_{T_A T_B}\big)|-\rangle_A|-\rangle_B \Big) \end{aligned} \tag{428}$$

J.2 Eavesdropping on Authentication

Impersonation Attack

Assuming that Eve leaves the particles unencoded, the system changes to one of the states (429) or (430) after the user's decoding operations on her/his U-qubit.

$$I_U I_{E(T)} \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{E(T_U)U} \quad (429)$$

$$H_U I_{E(T)} \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{E(T_U)U} \quad (430)$$

The detection and success probabilities total $\frac{1}{4}$.

Intercept-resend Attack

The system was changed by Trent depending on the user's identification information value 0 (eq. (431)) or 1 (eq. (432)).

$$I_T \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \quad (431)$$

$$H_T \left(|\Phi^+\rangle_{T_U U}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \quad (432)$$

When resending a particle to the user, prepared according to Eve's measurement result, the detection probability totals $\frac{1}{4}$.

Translucent Attack on Alice's qubits

With the transformation (A) the total system changes to states $|\xi_{A0}\rangle$ or $|\xi_{A1}\rangle$, depending on the user's authentication key value $id_{iU} = 0$ or $id_{iU} = 1$, respectively. The first operation is performed by Trent on the user's qubit (T), the second transforms the user's and Eve's particle (E), and the last one is made by the user (U).

$$\begin{aligned} |\xi_{A0}\rangle &= I_U U_E I_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\ &= \frac{1}{\sqrt{2}} \left(\alpha|00\rangle_{T_U U}|e_{00}\rangle_E + \beta|01\rangle_{T_U U}|e_{01}\rangle_E + \alpha'|11\rangle_{T_U U}|e_{11}\rangle_E + \beta'|10\rangle_{T_U U}|e_{10}\rangle_E\right) \end{aligned} \quad (433)$$

$$
\begin{aligned}
|\xi_{A1}\rangle &= H_U U_E H_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\
&= H_U U_{UE} \left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \otimes |E\rangle_E\right) \\
&= H_U \Big(\frac{1}{2}(\alpha|00\rangle|e_{00}\rangle_E + \beta|01\rangle|e_{01}\rangle_E + \alpha'|01\rangle|e_{11}\rangle_E + \beta'|00\rangle|e_{10}\rangle_E + \\
&\qquad \alpha|10\rangle|e_{00}\rangle_E + \beta|11\rangle|e_{01}\rangle_E - \alpha'|11\rangle|e_{11}\rangle_E - \beta'|10\rangle|e_{10}\rangle_E\Big) \\
&= \frac{1}{2\sqrt{2}}\Big(|00\rangle_{T_U U}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |01\rangle_{T_U U}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \alpha'|e_{11}\rangle + \beta'|e_{10}\rangle)_E + \\
&\qquad |10\rangle_{T_U U}(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E + \\
&\qquad |11\rangle_{T_U U}(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \alpha'|e_{11}\rangle - \beta'|e_{10}\rangle)_E\Big)
\end{aligned} \tag{434}
$$

In $|\xi_{A0}\rangle$ or $|\xi_{A1}\rangle$ errors are introduced with the probability of $\frac{\beta^2+\beta'^2}{2}$ or $\frac{1}{2}$, respectively. Thus, the overall detection probability totals $\rho_D = \frac{1}{4} + \frac{\beta^2+\beta'^2}{4}$ (see H.2 for more detailed calculations). With the unitary transformation (B) the total system changes to states $|\xi_{B0}\rangle$ or $|\xi_{B1}\rangle$, depending on the user's authentication key value.

$$
\begin{aligned}
|\xi_{B0}\rangle &= I_U U_E I_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))_{T_U U} \otimes |0\rangle_E\right) \\
&= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{T_U UE}
\end{aligned} \tag{435}
$$

$$
\begin{aligned}
|\xi_{B1}\rangle &= H_U U_E H_T \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_U U} \otimes |0\rangle_E\right) \\
&= H_U U_{UE} \left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_U U} \otimes |0\rangle_E\right) \\
&= H_U \left(\frac{1}{2}(|000\rangle + |011\rangle + |100\rangle - |111\rangle)_{T_U UE}\right) \\
&= \frac{1}{2\sqrt{2}}\left(|000\rangle + |010\rangle + |001\rangle - |011\rangle + |100\rangle + |110\rangle - |101\rangle + |111\rangle\right)_{T_U UE} \\
&= \frac{1}{2}(|00\rangle_{T_U U}|+\rangle_E + |01\rangle_{T_U U}|-\rangle_E + |10\rangle_{T_U U}|-\rangle_E + |11\rangle_{T_U U}|+\rangle_E)
\end{aligned} \tag{436}
$$

The detection probability totals $\frac{1}{4}$ (see H.2 for more detailed calculations).

