European Quantum Key Distribution Network

Henning Weier

München 2011

European Quantum Key Distribution Network

Henning Weier

Dissertation at the Faculty of Physics
of the
Ludwig–Maximilians–Universität München

Henning Weier
born in Düsseldorf, Germany

München, 17.06.2011

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Wolfgang Zinth
Tag der mündlichen Prüfung: 29.07.2011

Zusammenfassung

Information ist eines der höchsten Güter unserer Gesellschaft, sichere Kommunikation essenziell für Wirtschaft, nationale und internationale Stabilität. Die Quantenschlüsselverteilung (QKD) hat ein Problem der klassischen Informatik, nämlich den sicheren Austausch kryptographischer Schlüssel, gelöst. In den vergangenen 27 Jahren seit der Erfindung der QKD wurde viel Aufwand getrieben, sie für praktische Anwendungen einsetzbar zu machen und die Lücke zwischen theoretischen Sicherheitsbeweisen und realen Geräten zu schließen.
Diese Arbeit berichtet von verschiedenen Aspekten unseres freiraumoptischen QKD-Systems. Im ersten Teil wird dessen Einbindung in das europäische QKD-Netzwerk im Rahmen des SECOQC-Projekts beschrieben, für das dieses System über anderthalb Monate verlässlich sicheres Schlüsselmaterial geliefert hat. Das Gerät arbeitete dort erstmals tagsüber, ohne dass die helle Umgebung einen wesentlichen Einfluss auf den Betrieb hatte. So wurde die Tagungsstätte mit dem faserbasierten QKD-Basisnetz verbunden und die Realisierbarkeit heterogener QKD-Netzwerke bestätigt.
Das zweite Hauptaugenmerk dieser Arbeit liegt auf der Sicherheitsanalyse unseres QKD-Systems. Obwohl die Sicherheit des QKD-Prinzips zweifellos bewiesen ist, passen die Annahmen in diesen Beweisen nicht zu den realen Ausführungen der QKD-Systeme. Daher ist es überaus wichtig, diese Diskrepanz allmählich zu beseitigen. Ein vielversprechender Ansatz dazu ist die Adaption des klassischen Zertifizierungsprozesses. Dabei wird innerhalb ein Annahmenkatalog aufgestellt und gezeigt, dass jeder bekannte Angriff durch Gegenmaßnahmen abgesichert ist. In der vorliegenden Arbeit wird (soweit anwendbar) dieser systematische Ansatz verfolgt, um die Schwachstellen und mögliche Sicherheitsmaßnahmen zu diskutieren.
Eine dieser implementierungsabhängigen Schlupflöcher, nämlich die Totzeit von Einzelphotondetektoren wurde ausgenutzt, um einen neuen Angriff auf das System durchzuführen. Es war dadurch möglich, mehr als 98% des Schlüssels abzuhören, ohne einzelne Photonen detektieren zu müssen. Das zeigt eindrücklich, dass unsere Attacke eine unmittelbare Gefahr darstellt. Glücklicherweise gibt es eine einfache Maßnahme gegen diesen Angriff: Indem man die Vorspannung der Detektoren überwacht, kann man entscheiden, ob alle aktiv sind. Werden nur diese Ereignisse für die Schlüsselgenerierung verwendet, kann man diese und ähnliche Angriffe sicher abwenden.
Bisher verwenden einige wenige Banken QKD-Systeme, um ihre Daten zu schützen. Ist die Sicherheit dieser Geräte zertifiziert, die Integration unpromlematisch und natürlich der Preis gerechtfertigt, wird erwartet, dass der Bedarf deutlich steigt.

Abstract

Information is one of the key assets of our society. Secure communication is vital for economy, national and international stability. Quantum key distribution (QKD) has closed a remaining security loophole in classical information science, namely the secure cryptographic key exchange. In the past 27 years since the invention of QKD a lot of effort has been invested to bring QKD to practical applicability and bridge the gap between the theoretic security proofs and real devices.
This document reports on several aspects of our free-space quantum key distribution system. The first part covers the integration of this system into the European QKD network within the project SECOQC, where it was reliably producing secure key material during a period of about 1.5 months. There, the system worked even in bright daylight without significant influence on the output. It connected the public demonstration venue to the fibre based QKD backbone. The results of the project show that even heterogeneous QKD networks are feasible with today's technology.
The second focus of this work is the security analysis of our QKD system. While it is true that the security of the QKD principle is proven, the assumptions of these proofs are not met in realistic devices. Hence it is of utmost importance that this discrepancy will be diminished and eventually closed. One promising approach to this end could be to adopt the methodology of classical counterparts, e.g. the certification process. There, a set of assumptions is compiled and within these assumptions it is made plausible that every possible threat is countered by a measure to ensure security. In this document this systematic procedure (to the extent that seemed appropriate) has been used to report on the possible vulnerabilities and their potential countermeasures concerning this specific QKD system.
One of these implementation-specific loopholes, the dead time of the single photon detectors has been exploited in particular to launch a new attack on our QKD system. It was possible to gain more than 98% of the sifted key without even having to intercept the single photon stream from legitimate transmitter to receiver. This fact clearly shows that our attack is one of the most imminent threats to the system. Fortunately, a possible countermeasure against this attack is as simple: By monitoring the bias voltage of the single photon detectors it can be evaluated if all detectors were active at the time of a detection event. When only those events are being processed this and similar attacks are rendered impossible.
So far, a few banks are slowly employing QKD systems to protect their data. Given certified security for those devices, unproblematic integration into the existing networks and of course a justifiable price, the demand is expected to grow significantly.

Contents

1 Introduction

Digital communication plays an increasingly important role in almost everybody's life. People send and receive emails, go shopping in the world-wide web and manage their bank accounts and transactions conveniently from their homes. While some of these activities are relatively insensitive to security issues, some certainly are not. The fact that the new German identity card contains a digital identification option indicates that secured digital communication will soon also replace (at least partly) the conventional exchange of information between citizens and governmental organisations. As first examples, tax information has started to be delivered digitally, and public authorities have huge amounts of sensitive data to convey between them. Either because of privacy protection or for reasons of national security, this information has to remain secret to anybody but the legitimate receiver. The advantage of the structure of the internet, which connects more or less everyone to everyone else also is a possible security problem: Nobody can predict which route the information will take and who can gain access to it.
Cryptographic methods have been installed to prevent sensitive data from being read or even changed. Unfortunately, the security of most of those methods is very hard to assess. For example, asymmetric cryptography, widely used for securing most standard web transactions with security needs (like web-based bank transactions) relies on the fact that it is difficult to factorise large numbers into their constituting primes. Although one does not know a classical algorithm to solve such a problem efficiently today, it could not be shown (despite a lot of effort over the past centuries) that there is none. In fact, one of the most outstanding features of a quantum computer is the option to use the so-called Shor algorithm which does exactly that: factorising large integers in polynomial time. Not only because of that it is believed that while asymmetric cryptography (as used today) is supposedly secure today, it may only stay so for 10 or 20 more years. For many applications hardly anybody will be concerned about that; the data from most private transactions will be irrelevant in 10 or 20 years. But, especially when public authorities are involved, this may not be case. National (or international) security matters should hopefully be secure for a longer period of time and even private data like tax or health information should – for privacy protection – stay hidden ideally forever. This does not hold today. One could simply store the encrypted data and wait until the code can be broken and thus gain all information, even if after a long delay.
Yet, there is a information theoretically (i.e. provably) secure symmetric cryptography algorithm, the so-called one-time pad or Vernam cipher. It even is very

straightforward to perform, one simply needs a random bit string (called key) of the same length as the message and combines both by an XOR operation. All the receiver has to do are the same stages again (apply the same random bit string by XOR to the cipher text) to reconstruct the original message. The key may never be reused. Since each bit of the cipher text depends directly on the random bit string, the cipher text is also completely random (if the key is unknown). While this method is even very economic concerning computational power, the big problem is to equip both parties with the key. This exchange has to be equally secure and the communicating parties potentially need a lot of key material (for each message the key has to be as long as the message). Since there is no method to perform this task with information theoretic security in classical cryptography (the only possible way is a trusted courier), the one-time pad is used very rarely.
With quantum cryptography or quantum key distribution (QKD) as it is more precisely called, this gap can be filled. QKD is a method to securely generate a symmetric random key at both parties. There exist a number of security proofs confirming the information theoretic security. After the first QKD protocol had been published in 1984, some more protocols and first experimental demonstrations appeared in the 1990s. In the following decade, a lot of effort was spent to make QKD systems more compatible with potential users' demands, pushing primarily distances and key rates. While this is still a major development goal, another important task is being pursued for some years now, namely finding and fixing security loop holes in the setups. Although the security proofs are not subject to doubt, they rely on theoretic assumptions about the systems that are usually not met by real-world implementations.
In this thesis I will report on progress on both of these frontiers, on the one hand a QKD implementation within the EU project network SECOQC and on the other hand a general characterization of our setup concerning realistic attacks and a special attack that we have successfully launched on this setup as well as possible countermeasures.

2 Quantum Key Distribution

Contents

2.1 From Classical to Quantum Cryptography

Cryptography is the art of transforming a message into some illegible clutter of letters only the legitimate recipient shall be able to reconstruct. Already the ancient Egyptians, Spartans and Romans have developed their own techniques thousands of years ago. In more recent history, cryptographic algorithms have played important roles in World War I and II (e.g. the ENIGMA). The common availability of computers has boosted the potential of cryptography and its opponent cryptanalysis (the art of deciphering messages without being the legitimate conversation partner) to bring it to a whole new level. Furthermore, in our more and more digital world, sophisticated algorithms can now be used by almost anybody to secure his transmissions.

In modern cryptography, messages are strings of bits (bit = binary digit, value 0_B or 1_B). During the *encryption* process, the message gets transformed into the *ciphertext* with the help of a *crypographic key*. This is sent to the recipient, who uses his key for *decryption* to regain the original message. There are two kinds of cryptographic algorithms, *symmetric* ones where originator (usually called Alice) and recipient (Bob) use identical keys, and *asymmetric* ciphers, where the keys for encryption and decryption are different. The big advantage of asymmetric methods is that you can deploy the key for encryption (the *public key*) to everyone, while only the respective private key needs to be kept safe. This greatly simplifies the key distribution task. The caveat, on the other hand, is that asymmetric algorithms are based on a mathematical problem that is not proven to be hard to solve. In effect, symmetric algorithms are the method of choice for sensitive information that

needs to stay safe even for the next 20 or more years. With the advent of modern information theory one realized that there is an information theoretically secure (ITS) symmetric algorithm called *one-time pad* or *Vernam cipher*. It needs a random key as long as the message and applies a bitwise XOR operation between those two. The resulting ciphertext is as random as the key, but carrying out the same operation with the identical key again reconstructs the message. So it is actually very simple to use, whereas asymmetric algorithms usually need a lot of computational resources. The only problem with the one-time pad is that it needs symmetric key material as long as the ciphertext, since keys may not be reused.

As there is no known classical method of ITS key generation or key growing, the key material for one-time pads had to be transported by trusted couriers or similarly laborious procedures. Hence it was (and still is) used only very rarely. At the end of the 20th century, it turned out that symmetric key distrubion was one of the problems that could be solved by quantum information. The method discovered (see next section) was first called quantum cryptography, but, since only a symmetric key pair is generated quantum key distribution (QKD) is the better naming (for an overview of the existing protocols and implementations see [1]).

In quantum information the analog of the classical bit is the quantum bit or qubit. The corresponding Hilbert space is spanned by the two computational basis states $|0\rangle$ and $|1\rangle$, so that a qubit state can be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. So in contrast to a classical bit the qubit can be in any coherent superposition between the basis states, too. It can be realized as any two-level system, like for example the spin of an electron. In the following, I will consider qubits to be represented by the polarization of single photons.