J.3 Eavesdropping on QDC

Eve can only attack the A- or B- particle during their transmission, that is between Trent's encoding and Alice's or Bob's decoding operations. If the attack is not recognised in the first mandatory eavesdropping test (see J.2), the system changes to one of the following states

$|\xi_{ES1}\rangle$ – $|\xi_{ES16}\rangle$ during Trent's entanglement swapping.

$$
\begin{aligned}
|\xi_{ES}\rangle_1 &= |\xi_{A0}\rangle_A \otimes |\Phi^+\rangle_{T_B B} && (437)\\
|\xi_{ES}\rangle_2 &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{A0}\rangle_B && (438)\\
|\xi_{ES}\rangle_3 &= |\xi_{A1}\rangle_A \otimes |\Phi^+\rangle_{T_B B} && (439)\\
|\xi_{ES}\rangle_4 &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{A1}\rangle_B && (440)\\
|\xi_{ES}\rangle_5 &= |\xi_{A0}\rangle_A \otimes |\xi_{A0}\rangle_B && (441)\\
|\xi_{ES}\rangle_6 &= |\xi_{A0}\rangle_A \otimes |\xi_{A1}\rangle_B && (442)\\
|\xi_{ES}\rangle_7 &= |\xi_{A1}\rangle_A \otimes |\xi_{A0}\rangle_B && (443)\\
|\xi_{ES}\rangle_8 &= |\xi_{A1}\rangle_A \otimes |\xi_{A1}\rangle_B && (444)\\
|\xi_{ES}\rangle_9 &= |\xi_{B0}\rangle_A \otimes |\Phi^+\rangle_{T_B B} && (445)\\
|\xi_{ES}\rangle_{10} &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{B0}\rangle_B && (446)\\
|\xi_{ES}\rangle_{11} &= |\xi_{B1}\rangle_A \otimes |\Phi^+\rangle_{T_B B} && (447)\\
|\xi_{ES}\rangle_{12} &= |\Phi^+\rangle_{T_A A} \otimes |\xi_{B1}\rangle_B && (448)\\
|\xi_{ES}\rangle_{13} &= |\xi_{B0}\rangle_A \otimes |\xi_{B0}\rangle_B && (449)\\
|\xi_{ES}\rangle_{14} &= |\xi_{B0}\rangle_A \otimes |\xi_{B1}\rangle_B && (450)\\
|\xi_{ES}\rangle_{15} &= |\xi_{B1}\rangle_A \otimes |\xi_{B0}\rangle_B && (451)\\
|\xi_{ES}\rangle_{16} &= |\xi_{B1}\rangle_A \otimes |\xi_{B1}\rangle_B && (452)
\end{aligned}
$$

J.4 Simple Impersonation Attacks

Sender or Receiver Impersonation in Authentication

The impersonation of Alice and Bob are equivalent during authentication, since Trent encodes the respective authentication key in states of the form $|\Phi^+\rangle_{T_U U}$. It is assumed that Eve leaves her U-particles undecoded. When encoding Trent changes the system to one of the following states (453) or (454).

$$
\begin{aligned}
|\xi_{AUTH0}\rangle &= I_T\left(|\Phi^+\rangle_{T_{E(U)}E(U)}\right)\\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{T_{E(U)}E(U)} && (453)\\
|\xi_{AUTH1}\rangle &= H_T\left(|\Phi^+\rangle_{T_{E(U)}E(U)}\right)\\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{T_{E(U)}E(U)} && (454)
\end{aligned}
$$

During the first eavesdropping test Eve can be detected with the probability of $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + \frac{1}{2}\right) = \frac{1}{4} \qquad (455)$$

Sender Impersonation in QDC

If the errors are not recognised in the first eavesdropping test, the system changes to one of the following states $|\xi_{ES}\rangle_1$ or $|\xi_{ES}\rangle_{16}$ after Trent's entanglement swapping and Eve's and Bob's x basis measurements.