2.2 BB84 Protocol

In 1984, Ch. Bennett and G. Brassard published the first QKD protocol [2]. Although other protocols have been proposed since then, the so-called BB84 protocol is still the basis of many modern QKD systems. One reason for that is certainly its combination of simplicity and efficiency. It can be summarized as follows:

1. The transmitter (Alice) prepares photons randomly (and independently) in one of the four polarization states $|H\rangle, |V\rangle, |+\rangle, |-\rangle$ (horizontal, vertical, $+45°$ and $-45°$) and sends them to the receiver (Bob). He tries to analyse the polarization of the individual photons, randomly choosing the basis (H/V or $+/-$).

2. Bob tells Alice, which of the photons he has detected. Alice removes the rest of the entries from her list. Both parties now share the so-called *raw key* which

is formed as:

$$\left.\begin{matrix}|H\rangle \\ |+\rangle\end{matrix}\right\} \mapsto 0_B \qquad \text{and} \qquad \left.\begin{matrix}|V\rangle \\ |-\rangle\end{matrix}\right\} \mapsto 1_B \tag{2.1}$$

3. Alice and Bob exchange the basis settings they used for preparation and measurement, respectively. They remove those entries from their lists, where they chose different bases. This procedure is called *sifting* and the resulting keys are called *sifted keys*. Ideally, Alice and Bob's sifted keys should be identical, but eavesdropping on the quantum signals will lead to erroneous bits (see for example section 2.2.1). Furthermore, because of experimental imperfections, some errors will have been introduced into the keys. Usually, all existing errors are attributed to the misdeeds of an eavesdropper (Eve).

4. During the *error correction* process, the non-matching bits will be identified and corrected. For the BB84 protocol, this procedure is usually based on the well-known two-way communication algorithm called *Cascade* [3]. To avoid confusion, it should be noted that this error correction process is purely classical unlike quantum error correction protocols used e.g. in quantum computation. The error estimation allows Alice and Bob to calculate an upper limit on the information, Eve may have gained about their keys.

   During the error correction procedure, information about the key (in the form of parity bits) is exchanged between Alice and Bob. They count the number of disclosed bits and add them to the number of erroneous bits.

5. After error correction, Alice and Bob share (with a very high probability) perfectly correlated keys. But since some information may have leaked to a potential eavesdropper (due to an actual attack on the qubits or due to listening to the error correction communication), the legitimate parties can reduce Eve's knowledge about the resulting key by a classical method called *privacy amplification* [4, 5] to an arbitrarily low value. It basically uses so-called universal$_2$ hash functions [6] that scramble the keys maximally while at the same time shrinking them. More information about the shrinking factor will be provided in section 2.2.2.

The (classical) communication between Alice and Bob needs not be encrypted, but definitely authenticated to rule out complete man-in-the-middle attacks (see e.g. section 5.2.6). Thus for ITS authentication [7], the legitimate parties inevitably need some pre-shared secret. This is why quantum key distribution is sometimes also called quantum secret growing. While the need for authentication was already explicitly mentioned in the original publication [2], steps 4 and 5 have been developed later. Especially the method of privacy amplification is still extended to include more and more imperfections of real systems. This will be discussed further in later sections and chapters.

2.2.1 A Simple Attack

As a simple illustration for the origin of this security advantage, the so-called *intercept-resend attack* can be regarded: The general setting is that Eve has cut the quantum channel between Alice and Bob, analyzes the photons sent from Bob and sends the state to Alice that she has measured. Suppose Alice sends an $|H\rangle$ state and Bob has his analyzer set to the H/V basis (otherwise the event will be discarded during sifting). Now, if Eve measures the polarization in the H/V basis, too, she will find $|H\rangle$ and transmit $|H\rangle$ again and Bob will measure $|H\rangle$, too. Eve will know the bit, she will not have introduced an error. In 50 % of the cases, Eve will, however, set her analyzer to the $+/-$ basis. Then her measurement outcome is random and she will transmit $|+\rangle$ or $|-\rangle$. Bob's result will now be random, too, and in 50 % of those cases (so in total in 25 % of all cases), he will find $|V\rangle$, i.e. the opposite polarization that Alice has sent. In the end, Alice and Bob will have a quantum bit error rate (QBER) of 25 %, which means they will detect Eve's presence and discard the key. There are, of course, more sophisticated attacks, but it has been shown (see next section) that there exists an upper bound for the amount of information an eavesdropper could gain for a given QBER [8].

2.2.2 Security Proofs

The earlier proofs that QKD is ITS (also called unconditionally secure) [9–11] were a great achievement. This is especially true since a little earlier it had been shown that other quantum assisted protocols like quantum bit commitment were not secure [12]. Still, the first QKD security proofs contained some assumptions that were more or less difficult to meet in reality. Among these were noiseless channels or quantum computers for Alice and Bob. P. Shor and J. Preskill [13] combined ideas from previous publications to end up with a relatively simple proof for the BB84 protocol that only required the QBER to be below a certain threshold.
It was still assumed, however, even if that was not always explicitly mentioned, that the transmitter should only emit a single qubit at a time and the detector should only analyze this qubit and that it shouldn't be possible to gain any information about the qubit other than by measuring the chosen degree of freedom (here: polarization). As a first major step closer to realistic systems, new proofs tackled the requirement of ideal single photon sources in the transmitter. It was shown that the BB84 protocol was indeed secure against the most general attacks, even when attenuated laser pulses were used instead of true single photon sources [8, 14]. These proofs assumed that all multiphoton (so-called tagged) emissions were abused by the eavesdropper (see section 5.2.4) which imposed severe restrictions on the key rate at higher loss factors [15]. This problem was further resolved with the so-called decoy state extension to the protocol, described in section 6.2.7.2. It introduces laser pulses of different intensities to tighten the bound on tagged pulses and calculates their

influence according to [8].
It should be noted that the lack of true single photon sources was certainly not the only, most probably not even the most dangerous gap between existing proofs and existing QKD devices. H.-K. Lo, one of the co-authors of one of the security proofs, and co-workers demonstrated an attack using timing as an additional degree of freedom to show the vulnerability of a commercially sold QKD system [16]. More information about security relevant imperfections of our QKD system will be given in chapters 5 ff. While the aforementioned attack has also been inhibited (by the same group) [17], it is still one of the big challenges of QKD research to bring proofs and real QKD systems closer together [18].

2.3 Other Protocols

Of course, the BB84 protocol is not the only one that has been proposed until now. Ch. Bennett actually invented a second one himself, the so-called B92 or two-state protocol [19] that uses only two (non-orthogonal) states. Another noteworthy example is the SARG protocol [20]. It's advantage is that it is identical to BB84 on the hardware level, but it uses a different sifting method (closer to the B92), so that it is more robust against the photon-number splitting attack (see 5.2.4.1).
The protocols I've named so far have all been members of the so-called *prepare-and-measure* schemes. Alice prepares the qubits, sends them to Bob, who measures them. A second class of protocols uses a source of entangled qubits and two receivers. These methods usually have the advantage that the source does not have to be trusted. It's integrity is checked as part of the protocol. The Ekert or E91 protocol [21] uses the CHSH inequality [22] (a special type of Bell's inequality) to verify that the entangled state is genuine. For a test of the CHSH inequality a third basis has to be introduced, increasing the hardware complexity. This can be omitted in the BBM protocol [23], while still being able to detect a faulty source. It is more or less the entangled version of BB84, using the otherwise discarded unequal basis choices for the source check.
Then there is a conceptually different approach, the so-called continuous variable (CV) scheme. Instead of employing the discrete variables of single photon states as information carriers, here the continous variables of coherent states are used [24–28]. These schemes are especially interesting for fiber communiation in the telecommunication regime ($\lambda \approx 1.3$ μm and $\lambda \approx 1.5$ μm), since (in this wavelength region) problematic single photon detectors are not needed.

3 SECOQC Network

Contents

3.1 Overview

In this part I would like to give an overview over the achievements of the EU project SECOQC (Development of a Global Network for SEcure COmmunication based on Quantum Cryptography) [29], that was carried out by 41 research and industrial organizations from the EU, Switzerland and Russia between April 2004 and October 2008. While in the beginning, many different approaches to QKD and QKD systems were pursued, later the main tasks were to bring together the different QKD techniques and systems to form a network that supplies secure cryptographic key pairs to any two of its nodes.

3.1.1 Goal: Integrated Network

QKD systems that have been demonstrated so far are usually point-to-point links, i.e. they connect two parties directly. One could argue that this is really exactly

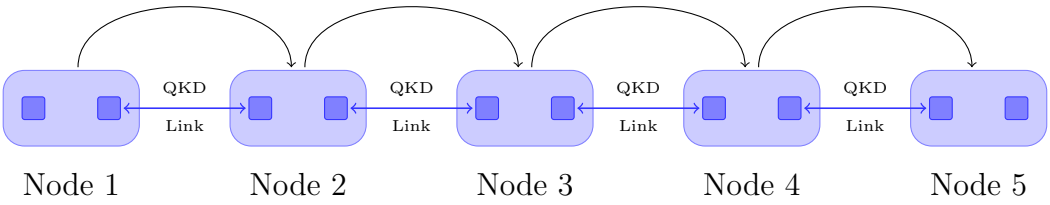

Figure 3.1: Hop-by-hop message transport from node 1 to node 5 with only point-to-point links in between. In the trusted repeater scenario, each transmitting node encrypts the message with a key it shares with the receiving node which then decrypts the message again.

what one needs, since whenever two parties want to communicate privately, they would just need one of these links. But as soon as there are more than two parties, and anyone might want to communicate with anyone else, the effort involved in setting up individual links between each pair of members scales (asymptotically) quadratically with the number of participants. This problem had to be solved before in similar situations, e.g. with telephones or computers and the usual solution is to build network structures so that everyone is connected to everyone else, but not necessarily by a direct link.
It is important to note that the network discussed here was planned (and implemented) as a means to generate and distribute ITS keys. It was not, however, meant to provide secure communication services. Nevertheless, for demonstration purposes, the QKD network was extended by some applications that made use of the key.

3.1.2 Trusted Repeaters vs. Quantum Channel Switching

Unlike in classical connections, QKD links are necessarily point-to-point in the sense that unknown quantum signals cannot be distributed (identically) to different parties. Yet, there are two conceptually different ways of interconnecting the specific point-to-point links to form a network: One possibility is to switch the path of the qubits to direct them to their final destination. This is called quantum channel switching (QCS). The other option (the one used in the SECOQC project) is that of the trusted repeater (TR). Here, secrets are generated by QKD between the parties sharing a direct QKD link, but then these secrets can be transported securely over a classical network in a so-called hop-by-hop fashion (see Fig. 3.1). Each node takes the key that shall be transmitted to a distant node, plus an authorization tag, encrypts both with a one-time pad using a key it shares with the next node in line and sends it there. The latter node decrypts it, checks the authentication tag and uses the same procedure to transfer it to the next node on the route.
Both methods have advantages and drawbacks, some of which shall be briefly discussed here:

- The main disadvantage of the TR scenario is that all of the nodes (that contribute to the key transport) have to be trusted (hence the name), as they have direct access to the secret key. This might or might not be a knock-out criterion, depending on whether the communicating parties can trust the QKD network provider, perhaps because it's all one and the same organization. This constraint does not apply to the case of QCS, here only the endpoints have to be regarded secure (which is generally always the case).

- One advantage of the TR model is that it extends the range of QKD secured communication channels even with todays technology. While it consumes a lot of key material, there is no technical problem with a lot of hops. In QCS networks, quantum repeaters could overcome current distance limitations, but they are still not available for such purposes. As long as that does not change, QCS is restricted to the distance which can be achieved with a single link.

- Another advantage of the TR system is that the networks can be composed of different link techniques, while that is (at least in general) difficult for the QCS approach. The benefit is that depending on the circumstances the optimal method can be used in the TR case for each link. Today different techniques seem to be promising for different scenarios: Various fiber systems would probably be used when the distance is some tens of km (providing fibers can be deployed), while for short ranges and very long ones (with the help of satellites), as well as for mobile applications, free space links might be the better option.

- There is one more major difference between the two types of networks: While they both need pre-shared secrets with their next neighbors for authentication purposes, TR nodes only have a few next neighbors, whereas for QCS nodes every other node is a direct link partner, so that the amount of pre-shared secrets that has to be deployed at installation time scales quadratically with the number of nodes. A large network of this type would certainly become more difficult to manage.

Summarizing these arguments, with todays technology (i.e. without practical quantum repeaters) and under the assumption that all nodes are trustworthy, the TR type of network is favorable compared to the QCS idea and was hence implemented in the SECOQC network.

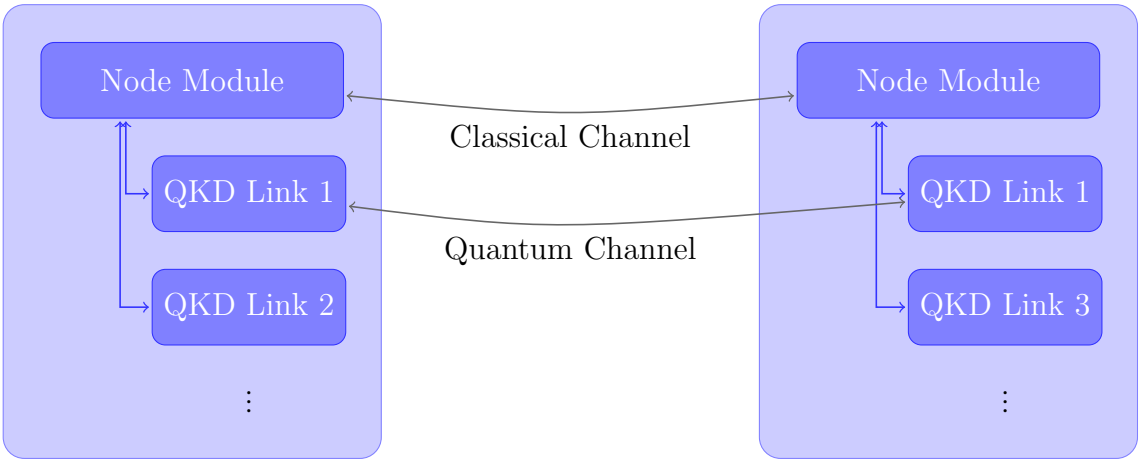

Figure 3.2: Schematic drawing of a SECOQC node.

3.2 Architecture and Topology

3.2.1 Nodes: Providing Classical Functionality

The classical functionality of the TR nodes of the network has to enable several requirements. Not only should they support the classical communication required for QKD methods, they should furthermore carry out the whole key transport service, including routing and ITS authentication, encryption/ decryption of transported key material as well as its management and storage. A schematic drawing of two nodes is shown in Fig. 3.2.

Each node contains a so-called node module and at least one QKD device. Usually, stand-alone QKD devices use a more or less direct classical channel for sifting, error correction, privacy amplification and authentication of all the classical messages involved in these procedures. In the SECOQC network, all classical communication was routed through the node modules and the authentication was taken over by them, too. This was decided, firstly since the node modules were to take care of the key management and ITS authentication needs fresh keys from time to time and secondly because authentication works the same regardless of the actual QKD method implemented in the specific device. This is not true for sifting, error correction and privacy amplification, hence this was left in the responsibility of the QKD devices. When the device has processed a certain amount of key material and got confirmation from the node module that all implicated messages were authentic, the key is pushed to the node module for further use.

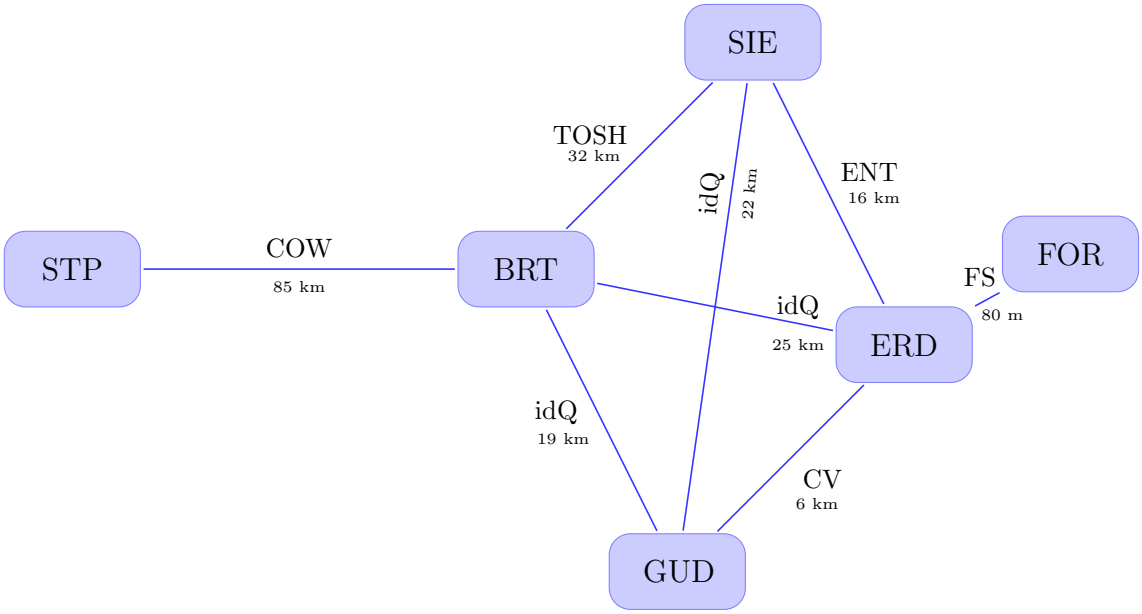

Figure 3.3: Topology of the SECOQC network in Vienna. The node STP was located near St. Pölten, approximately 50 km West of Vienna, this and the nodes BRT (Breitenfurterstrasse), SIE (Siemensstrasse), GUD (Gudrunstrasse), ERD (Erdberger Lände) are part of the Siemens Austria fiber communication network. The node FOR (Siemens Forum) was not connected to the network by fiber, but the public demonstration took place there, so our free space link was used to bridge the gap.

3.2.2 SECOQC Network Topology in Vienna

The QKD network demonstrator was set up in the Vienna area in 2008. Four nodes of a fiber network ring in Vienna were provided at Siemens Austria branches: One at Breitenfurterstrasse (BRT), one at Siemensstrasse (SIE), one at Gudrunstrasse (GUD) and one at Erdberger Lände (ERD) (see Fig. 3.3). These nodes were not only connected by a dedicated (dark) fiber each to their neighbors in the ring, but also "diagonally". Since there was no direct connection between BRT and ERD or SIE and GUD, this was done by directly connecting one fiber from SIE and one from GUD at BRT and the same at ERD. Hence the "diagonals" are as long as the (shorter) sums of the respective edges.
In addition to the fiber ring, there was one fiber connection to a telecommunication facility near St. Pölten (STP), about 50 km West of Vienna. The fiber link from BRT to STP, totaling 85 km, was the longest one in the network.
Just across the road from ERD there is the Siemens Forum (FOR), were the public demonstration was held in October 2008. To connect this building to the SECOQC network, our free space system was set up on the roofs of ERD and FOR. The results of that will be discussed in the next chapter. I will now summarize the other QKD systems that were used in the network.

3.3 QKD Point to Point Links

3.3.1 idQ: Autocompensating Plug&Play System

Three of the QKD point to point links were equipped with variations of ID Quantique's commercially available QKD system called "Cerberis". They are based on the so-called plug and play autocompensating design [30, 31] (see Fig. 3.4): There, a strong laser pulse ($\lambda = 1550$ nm) is sent from Bob to Alice after passing through an unbalanced interferometer, with a polarization rotation by 90° in the long arm. At Alice the pulse is reflected at a Faraday mirror (FM), then some phase shift is applied (PM1) to encode the quantum state, the pulse is attenuated strongly (VA) according to the measured intensity on the calibration detector (CD) and returned to Bob. He can set a certain phase (PM2) in one arm of his interferometer and analyze the state with a single photon detector each at the output (D1, D2). Since one of the beam splitters of Bob's interferometer is a polarizing one (PBS) and all fibers inside Bob are polarization maintaining, both pulses take the same path and together with the Faraday mirror this compensates for the otherwise possibly problematic polarization changes in the fibers. The circulator (C) makes sure that the pulses from the laser are directed towards Alice while the photons from Alice hit the single photon detector. At Alice, the phase modulator (PM1) and the variable attenuator (VA) are controlled by a PC, at Bob the phase (PM2) is set by another PC.

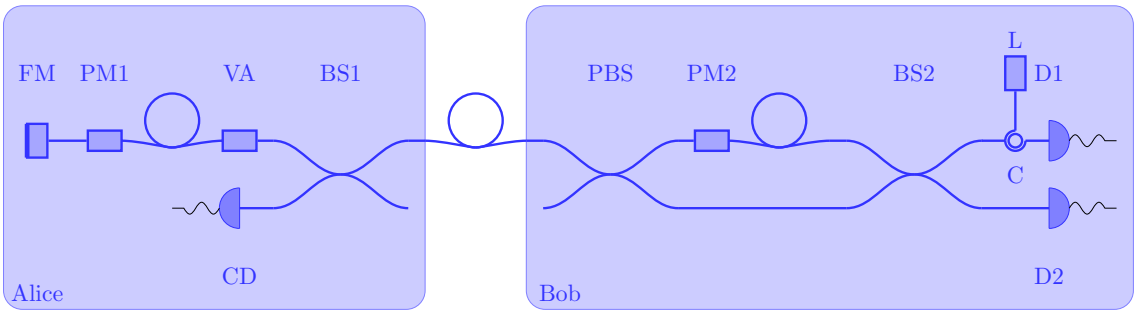

Figure 3.4: Schematic drawing of the autocompensating plug & Play QKD system from ID Quantique. The (bright) pulses from laser (L) are fed into an unbalanced interferometer formed by a beam splitter (BS2) and a polarizing beam splitter (PBS). All fibers are polarization maintaining and since the polarization in the longer (i.e. upper) arm is rotated by 90°, all the light exits the interferometer in the same port. At Alice, the pulses are reflected on the Faraday mirror (FM), their phase is modified (PM1) and they are attenuated (VA) to the single photon level according to the intensity on the calibration detector (CD). Then they return to Bob where they are analyzed in his interferometer relative to the phase setting of PM2.

Two protocols, BB84 and SARG [15,20] could be performed with these setups. The advantage of the SARG protocol is that – while keeping it secure against photon-number splitting attacks – it is less sensitive to losses than the standard BB84. In low loss situations, however, it produces less secure key than BB84. Hence it was implemented in the longer link from BRT to ERD. The links from BRT to GUD and GUD to SIE were used with the BB84 protocol. The link between BRT and ERD produced about 1 kbit/s secure key.
A similar system from ID Quantique was employed to securely transport the ballot counts in several Swiss elections, including the national election in 2007.