$$
\begin{aligned}
|\xi_{ES}\rangle_1 &= |\xi_{AUTH0}\rangle \otimes |\Phi^+\rangle_{T_BB} \\
&= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{T_{E(A)}T_BE(A)B} \\
&= \frac{1}{2\sqrt{2}}\Big(\big(|\Phi^+\rangle + |\Psi^+\rangle\big)_{T_{E(A)}T_B}|+\rangle_{E(A)}|+\rangle_B \; + \\
&\qquad \big(|\Phi^-\rangle + |\Psi^-\rangle\big)_{T_{E(A)}T_B}|-\rangle_{E(A)}|+\rangle_B \; + \\
&\qquad \big(|\Phi^-\rangle - |\Psi^-\rangle\big)_{T_{E(A)}T_B}|+\rangle_{E(A)}|-\rangle_B \; + \\
&\qquad \big(|\Phi^+\rangle - |\Psi^+\rangle\big)_{T_{E(A)}T_B}|-\rangle_{E(A)}|-\rangle_B\Big) \qquad (456)
\end{aligned}
$$

$$
\begin{aligned}
|\xi_{ES}\rangle_2 &= |\xi_{AUTH1}\rangle \otimes |\Phi^+\rangle_{T_BB} \\
&= \frac{1}{2\sqrt{2}}(|0000\rangle + |0010\rangle + |1000\rangle - |1010\rangle + \\
&\qquad |0101\rangle + |0111\rangle + |1101\rangle - |1111\rangle)_{T_{E(A)}T_BE(A)B} \\
&= \frac{1}{4}\Big(\big(|\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle + |\Psi^-\rangle\big)_{T_{E(A)}T_B}|+\rangle_{E(A)}|+\rangle_B + \\
&\qquad \big(|\Phi^+\rangle - |\Phi^-\rangle + |\Psi^+\rangle - |\Psi^-\rangle\big)_{T_{E(A)}T_B}|-\rangle_{E(A)}|+\rangle_B + \\
&\qquad \big(|\Phi^+\rangle + |\Phi^-\rangle - |\Psi^+\rangle - |\Psi^-\rangle\big)_{T_{E(A)}T_B}|+\rangle_{E(A)}|-\rangle_B + \\
&\qquad \big(-|\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle - |\Psi^-\rangle\big)_{T_{E(A)}T_B}|-\rangle_{E(A)}|-\rangle_B\Big) \qquad (457) \\
& \qquad (458)
\end{aligned}
$$

During the second (optional) eavesdropping test Eve can be detected with the probability of $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + 8 * \frac{1}{16}\right) = \frac{1}{4} \qquad (459)$$

Each Bell state $|\Phi^+\rangle_{T_{E(A)}T_B}$, $|\Phi^-\rangle_{T_{E(A)}T_B}$, $|\Psi^+\rangle_{T_{E(A)}T_B}$, and $|\Psi^-\rangle_{T_{E(A)}T_B}$ occurs for all x basis measurement combinations $|+\rangle_{E(A)}|+\rangle_B$, $|-\rangle_{E(A)}|+\rangle_B$, $|+\rangle_{E(A)}|-\rangle_B$, and $|-\rangle_{E(A)}|-\rangle_B$. Hence, Eve can neither derive Bob's final basis nor can she deduce Bob's derivation of her basis ($\rho_S = 0$).

Receiver Impersonation in QDC

If the errors are not recognised in the first eavesdropping test, the system changes to one of the following states $|\xi_{ES}\rangle_3$ or $|\xi_{ES}\rangle_4$ after Trent's entanglement swapping and Alice's and Eve's x basis measurements.