3.3.2 COW: Coherent One Way System

The link between BRT and STP was fitted with a coherent one way system (COW) developed by the University of Geneva [32–34]. In the COW QKD protocol, qubits are encoded in time (see Fig. 3.5). Alice prepares mutually coherent laser pulses at certain time slots, and at each time slot, the intensity can be 0 or $\mu < 1$. A binary 0_B corresponds to a sequence $(0, \mu)$ and a binary 1_B to $(\mu, 0)$, but there are also decoy pulses with sequence (μ, μ). Bob mostly measures the time of arrival of photons on the data detector D_B. Some fraction of pulses (here: 10 %), however is reflected at a beam splitter to pass an unbalanced interferometer with a path length

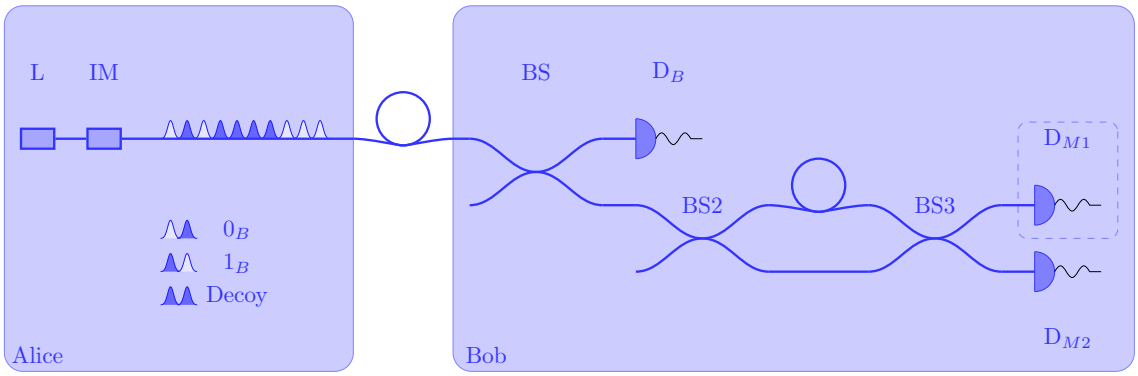

Figure 3.5: Schematic drawing of the COW setup. The attenuated laser pulses originating from Laser L are intensity modulated (intensity modulator IM) and sent towards Bob. The first (biased) beam splitter (BS) is used to decide whether a pulse is used for key bit generation or a coherence check. In the first case, the timing information of events at detector D_B is analyzed. In the latter case the interferometer is set such that detector D_{M2} should not click if two consecutive non-empty pulses arrive there. Hence, detector D_{M1} can be omitted for convenience.

difference equal to the time delay between two consecutive pulses. At its outputs, there are monitor detectors. These are used to check the level of coherence between consecutive non-empty pulses (i.e. in decoy pulses or $(0_B, 1_B)$ sequences), which is a measure for the estimation of a potential eavesdroppers knowledge. To this end, the timing information of detection events in detector D_{M2} are transmitted to Alice. The detector should never fire in those cases where two consecutive non-empty pulses arrive at the interferometer.
A brief description of the protocol:

1. Alice sends pulses to Bob, with the following probabilities: Bit 0_B, 1_B: $p(0_B) = p(1_B) = (1-f)/2$, decoy pulses $p((\mu,\mu)) = f$.
2. Bob reports the time of the detection events in detectors D_B and D_{M2}.
3. Alice announces which of the raw key bits have to be removed due to decoy states.
4. Alice calculates Eve's information from the number of detections in D_{M2}.
5. Alice and Bob perform error correction and privacy amplification.

The system is immune to PNS attacks, since acting on individual photons is generally detected. The decoy pulses were introduced to catch coherent attacks on consecutive pulses. However, it has to be noted that a complete security proof so far does not

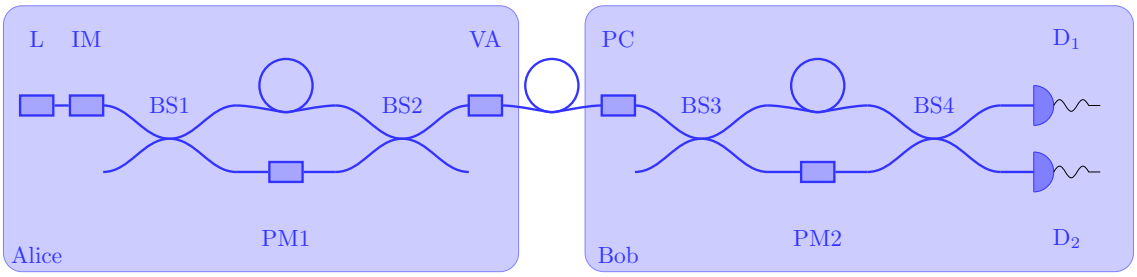

Figure 3.6: Schematic drawing of the TOSH setup. The attenuated pulses originating from a laser (L) are intensity modulated (IM) and pass through an unbalanced Mach-Zehnder interferometer with a phase modulator (PM1) in one arm. One of the outputs is attenuated (VA) and connected to Bob. There (unlike in the idQ setup) the birefringence effects of the fiber between Alice and Bob have to compensated (PC), before the pulses are analyzed by a second Mach-Zehnder interferometer and two single photon detectors (D_1, D_2).

exist and because of the very different approach, existing proofs of other QKD schemes seem to be difficult to adapt.

While in some different experiments [33, 34] such systems were equipped with superconducting single photon detectors, in this case free running InGaAs APDs [35] have been employed. The secure key rate was measured to be about 600 bit/s with a QBER between 3 % and 5 % over the substantial distance of 82 km optical fiber.

3.3.3 TOSH: One Way Weak Pulse System

Toshiba Research Europe Ltd contributed a one way weak pulse QKD link [36] to the network. It was based on a decoy-state extended BB84 protocol with phase encoding (see Fig. 3.6). Alice sends laser pulses through an asymmetric Mach-Zehnder interferometer with a phase modulator in one arm to prepare the qubits and Bob uses a similar interferometer with two APDs at the outputs to analyze them. Since unlike the systems from ID Quantique, here the pulses are sent directly from Alice to Bob, polarization changes in the fibers have to be compensated for actively.

The system was installed between the nodes BRT and SIE with a distance of 32 km. It yielded 3.1 kbit/s of secure key averaged over a period of 24 hours at a QBER of 2.6 %.

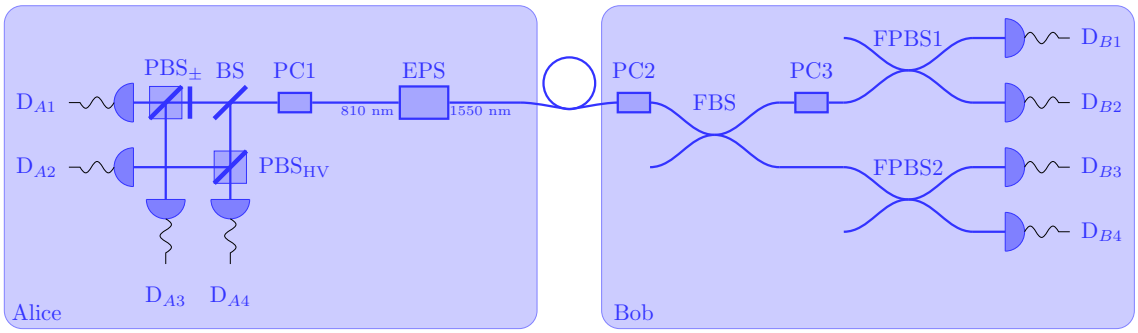

Figure 3.7: Schematic drawing of the basic ENT setup. The entangled photon source (EPS) at Alice emits photon pairs with one photon at $\lambda_1 = 810$ nm and its partner photon at $\lambda_2 = 1550$ nm. The first one is directed to a local free space polarization measurement apparatus (consisting of polarization controller PC1, beam splitter BS, polarizing beam splitters PBS_{HV} and $PBS_{\pm}$ and the four single photon detectors D_{A1} to D_{A4}. The longer wavelength photon is sent through the external fiber to Bob's setup, which is very similar to the one at Alice. The main difference is that here the components are fiber based and designed for 1550 nm. There are two polarization controllers (PC2, PC3), a fiber beam splitter (FBS), two polarizing fiber beam splitters (FPBS1, FPBS2) and four InGaAs APDs (D_{B1} to D_{B4}).

3.3.4 ENT: Entangled Photon Pair System

The link between SIE and ERD was provided in a joint action by the University of Vienna, the Austrian Institute of Technology and the Royal Institute of Technology of Kista in Sweden. The system [37] (see Fig. 3.7) is based on a down conversion source producing entangled photon pairs at non-degenerate wavelengths (one photon at $\lambda = 810$ nm, the other one at $\lambda = 1550$ nm). The polarization of the first one is measured locally, so that the transmitter part acts as a heralded single photon source with one of four randomly chosen polarizations. The output photons are coupled into the fiber and sent to Bob, who is equipped with a similar single photon polarization analyzer. In this system, Alice and Bob use the BBM protocol [23], which is effectively an entangled photon version of the BB84. It offers security without the need of measuring a Bell inequality like in the protocol proposed by Ekert [21], nevertheless remaining secure against tempering with the source.

The entangled photon source contains two nonlinear crystals (PPKTP) in type-I collinear phasematching, pumped by a cw laser at $\lambda = 532$ nm, yielding a trigger count rate of up to 1.5 MHz at 14 mW pump power. For the SECOQC demonstration, it was run at 6 mW pump power, resulting in 750 kHz trigger rate, a coincidence count rate at Bob of 8 kHz and a secure key rate of 2.5 kbit/s. The visibility was

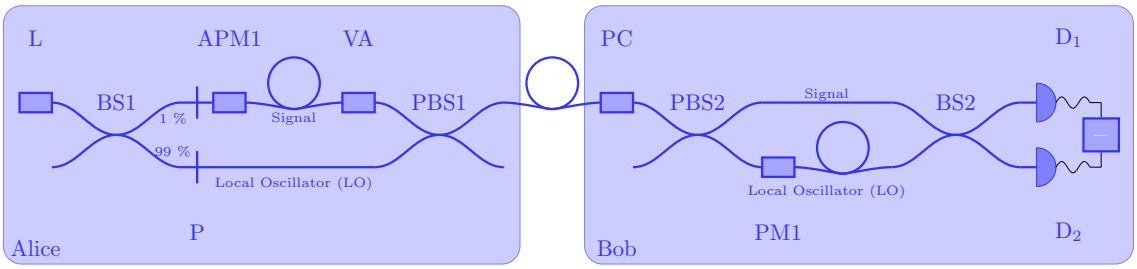

Figure 3.8: Schematic drawing of the CV setup. At Alice, a laser (L) pulse at $\lambda = 1550$ nm is split up by a 99:1 beam splitter (BS1) into a strong local oscillator (bottom) and a weak signal pulse (top) and both parts are polarized (P). The signal pulse is phase or amplitude modulated (APM1), delayed and further attenuated (VA), then both pulses are combined into one spatial mode by a polarizing beam splitter (PBS1) and sent to Bob. There, after polarization compensation (PC), the pulses are split up again by PBS2. Now the local oscillator part passes a phase modulator (PM1) to select which quadrature is measured and delayed to be overlapped with the signal pulse at BS2 in a homodyne detection.

on average 93 % and hence the QBER about 3.5 %.

3.3.5 CV: Continuous Variable System

The last long-distance QKD link set up in Vienna was developed by a collaboration of Laboratoire Charles Fabry de l'Institut d'Optique, THALES Research and Technology France and Université Libre de Bruxelles, connecting the nodes GUD and ERD. In contrast to all previously described systems, this one does not employ qubit encoding of photons detected by single photon detectors. Here the information is conveyed via the two quadratures (amplitude and phase) of the electromagnetic field of a coherent state [25]. This method is called continuous variable (CV) QKD. To prepare her signal, Alice splits off a small fraction of a laser pulse (pulse length 100 ns, repetition rate 500 kHz, wavelength 1550 nm), phase or amplitude modulates it and delays it. The strong and the weak pulse are (both time and polarization multiplexed) sent to Bob who de-multiplexes the two pulses and overlaps them on a beam splitter, performing a so-called homodyne detection of one of the two quadratures using PIN photodiodes. To evaluate the knowledge of an eavesdropper, the noise level is compared to the shot-noise limit. Unlike with previously discussed systems, the performance of CV systems can be significantly improved by sophisticated error correction algorithms. In this case, a method called reverse reconciliation [38, 39] was used to distill a key from the measurement values.
The system yielded a secret key rate of 8 kbit/s over a period of 57 h of continuous

operation over the link distance of 6.2 km.

3.3.6 FS: Last Mile Free Space QKD System

Our free space QKD system was used to bridge the gap between the closest one of fiber nodes (ERD) and the FOR building, where the public demonstration was held. A more detailed description of our system will be given in the following chapter.