$$
\begin{aligned}
|\xi_{ES}\rangle_3 &= |\Phi^+\rangle_{T_AA} \otimes |\xi_{AUTH0}\rangle \\
&= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{T_AT_{E(B)}AE(B)} \\
&= \frac{1}{2\sqrt{2}}\Big(\big(|\Phi^+\rangle + |\Psi^+\rangle\big)_{T_AT_{E(B)}} |+\rangle_A |+\rangle_{E(B)} \; + \\
&\qquad \big(|\Phi^-\rangle + |\Psi^-\rangle\big)_{T_AT_{E(B)}} |-\rangle_A |+\rangle_{E(B)} \; + \\
&\qquad \big(|\Phi^-\rangle - |\Psi^-\rangle\big)_{T_AT_{E(B)}} |+\rangle_A |-\rangle_{E(B)} \; + \\
&\qquad \big(|\Phi^+\rangle - |\Psi^+\rangle\big)_{T_AT_{E(B)}} |-\rangle_A |-\rangle_{E(B)} \Big) \qquad (460) \\
|\xi_{ES}\rangle_4 &= |\Phi^+\rangle_{T_AA} \otimes |\xi_{AUTH1}\rangle \\
&= \frac{1}{2\sqrt{2}}(|0000\rangle + |0001\rangle + |0100\rangle - |0101\rangle + \\
&\qquad |1010\rangle + |1011\rangle + |1110\rangle - |1111\rangle)_{T_AT_{E(B)}AE(B)} \\
&= \frac{1}{4}\Big(\big(|\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle - |\Psi^-\rangle\big)_{T_AT_{E(B)}} |+\rangle_A |+\rangle_{E(B)} + \\
&\qquad \big(|\Phi^+\rangle + |\Phi^-\rangle - |\Psi^+\rangle + |\Psi^-\rangle\big)_{T_AT_{E(B)}} |-\rangle_A |+\rangle_{E(B)} + \\
&\qquad \big(|\Phi^+\rangle - |\Phi^-\rangle + |\Psi^+\rangle + |\Psi^-\rangle\big)_{T_AT_{E(B)}} |+\rangle_A |-\rangle_{E(B)} + \\
&\qquad \big(- |\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle + |\Psi^-\rangle\big)_{T_AT_{E(B)}} |-\rangle_A |-\rangle_{E(B)} \Big) \qquad (461)
\end{aligned}
$$

Again, the detection probability totals $\frac{1}{4}$.

$$\rho_D = \frac{1}{2} * \left(0 + 8 * \frac{1}{16}\right) = \frac{1}{4} \qquad (462)$$

Because each Bell state occurs for each combination in the final bases, Alice and Eve cannot deduce their final measurement result and $\rho_S = 0$.

J.5 Advanced Impersonation Attacks

Impersonation of Sender or Receiver and Authority

The sender and receiver impersonations can be derived from J.4.

Impersonation of the Authority

In the third impersonation attack Eve sends the A- and B-qubits unencoded to Alice and Bob, respectively. Alice's and Bob's decoding change the A- or B-system to one of the following states (463) – (466).

$$
\begin{aligned}
|\xi_{AUTH0}\rangle_A &= I_A\left(|\Phi^+\rangle_{E(T)_A A}\right) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{E(T)_A A} \qquad (463)\\
|\xi_{AUTH1}\rangle_A &= H_A\left(|\Phi^+\rangle_{E(T)_A A}\right) \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{E(T)_A A} \qquad (464)\\
|\xi_{AUTH0}\rangle_B &= I_B\left(|\Phi^+\rangle_{E(T)_B B}\right) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{E(T)_B B} \qquad (465)\\
|\xi_{AUTH1}\rangle_B &= H_B\left(|\Phi^+\rangle_{E(T)_B B}\right) \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{E(T)_B B} \qquad (466)
\end{aligned}
$$

During the first eavesdropping test Eve can be detected with the probability of $\frac{1}{2}$.

$$\rho_D = 2 * \frac{1}{2}\left(0 + \frac{1}{2}\right) = \frac{1}{2} \qquad (467)$$

After Eve's entanglement swapping and Alice's and Bob's x basis measurements the entire system is in one of the following states (468) – (470). In eq. (469) the upper sign line represents $|\xi_{ES}\rangle_2 = |\xi_{AUTH1}\rangle_A \otimes |\xi_{AUTH0}\rangle_B$ and the lower sign line denotes $|\xi_{ES}\rangle_3 = |\xi_{AUTH0}\rangle_A \otimes |\xi_{AUTH1}\rangle_B$. In eq. (470) same states are combined, resulting in the multiplier 2 and different sign lines.