4 Free Space QKD Link

Contents

Our free space QKD system uses the polarization of strongly attenuated laser pulses to run the BB84 protocol with decoy state extension [40]. I will now describe the system in more detail[1]:

4.1 Transmitter Optics

The transmitter's task is to prepare faint laser pulses at the four necessary polarizations ($H, V, +45°, -45°$), with three possible intensities each ($\mu_V = 0, \mu_S, \mu_D$). The intensity classes, called vacuum, signal and decoy states, are essential for the decoy state protocol extension of BB84. In principle this could be realized in different ways. For instance, one could use one laser, switch the attenuation and rotate the polarization from pulse to pulse. On a different approach, we are using eight laser diodes, one set oriented at the four polarizations driven with intensity μ_S and another set driven at μ_D. For vacuum pulses, no diode is activated. This method is (at least at first glance) technically easier to set up, while there are some disadvantages,

[1] Results of our free space QKD system partly related to this chapter have been presented in SECOQC and QAP project reports as well as in [29, 41, 42].

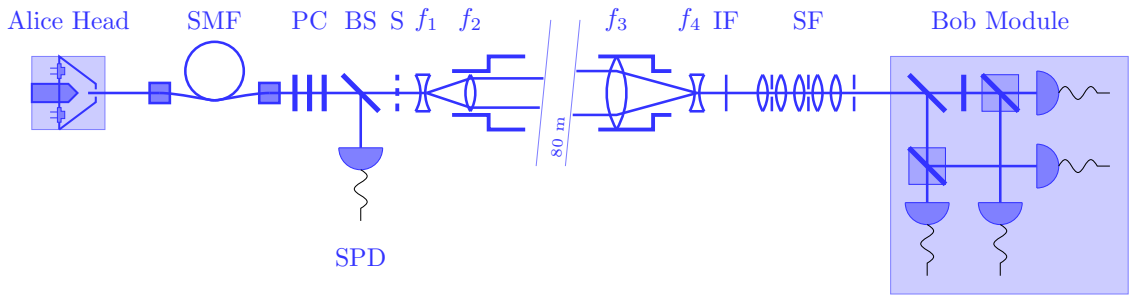

Figure 4.1: Schematic drawing of our free space QKD system as used in the SECOQC demonstration at Vienna in Autumn of 2008. In the Alice head, the beams from 8 laser diodes are combined into a piece of single mode fiber (SMF) for spatial mode filtering. The polarization controller (PC) is there to undo the polarization rotation introduced by the fiber. A non-polarizing beam splitter (BS) reflects a fraction of the beams onto a single photon detector (SPD) for mean photon number calibration. The transmitted part of the beam passes Alice's telescope (lenses f_1 and f_2). After free space propagation of 80 m, the beam is picked up by Bob's telescope (f_3 and f_4) and has to pass a spectral (IF) and spatial filter (SF) before being measured by the single photon polarization analyzer (Bob Module).

too. The major drawbacks originate from the fact that the pulses from the two sets of laser diodes should ideally only differ in polarization. The resulting security implications will be discussed in chapter 5.

The beams of the eight laser diodes (wavelength $\lambda = 850$ nm) are combined by some specially shaped mirrors into a spatial filter (SMF, see Fig. 4.1). In this case, we used a short piece of single mode optical fiber that was temperature stabilized so that the main source for stress induced birefringence changes was eliminated. At the output of the fiber, a polarization controller was mounted to undo the polarization rotation introduced by the fiber. After that the beam passed a non-polarizing beam splitter (BS), where a part of the beam was reflected into a single photon detector (SPD) for monitoring and control of the mean photon numbers per pulse. In the transmitted arm there was a shutter (S) next, which could be closed while the mean photon numbers were calibrated, in order to prevent stray light from hitting the SPD. Finally two lenses with $f_1 = -15$ mm and $f_2 = 50$ mm formed a telescope to direct the light towards Bob.

4.2 Receiver Optics

The receiver's telescope constituted an $f_3 = 310$ mm and an $f_4 = -15$ mm lens to collimate the incoming beam, which then had to pass through a spatial filter that was formed by two $f = 30$ mm lenses with a $d = 150$ μm pinhole in between. The beam was then focused by an $f = 150$ mm lens into the Bob module, after undergoing spectral filtering by an interference filter (IF) of width 3 nm (FWHM). By narrowing the spectral transmission and the field of view to less than 200 μrad the system got close to being operational during daylight. Another important ingredient towards this goal was to shield off as much stray light as possible. The surface of Alice's box facing towards Bob was painted black and a black tube was used around Alice's telescope to suppress stray light hitting her exit lens.

4.3 Support Electronics

The 8 laser diodes in the Alice head were controlled by a custom made short pulse (FWHM < 1 ns) laser diode driver, connected to a PC through a PCI interface. The PC used prepared files from a quantum random number generator (QRNG) to determine basis, bit value and the pulse class (signal, decoy or empty).
At the receiver, when a photon hit one of the SPDs of the Bob module, it delivered a NIM signal that was fed into a home-made timetagging unit. This recorded the time of arrival of the detection events and which detector they appeared in and handed this over to a PC.
In order to be able to adjust the pointing direction of Alice's and Bob's telescopes, both optics parts were mounted on tip-tilt stages, equipped with stepper motors which were controlled by the two PCs.

4.4 Software

4.4.1 Synchronization

Since Alice and Bob only had their simple local and uncorrelated clock generators the synchronization of the transmission/ detection events was implemented in software. Bob basically used the arrival time of the detection events to find and maintain the 10 MHz repetition rate of the transmitter. A (software gating) time window of 3 ns (total width) was applied around the expected signal detection events, in order to filter background events with an attenuation of more than 15 dB. Thus the contribution of background events (especially during the day) on the QBER was reduced substantially.
Furthermore, this process assigned a pulse number to each detection event inside the time window. Due to the potentially different starting times of Alice and Bob (these

time differences were not known a priori), there was an offset between their pulse number assignments. To find this offset, pseudorandom sequences were introduced in the photon stream (encoded in the intensity rather than polarization). By analysing these, Bob was able to infer the start time difference within a period of some 100 ms. NTP synchronization of the PC clocks was sufficient to determine this remaining parameter. Further information can be found in [41, 42].

4.4.2 Sifting, Error Correction and Privacy Amplification

After successful synchronization, Alice and Bob have agreed on a common pulse number reference. Then, in the sifting process, Bob told Alice, in which pulse slots he has detected photons. Alice removed the other entries from her list and both discarded the cases where they had chosen different bases. The resulting sifted keys were supposed to be equal on both sides, except for some (quantum) bit errors. These could result from imperfections of the setup or from the presence of an eavesdropper. To be on the safe side, they were attributed to a potential eavesdropper.
For error correction, Alice and Bob used the Cascade protocol [3] with a slight modification: In order to make the communication more efficient, the process was applied to several parts of the key in parallel (otherwise there is only one bit transferred over the network, whith a giant protocol overhead). At the end of a protocol run, Alice and Bob shared the same key (with very high probability) and they have calculated the QBER and the amount of information on the key that has been made public during error correction. All this was handed over to the privacy amplification process.
The privacy amplification process [4, 5] calculated the amount of information, a potential eavesdropper could have gained from the values listed above. With a decoy state protocol extension, more values (like the different mean photon numbers and the corresponding detection probabilities) have to be included in this calculation. The error corrected key then was shrunk by the calculated value using Toeplitz matrices as universal hash functions [6, 7].

4.4.3 Authentication

It is important to note that without proper authentication, QKD systems are susceptible to man-in-the-middle attacks. Hence, a pre-shared secret between QKD link partners is vital as a necessary requirement for authentication.
In the SEOCQC network demonstration (see Chapter 3), authentication of the communication (all messages sent during operation (pointing, sifting, error correction and privacy amplification)) was provided by the node modules. For standalone operation, our QKD system is provided with its own authentication module. Different methods can be used, but for QKD unconditionally secure authentication introduced by Wegman and Carter [7] is usually preferred. In short, it works like this: Each

message is run through a universal hash function [6] that is known only by the two legitimate parties (it hence serves as a pre-shared secret). The output of the hash function (some tens of bits) is encrypted with a one-time-pad and sent to the other party as an authentication tag. The receiver checks the tag by performing the same procedure and comparing the result. Since each authentication process needs fresh key, our system does not authenticate each message individually, but rather all the messages belonging to a part of the final key. For many hash functions it is even possible to take advantage of this technique without having to save the complete messages. Rather they can be fed into the hash function along the way, so that the memory requirements are hardly increased.

4.4.4 Automatic Telescope Alignment

The setups are usually subjected to substantial temperature changes. These have a strong influence on the pointing direction and thus on the alignment and coupling efficiency between Alice's and Bob's telescope. This results in a dramatic decrease of signal count rate after a few hours. As a countermeasure we have mounted the telescopes on tip-tilt stages equipped with stepper motors. A piece of software runs on Bob's PC that only uses the current signal count rate as input to control the alignment. The algorithm uses a method similar to the lock-in technique, in order to maximize the signal counting rate by applying small changes to the pointing direction of both telescopes and by evaluation of the corresponding count rates. Like the lock-in technique, it is insensitive to fluctuations at comparatively high frequencies. The control bandwidth is on the order of some tens of mHz, since we only want to compensate for slow thermal drifts. More information is available from [41, 42].

4.4.5 Decoy State Protocol Extension

The system is designed to use a decoy state extension [40] to the original BB84 protocol in order for it to become more robust against photon number splitting (PNS) attacks.
Unfortunately, during the setup period of the SECOQC trial, we noticed that the different mean photon numbers per pulse ($\mu_s = 0.3, \mu_d = 0.35$) were not sufficiently stable for running the decoy state protocol. We therefore were forced to work without decoy states, so that we do not claim that the experiment was robust against PNS attacks.

4.4.6 Location

Our setup was installed as the link between the nodes FOR and ERD (see Fig. 3.3) at the SECOQC network demonstration in Autumn of 2008. The public demonstration

Figure 4.2: Images of the site where our QKD link was installed in Vienna. Left: The bird's eye view on the positions of transmitter and receiver. Right: View from Alice to Bob with an alignment laser switched on.

took place at Siemens Forum (FOR), so that our link bridged the last mile (in fact a little less) to the closest fiber node. Alice and Bob were placed on two buildings with a distance of about 80 m between transmitter and receiver. While this is not a lot, it shows one of the possible use cases of free space QKD systems, the secure connection of different buildings in rather close proximity.

4.4.7 Results

During the preparation for the SECOQC demonstration event, the system was continuously adapted to make it daylight operable. The last enhancements were painting the front of the transmitter box black (see Fig. 4.3) and shading the external lens of the transmitter telescope by a 25 cm long black tube.
The field of view of the receiver was measured by scanning its pointing direction over a small light bulb that was inserted into the transmitter box and also used for coarse alignment of both telescopes. Figure 4.4 shows the result, the acceptance angle was smaller than 0.01 arcsec, corresponding to an area at the transmitter of less than 15 mm in diameter.
With those modifications the system was running during September and October 2008, occasionally interrupted by service or bad weather (e.g. dense fog) periods. The data shown in Fig. 4.5, were taken during a cloudless day in late September over a time span of a bit less than 36 hours. The raw count rate varied from roughly 100 kHz at night (during rather poor transmission conditions because of high humidity) to almost 300 kHz during the day. We measured a peak background count rate after spatial and spectral filtering of around 100 kHz during bright daylight, which was still in a reasonable range in order not to saturate the detectors including the signal rate. After applying a 3 ns timewindow (at a repetition rate of 10 MHz), the background rate contributed about 1 % to the QBER.

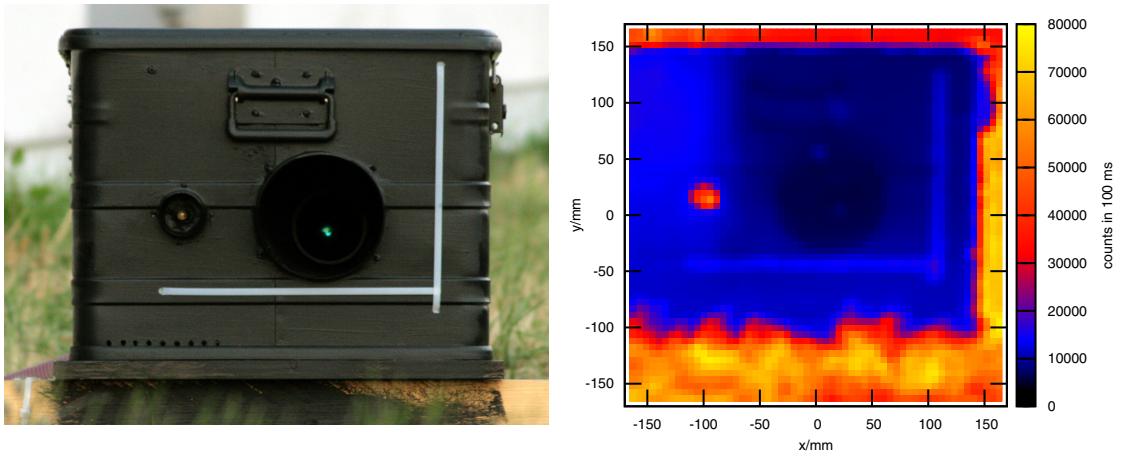

Figure 4.3: The left part shows a photograph of the box that contained the transmitter. The front surface was painted black and the telescope front lens was shaded of by a 25 cm long black tube so that as little light as possible was reflected from the important area towards the receiver. On the right there is a scan of the detector over roughly the same area that is shown in the left image, yet here the number of detection events of the receiver module are shown. One can also see the light from the small light bulb left of the transmitter telescope that was used as an alignment help.

Even with a rather strongly fluctuating signal rate, the sifted key rate stayed more or less constant at an average of about 40 kbit/s. This was mainly due to a limitation of our communication software, which was resolved only after the trial, unfortunately. The sifted key contained bit errors between 2 % and 3 %, the average was 2.3 %. After the correction, a final key was distilled with an average rate of approximately 14 kbit/s (over this period).
It should be mentioned again that due to stability problems with the electronics, we could not run the decoy state protocol and hence the QKD run can't be claimed to have been secure against PNS attacks. Additional information about the performance of the system can be found in [29].

Time Span	Counting Rate	Sifted Key Rate	Secure Key Rate	QBER
> 24 h	100 .. 300 kHz	40 kbit/s (av.)	14 kbit/s (av.)	2.3 % (av.)

Table 4.1: Results of the measurement run from September 26th till September 27th, 2008, of our free space QKD system at the SECOQC demonstration experiment. Data were taken on a sunny day and the following night.

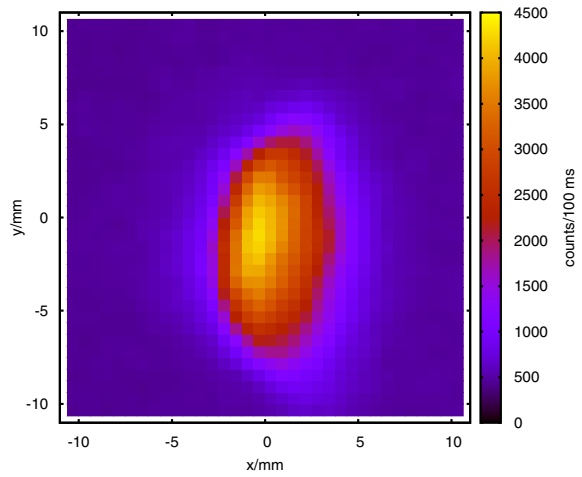

Figure 4.4: A scan of the receiver pointing direction over a small light bulb close to the transmitter telescope to determine the field of view. The area from which photons are accepted by the detectors is less than 15×10 mm^2.

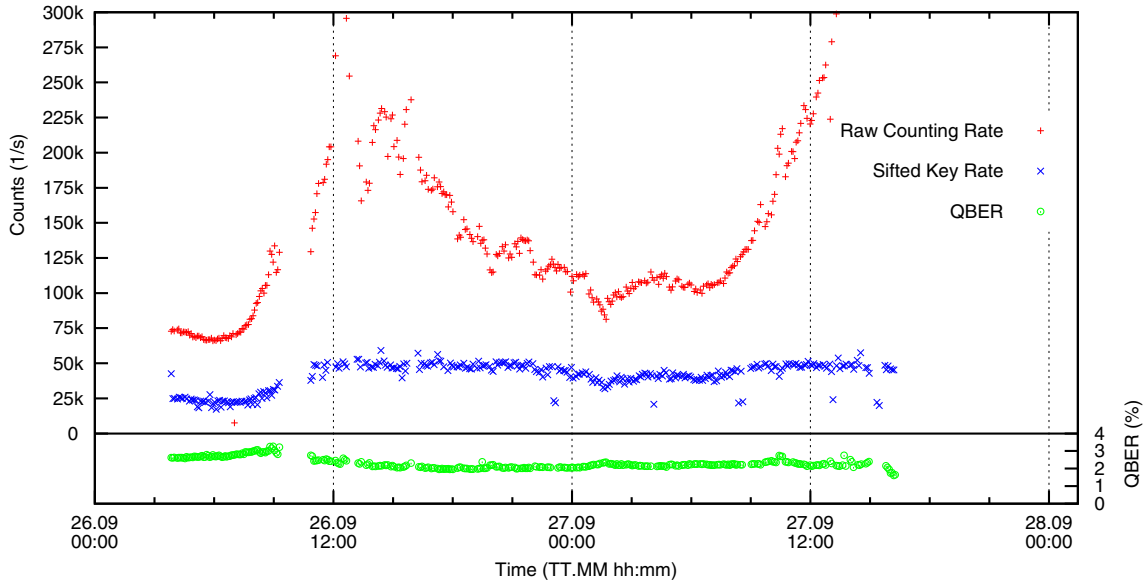

Figure 4.5: Results of a free space QKD run lasting about 36 hours altogether. The system recalibrated itself every 15 minutes, during those periods no key was produced. One can observe a significant increase in raw count rate during the day, but the sifted key rate is not so much affected, neither is the QBER. This is mainly due to very rigid temporal, spatial and spectral filtering.

5 Security Analysis of our Free Space QKD System

Contents

In order to take a systematic approach at a security analysis of our system, here I've tried to work along the so-called Common Criteria (CC) [43–45][1]. They have been developed as an international standard for certification of security related information technology systems. I have tried to omit some formally necessary, but in my opinion negligible parts of the CC, e.g. the so-called "security objectives". I want to state clearly that the present work is not meant as a formal security target (ST), intended for evaluation in a certification process. Instead, it is a first attempt to systematically collect potentially security relevant properties of our system. Some of these properties will be applicable to other systems, while others may not. The following lists are not claimed to be exhaustive, but to my knowledge they cover the known problems and solutions.
Even if I do not use the complete formalism, I will mainly stick to the language of the CC. For example, I will call our QKD system "target of evaluation (TOE)".
The structure of an ST can be briefly described as follows: It usually starts with an introduction that includes formalities like a unique ST identification and conformance claims with so-called protection profiles (PPs), which describe classes of systems rather than a single one. This introduction is formally followed by the TOE description, that has been omitted here since it is covered by chapter 4. The part called "TOE Security Environment" is composed of a list of assumptions (5.1) – e.g. that nobody has physical access to the TOE –, some elaboration of the possible threats (5.2) and the so-called organisational security policiess (OSPs). The next section in formal STs is called "Security Objectives", describing what the TOE should provide security against. They have been omitted here, because each Security Objective would just have negated a threat that was listed before. The following part called "Security Functional Requirements (SFR)" deals with the security functions that are implemented to achieve the Security Objectives. In the present work the SFR answer directly to the threats.

5.1 Assumptions

The security analysis of the TOE is based on the following assumptions:

5.1.1 Quantum Mechanics: A.01

The basic postulates of standard quantum mechanics (e.g. [46]) are assumed to be correct. They imply fundamental principles like the no-cloning-theorem or the indistinguishability of non-orthogonal states, thus leading to the provable security of quantum key distribution (in connection with an authentic classical channel).

[1] Chapter 5 and 6 represent the outcome of a continued effort that started as a project called "SiAnQCS" with the German Bundesamt für Sicherheit in der Informationstechnik (BSI). Some of the results shown here were presented in the corresponding project reports.

5.1.2 Protected Area: A.02

It is assumed that the TOE is used inside a secured area. The adversary may have physical access to the classical and quantum channel outside the secured area. This means that there exists a restricted area, inside which the adversary is not capable of placing massive objects like sensors of any sort. It includes the impossibility of tempering with the power supply of the TOE.

5.1.3 OS/ Third Party Software Security: A.03

Within the scope of this document it will have to be assumed that the used third party programs like operating system and SSL implementation are secure. It is attempted to keep the use of third party software as limited as possible. In future versions of the TOE a lot of tasks that are performed by third party software now will be integrated in dedicated hard-/ software.

5.1.4 Independence of Side Channels: A.04

In the analysis of side channels, it will be assumed that the different side channels are independent of each other[2].

5.1.5 Neglection of Collective and Coherent Attacks: A.05

Within the scope of this document, it will be assumed that only individual attacks are performed, i.e. attacks on single qubits only[3].

5.2 Threats

5.2.1 Assets

The main goal of the TOE is the secure generation of symmetrical secret keys between the two parties that are connected via the TOE. The keys are required to be safely usable for any cryptographic method, including encryption of redundant information[4].

[2]The advantage of this assumption is that each side channel can be tackled separately, while otherwise they would have to be evaluated as a whole. It is possible that some side channels are correlated and the eavesdropper might be able to gain more information by using those correlations.

[3]Since collective and coherent attacks are usually even more difficult to perform than individual attacks, most of the theoretically proposed eavesdropping attacks on the quantum channel are individual attacks, this is especially true for implementation specific attacks.

[4]Redundant plain text can help the eavesdropper gather information about the key when the latter is reused.

5.2.2 Threat Agents

- A possible adversary (with substantial expertise, standard equipment for the classical channel and extraordinary expertise and equipment that is already available today or may be available within the time the TOE may be used (e.g. the next 10 years) [5]) to listen on the classical channel and actively eavesdrop on the physical quantum channel.

- Different threats could arise from a hacker (with substantial expertise, standard equipment), trying to compromise the system by attacking the classical channel.

- The malfunction of some parts of the system might lead to a corruption of the integrity of the key generation process.

5.2.3 Direct Attacks on Ideal Quantum Channel: TQ.01

Attacks on the ideal quantum channel[6] are those that can be carried out theoretically against the ideal quantum key distribution protocol BB84 [2]. It is usually assumed that a possible adversary may use every measure that is allowed by quantum mechanics, even if there is no known technology today that can accomplish this. These attacks do not use implementation specific weaknesses like the side channels that are reported on in the next section. These attacks usually employ some interaction between the single photons that are used for the quantum channel and a probe that is controlled by the eavesdropper. Many different attacks have been proposed, e.g. there is an optimal so-called individual attack [47]. There exist security proofs for the BB84 protocol even against the most general attacks possible [13].

5.2.4 Side Channel Attacks on Quantum Channel

Apart from attacks on the ideal quantum channel, there are some that tackle the specific physical implementation. The following possible threats to the realisation

[5] Many attacks on the quantum channel require so-called *quantum non demolition measurements* and/or quantum memory with properties that have not been shown in experiments, yet.