$$
\begin{aligned}
|\xi_{ES}\rangle_1 &= |\xi_{AUTH0}\rangle_A \otimes |\xi_{AUTH0}\rangle_B \\
&= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{T_A T_{E(B)} A E(B)} \\
&= \frac{1}{2\sqrt{2}}\Big(\big(|\Phi^+\rangle + |\Psi^+\rangle\big)_{T_A T_{E(B)}}|+\rangle_A|+\rangle_{E(B)} + \\
&\qquad \big(|\Phi^-\rangle + |\Psi^-\rangle\big)_{T_A T_{E(B)}}|-\rangle_A|+\rangle_{E(B)} + \\
&\qquad \big(|\Phi^-\rangle - |\Psi^-\rangle\big)_{T_A T_{E(B)}}|+\rangle_A|-\rangle_{E(B)} + \\
&\qquad \big(|\Phi^+\rangle - |\Psi^+\rangle\big)_{T_A T_{E(B)}}|-\rangle_A|-\rangle_{E(B)}\Big) \qquad (468)\\
|\xi_{ES}\rangle_2 &= |\xi_{ES}\rangle_3 \\
&= |\xi_{AUTH1}\rangle_A \otimes |\xi_{AUTH0}\rangle_B \text{ or } |\xi_{AUTH0}\rangle_A \otimes |\xi_{AUTH1}\rangle_B \\
&= \frac{1}{4}\Big(\big(|\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle \pm |\Psi^-\rangle\big)_{T_{E(A)} T_B}|+\rangle_{E(A)}|+\rangle_B + \\
&\qquad \big(|\Phi^+\rangle \mp |\Phi^-\rangle \pm |\Psi^+\rangle \mp |\Psi^-\rangle\big)_{T_{E(A)} T_B}|-\rangle_{E(A)}|+\rangle_B + \\
&\qquad \big(|\Phi^+\rangle \pm |\Phi^-\rangle \mp |\Psi^+\rangle \mp |\Psi^-\rangle\big)_{T_{E(A)} T_B}|+\rangle_{E(A)}|-\rangle_B + \\
&\qquad \big(-|\Phi^+\rangle + |\Phi^-\rangle + |\Psi^+\rangle \mp |\Psi^-\rangle\big)_{T_{E(A)} T_B}|-\rangle_{E(A)}|-\rangle_B\Big) \qquad (469)
\end{aligned}
$$

$$
\begin{aligned}
|\xi_{ES}\rangle_4 &= |\xi_{AUTH1}\rangle_A \otimes |\xi_{AUTH1}\rangle \\
&= \frac{1}{4}(|0000\rangle + |0001\rangle + |0100\rangle - |0101\rangle + \\
&\quad |0010\rangle + |0011\rangle + |0110\rangle - |0111\rangle + \\
&\quad |1000\rangle + |1001\rangle + |1100\rangle - |1101\rangle - \\
&\quad |1010\rangle - |1011\rangle - |1110\rangle + |1111\rangle)_{E(T)_A E(T)_B AB} \\
&= \frac{1}{4\sqrt{2}}\Bigg(2 * \left(|\Phi^+\rangle + |\Phi^-\rangle \pm |\Psi^+\rangle \mp |\Psi^-\rangle\right)_{E(T)_A E(T)_B} |+\rangle_A |+\rangle_B + \\
&\qquad 2 * \left(\pm |\Phi^+\rangle \pm |\Phi^-\rangle + |\Psi^+\rangle - |\Psi^-\rangle\right)_{E(T)_A E(T)_B} |-\rangle_A |+\rangle_B + \\
&\qquad 2 * \left(\pm |\Phi^+\rangle \mp |\Phi^-\rangle + |\Psi^+\rangle + |\Psi^-\rangle\right)_{E(T)_A E(T)_B} |+\rangle_A |-\rangle_B + \\
&\qquad 2 * \left(|\Phi^+\rangle - |\Phi^-\rangle \pm |\Psi^+\rangle \pm |\Psi^-\rangle\right)_{E(T)_A E(T)_B} |-\rangle_A |-\rangle_B \Bigg)
\end{aligned} \tag{470}
$$

During the second optional eavesdropping test Eve can be detected with the probability of $\frac{3}{8}$.

$$
\rho_D = \frac{1}{4} * \left(0 + 2 * \frac{1}{2} + \frac{1}{2}\right) = \frac{3}{8} \tag{471}
$$

Eve cannot be successful, since each Bell state occurs twice for each combination in the final bases of Alice and Bob ($\rho_S = 0$).