[6] We define an ideal quantum channel as a perfect source and a perfect detector. The source prepares exactly the state $|\psi\rangle \in \{|\phi_0\rangle = |H\rangle, |\phi_1\rangle = |V\rangle, |\phi_2\rangle = |+\rangle, |\phi_3\rangle = |-\rangle\}$ it wants to transmit. These states differ only in the polarisation degree of freedom, all other degrees of freedom are the same for all states. The detector analyses the polarisation by applying one of the two sets of measurement operators $\{M_0 = |\phi_0\rangle\langle\phi_0|, M_1 = |\phi_1\rangle\langle\phi_1|\}$ (H/V basis) or $\{M_2 = |\phi_2\rangle\langle\phi_2|, M_3 = |\phi_3\rangle\langle\phi_3|\}$ (+/− basis). The probability of an occurence of measurement outcome i provided an input state $|\phi_j\rangle$ is $p_{ij} = |\langle\phi_i|\phi_j\rangle|^2$. The adversary may, however, do whatever is allowed by quantum mechanics to identify or change the transmitted quantum state.

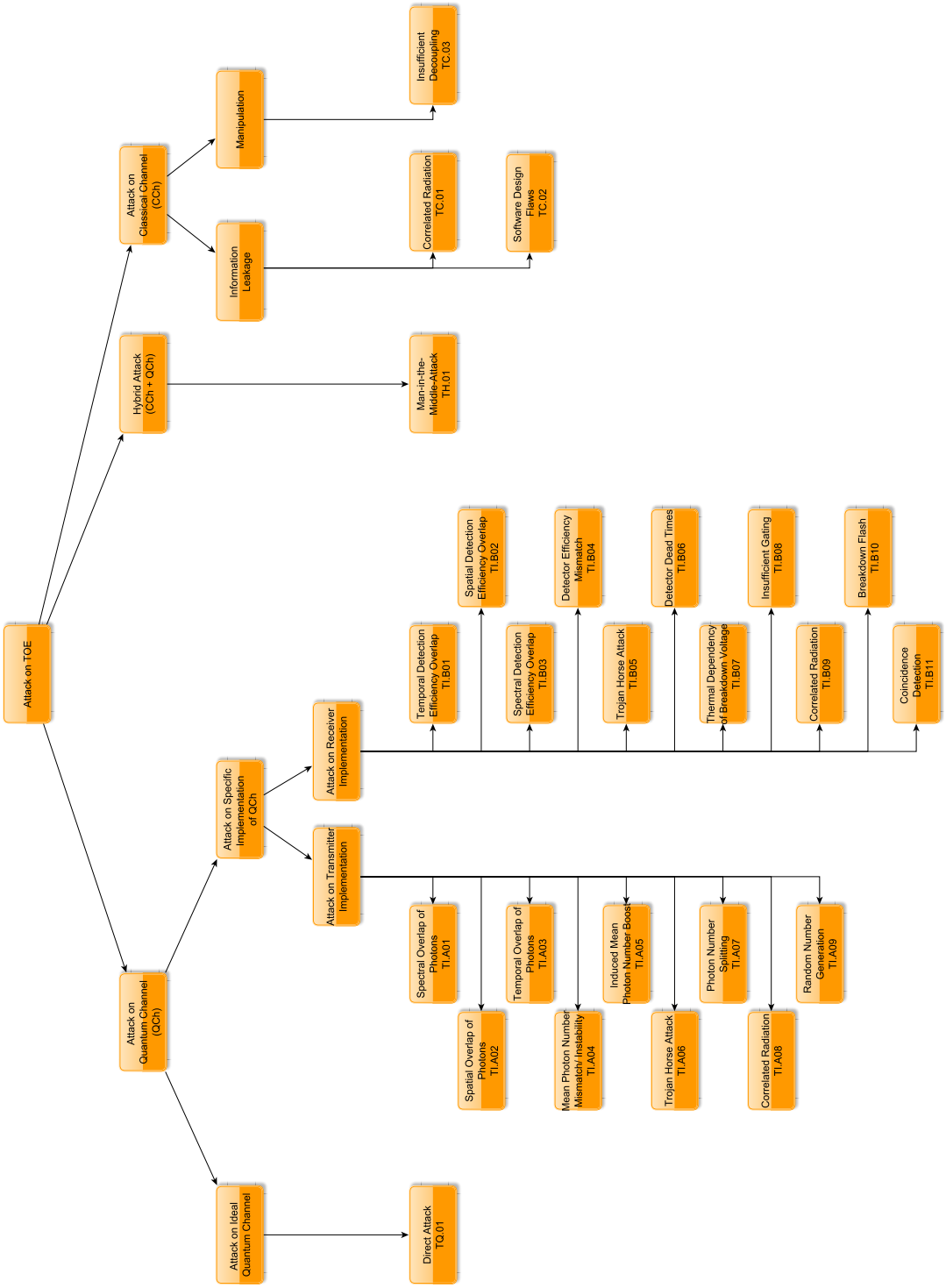

Figure 5.1: Attack tree

used in this specific TOE have been identified. There are also security proofs taking into account several experimental imperfections of QKD systems [8, 14]. This class of attacks is divided into those resulting from a non-ideal implementation of the transmitter and the receiver respectively.

5.2.4.1 Attacks due to imperfections on Transmitter side

The first class of attacks is enabled by possible shortcomings in the design/ realization of the transmitter module.

TI.A01: Spectral Overlap of Transmitted Photons There are eight laser diodes in the transmitter module (so-called Alice Module). They should differ only in the polarisation of the photons they emit, the spectra should be indistinguishable. If this is not the case, an eavesdropper might gain information about the polarisation of a photon by measuring the wavelength of it. The measurement would have to be non-destructive concerning the polarisation state, which is at least theoretically possible. Such an attack would not be noticed by the legitimate communication partners and has hence to be considered in this class of threats.

TI.A02: Spatial Overlap of Transmitted Photons Similar to the spectral overlap, the light emitted from all eight laser diodes has to be combined into one single optical mode. If this is not done, an adversary can gain information about the polarisation of a photon by measuring its lateral position. The measurement would also have to be non-destructive concerning the polarisation state.

TI.A03: Temporal Overlap of Transmitted Photons Similar to spectral and spatial overlap, the light pulses emitted from all eight laser diodes have to be indistinguishable with regard to temporal distribution. Otherwise, an eavesdropper might gain some information about the polarisation of a photon by measuring its time of arrival. The measurement would also have to be non-destructive concerning the polarisation state.

TI.A04: Mean Photon Number Mismatch or Instability Similar to the attacks mentioned before, the light pulses emitted from the two sets of four laser diodes each have to be indistinguishable with respect to the average number of photons contained in them. If this was not the case, information might leak to a non-authorised party. Furthermore, these parameters have to stay constant and their absolute value has to be in accordance with the applied theory (for privacy amplification).

TI.A05: Induced Mean Photon Number Boost or Mismatch An adversary may try to shift the threshold of the laser diodes by shining in light from the outside.

This could effectively induce a mean photon number mismatch or increase the mean photon number of all laser diodes, which would - if it remained unnoticed - pose a significant security threat.

TI.A06: Trojan Horse Attack Transmitter The adversary could try to shine light into the transmitter unit to infer information about the state of the system. Since there are no actively switched optical elements in the TOE, this attack is not quite straight forward. Still, there may be ways of reading out which of the laser diodes is activated.

TI.A07: Photon Number Splitting In the ideal protocol, a single photon source is used to make sure that every time slot contains one photon at maximum. The TOE uses laser pulses strongly attenuated to the single photon level. Because the number of photons within the pulses is distributed according to the Poisson statistics, there is a non-vanishing possibility that a pulse contains more than one photon. By performing a so-called photon number splitting (PNS) attack, an adversary could gain information about those photons without disturbing the qubit that is used for key generation.

TI.A08: Correlated Radiation The TOE could emit electromagnetic radiation into the environment or onto supply or communication lines that might be used by an eavesdropper to gain information about the polarization of the photons or about the key itself. The secured area has to be defined bigger than the area in which such attacks would be possible.

TI.A09: Random Number Generation The transmitter part of the TOE contains a random number generator that determines which of the eight laser diodes fires. If an adversary could gain knowledge about the bit stream produced by the random number generator, he or she would be able to predict the photons' polarization and hence get information about the key.

5.2.4.2 Attacks due to imperfections on Receiver side

TI.B01: Temporal Detection Efficiency Overlap The receiver module of the TOE contains four separate single photon detectors. The delay between the arrival time of a photon at the input of the module and the rising edge of the electronic signal that is produced, can vary from one detector to the next. When a global time window is applied in order to discriminate signal from background events, this leads to an effective difference of the detection efficiency for different detectors at different times [48, 49] with two implications:

- Passive: Depending on the arrival time of a signal photon, an eavesdropper could determine (with some probability), which of the detectors is more likely to register an event. This would not cause any errors. A similar attack has been shown in [50], where the detection times were transmitted over the classical channel for synchronization.

- Active: An attacker could use this to control the receiver module. He could shine in light at a certain time to increase the probability that a distinct detector registers the event [16, 51]. If Eve can do that perfectly (i.e. there are distinct time intervals when only one detector registers the event, one for each detector), she can completely predetermine the outcome of Bob's measurement, e.g. by doing an intercept-resend attack and hence produce no error at all [52].

TI.B02: Spatial Detection Efficiency Overlap Like in the transmitter module, the spatial modes defined by the APDs and the rest of the receiver's optics system might not overlap completely. This results in two different possible problems:

- Efficiency mismatch: Obviously, there might be different effective efficiencies for different spatial modes of the signal beam. These might even change in time if the transmitter mode (modeled as one single spatial mode now) to the different receiver modes' coupling efficiency is not constant.

- Further degree of freedom for a pre-pulse attack as explained in TI.B06 only instead of using a bright light pulse with a certain polarisation, Eve could use a bright pulse shining in with a special spatial mode. In this way, she might be able to manipulate the efficiency of individual single photon detectors, rather than attacking at least three detectors at a theoretically fixed ratio.

TI.B03: Spectral Detection Efficiency Overlap This liability is equivalent to TI.B01 and TI.B02, with the distinction that the degree of freedom is spectral efficiencies instead of spatial or temporal efficiency differences.

TI.B04: Detector Efficiency Mismatch There may be a general difference between the efficiencies of the four detectors, but this can be covered in the same way the previous paragraphs are handled.

TI.B05: Trojan Horse Attack Receiver The attacker could try to shine rather bright light into the receiver unit and analyse its reflected parts to gain information about the current internal state of the receiver. This attack is not applicable to this TOE. There are no actively switched optical devices inside the receiver that could be utilized for such an attack.

TI.B06a: Detector Dead Times I This attack is covered in more detail in Chapter 7. I want to summarize it briefly here:
After a state-of-the-art (ungated) single photon detector has registered a photon, it needs some time to recover until it can detect the next one. This so-called dead time can already be used passively to gain some knowledge about the key without introducing additional errors [53]. Additionally, this effect can be employed to attack the system actively: When a sufficiently bright pulse (still on the single-photon level) of light of one polarisation (e.g. horizontal) is coupled into the detector just before the time window of a signal pulse, the chance can be made arbitrarily high that if a photon was detected (which can be found out by Eve during the sifting process), it was of the orthogonal polarisation (here: vertical). Theoretically, if no countermeasures are taken, this can lead to Eve's full information about the key, without her introducing any additional errors. Even worse: This attack is **feasible with todays technology** without a lot of effort. It is probably the most effective attack that can be launched against the TOE.
The impact of this attack is even increased since the effective dead time of the detectors (at least of this specific implementation of the TOE) is not constant, but depends on the counting rate. The reason for this is that if a photon hits the detector shortly after a previous one has been registered, the APD will be still in the charging process and the resulting electronic pulse will be rather low. If it is too low to be detected by the discriminator, no pulse will be recorded by the system, but still the charging process of the APD will start newly, whence the effective dead time is prolonged. The higher the count rate, the higher the probability that such an event occurs. In fact, using this effect, Eve can more or less selectively tune the efficiency of the single photon detectors. Because of this effect, it is also not possible to simply use the countermeasure proposed in [53], which is suppressing the other detector's pulses by software during the attributed dead time of one detector. This dead time is not a fixed time span, but can be adjusted by Eve actively.

TI.B06b: Detector Dead Times II A different attack with similar results was introduced in [54–56]. It uses a somewhat reciprocal idea of the previously explained, always blinding the single photon detectors with bright enough light and only letting one of them recover from time to time or even increasing the light intensity to produce a signal pulse in the linear APD mode. A click during this active time means that it has to have happened in the one detector that Eve did not blind during that time.

TI.B07: Thermal Dependency of Breakdown Voltage Instead of using the dead time to blind detectors, it is also possible to illuminate them very strongly (for a short period of time) and thus heat them. Since the breakdown voltage of the APD increases with increasing temperature, one can decrease the APD's efficiency this

way. This effect can be used to launch similar attacks like TI.B06a and TI.B06b with hardware gated detectors [57]. As we don't employ hardware gating in our setup, this will have the same effect as the aforementioned ones.

TI.B08: Insufficient Gating Some QKD systems use hardware gating in the sense that they increase the bias voltage of the APD over the breakdown threshold only around the time a signal photon is expected. Still, if they are illuminated by bright enough light, they output a pulse even during the time they should be switched off. This can be used for an efficient intercept-resend attack [58, 59]. Since no hardware gating occurs in our setup, this attack cannot be conducted with our system.

TI.B09: Correlated Radiation The TOE could emit electromagnetic radiation into the environment or onto supply or communication lines that might be used by an eavesdropper to gain information about the polarization of the photons or about the key itself.

TI.B10: Breakdown Flash The devices used for single photon detection in the TOE (APDs) are known to emit a so-called breakdown flash whenever they detect a photon [60]. An adversary could try to detect and analyze the polarization of the breakdown flash and thus gain information about the measurement result of the TOE. This is a special case of correlated radiation.

TI.B11: Coincidence Detection When two (different) detectors produce an event within one time window (applied by software), we call this a coincidence detection. The original BB84 protocol has not considered this possibility. Since it is impossible for Alice and Bob to gain information from such events, one obvious solution is to discard them. Unfortunately, this opens a quite big door for an eavesdropper [8, 14]. Eve could use comparatively bright pulses of a certain polarization (e.g. horizontal, in reality she would probably switch them more or less randomly) and send her pulse into the system together with the pulse from the transmitter. In case her pulse has the same polarization as Bob's pulse, only one detector will produce an event. If Eve uses sufficiently bright pulses, all other cases will result in coincidences between at least two detectors and hence be discarded. Eve will gain (asymptotically) full knowledge about the key without introducing errors.

TI.S01: Finite Key Length The keys produced by real QKD devices are necessarily of finite length. The original protocols neglect this fact which can be exploited by an eavesdropper.

5.2.5 Attacks on Classical Channel

Ideally, there is no attack on the classical channel alone (for an attack on both channels see next section) apart from a DOS attack. In reality, this may not be the case.

5.2.5.1 Information Leakage

There could be two possible ways the system could leak information via the classical channel:

TC.01: Correlated Radiation As in the quantum channel part there might be an information leakage by correlated radiation being emitted from the physical parts of the classical channel.

TC.02: Software Design Flaws The software of the TOE that communicates over the classical channel could give out secret information over this channel.

5.2.5.2 Manipulation

TC.03: Insufficient Decoupling If the quantum channel is not sufficiently decoupled from the classical part, an adversary could try to manipulate the quantum channel by tampering with the classical channel. She could, e.g. try to change the voltage levels of the classical channel in order to possibly change some voltage levels of the quantum part.

5.2.6 Hybrid Attacks

TH.01: Man-in-the-middle-attack As long as the classical channel is not authenticated, the TOE may be subject to a Man-in-the-middle attack. In this scenario, the eavesdropper is located between the two legitimate parties in the quantum channel as well as in the classical channel. She impersonates Bob towards Alice and Alice towards Bob. In fact she can exchange a key with Alice and Bob and de- and encrypt their whole communication afterwards. The eavesdropper will have complete knowledge about the key, hence authentication of the classical channel is highly important.

5.2.7 Summary

Threat	Description
TQ.01	Direct Attacks on Ideal Quantum Channel
TI.A01	Spectral Overlap of Transmitted Photons
TI.A02	Spatial Overlap of Transmitted Photons
TI.A03	Temporal Overlap of Transmitted Photons
TI.A04	Mean Photon Number Mismatch or Instability
TI.A05	Induced Mean Photon Number Boost or Mismatch
TI.A06	Trojan Horse Attack Transmitter
TI.A07	Photon Number Splitting
TI.A08	Correlated Radiation
TI.A09	Random Number Generation
TI.B01	Temporal Detection Efficiency Overlap
TI.B02	Spatial Detection Efficiency Overlap
TI.B03	Spectral Detection Efficiency Overlap
TI.B04	Detector Efficiency Mismatch
TI.B05	Trojan Horse Attack Receiver
TI.B06a	Detector Dead Times I
TI.B06b	Detector Dead Times II
TI.B07	Thermal Dependency of Breakdown Voltage
TI.B08	Insufficient Gating
TI.B09	Correlated Radiation
TI.B10	Breakdown Flash
TI.B11	Coincidence Detection
TI.S01	Finite Key Length
TC.01	Correlated Radiation
TC.02	Software Design Flaws
TC.03	Insufficient Decoupling
TH.01	Man-in-the-middle Attack

6 Security Functional Requirements (SFR)

Contents

6.1 Protection Against Direct Attacks on Ideal Quantum Channel: SFQ.01

In the ideal case an upper bound on Eve's information about the key (after sifting and error correction) can be calculated. By hashing the key to a smaller length, Eve's information on the final key can be reduced to fit the requirements of A.04. This method is called privacy amplification (PA) [4, 5]. The resulting key length ratio can be calculated using the following formula [8]:

$$R = \max(1 - 2H_2(\delta), 0) \tag{6.1}$$

With quantum bit error rate (QBER) δ and the binary entropy function $H_2(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$. Suitable hash functions can be found within the class of $universal_2$ hash functions [6].

6.2 Protection Against Side Channel Attacks on the Quantum Channel

In general, there are two basic strategies against these attacks: The most obvious is to try to eliminate the reason for the attack, improve the (non-ideal) implementation. This way one can usually reduce the effect significantly. After that, in case the eavesdropper is still able to gain information because of this effect, it would be sufficient to find an upper bound of information the eavesdropper can get with regard to the system specifications. If this is known, the key lengths can be further reduced during the PA process.
We have measured some of the TOE's properties and the results are mentioned where appropriate, although this would not be part of a CC document. It's important to note that the measurements will never be perfect and the resulting uncertainty may still allow the eavesdropper to gain more information than what was expected.

6.2.1 Spectral Overlap (TI.A01)

6.2.1.1 Spectral Selection of Laser Diodes: SFI.01

The laser diodes in the transmitter module are selected so that their spectral distribution overlaps maximally. This has been investigated in detail in [61].

6.2.1.2 Spectral Filtering: SFI.02*[1]

To reduce the information leakage to an eavesdropper further, spectral filtering can be applied to restrict the spectral distinguishability.

6.2.1.3 Privacy Amplification Against Spectral Distinguishability: SFI.03*

The resulting information that is accessible to an eavesdropper due to spectral distinguishability can be reduced to a necessary level by privacy amplification. As an estimation of the amount the mutual information between basis value $b \in B$ and measured wavelength $\lambda \in \Lambda$ can be calculated as follows:

$$H(B:\Lambda) = H(B) + H(\Lambda) - H(B,\Lambda) \tag{6.2}$$

with

$$H(\Lambda) = -\int p^{\lambda}(\lambda) \log_2 \left[p^{\lambda}(\lambda)\right] \mathrm{d}\lambda \tag{6.3}$$

$$H(X) = -\sum_b p^0(b) \log_2 \left[p^0(b)\right] \tag{6.4}$$

$$H(B,\Lambda) = -\sum_b \int p(b,\lambda) \log p(b,\lambda) \,\mathrm{d}\lambda \tag{6.5}$$

with $p^{\lambda}(\lambda) = \sum_b p^0(b) I_b(\lambda)$ and $I_b(\lambda)$ as the intensity of basis b at wavelength λ, $p^0(b)$ the probability of choosing a particular $b \in B$ and the conditional probability $p(b,\lambda)$ of finding a particular value of $b \in B$ when a particular $\lambda \in \Lambda$ was found.

6.2.1.4 Experimental Estimation

To estimate the amount of information given away from our setup, we used a home-built single-photon spectrometer to measure the Intensity distribution $I_b(\lambda)$ (see Fig. 6.1) and found that the resulting information gain for Eve was $H(B:\Lambda) < 7{\cdot}10^{-3}$ bit per pulse [61].[2]

6.2.2 Spatial Overlap (TI.A02)

6.2.2.1 Spatial Filtering: SFI.04

If multiple laser diodes are used for the different polarizations, spatial distinguishability can hardly be reached by alignment procedures, especially since the spatial profile of laser diodes depends strongly on the polarisation axis. Hence, spatial filtering will be inevitable. This can be done by guiding the emitted light through a series of pinholes or through a single mode optical fibre.

[1] An asterisk (*) means here, that this function has not been implemented in the current setup.

[2] Here it is assumed that the eavesdropper does not block any pulses. He could just let those photons reach the transmitter that allow him to infer as much as possible about the polarisation.

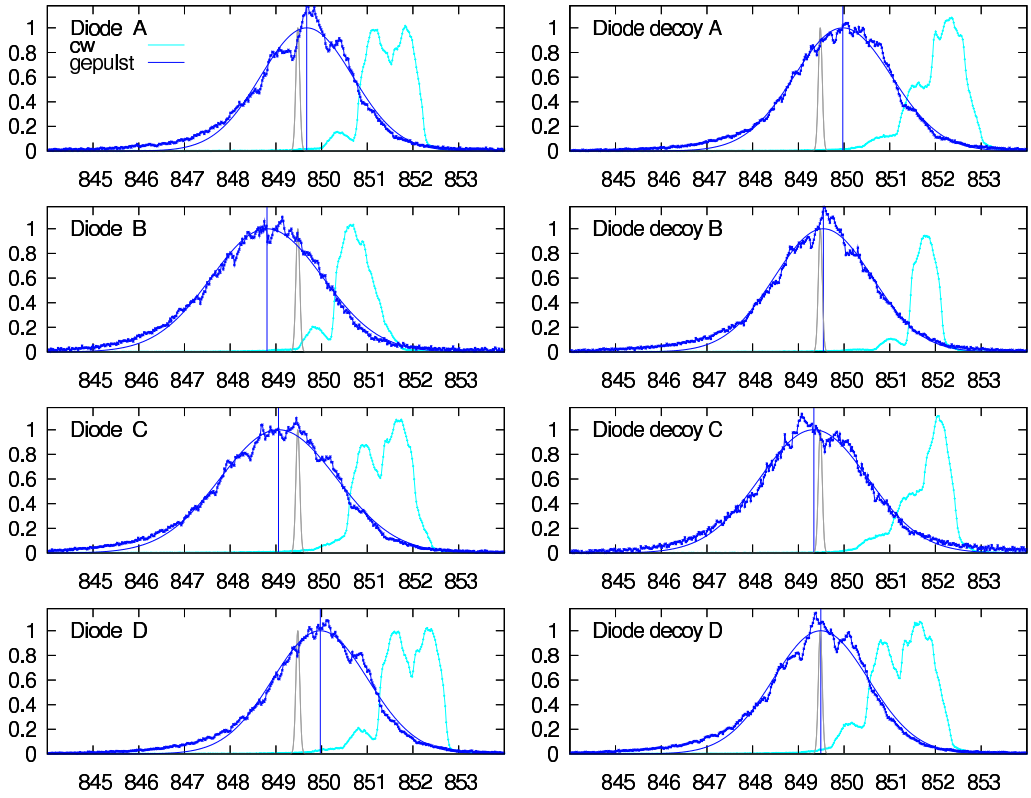

Figure 6.1: Experimental analysis of the spectra of the eight laser diodes used in the TOE each in cw and pulsed mode [61].

6.2.2.2 Privacy Amplification Against Spatial Distinguishability: SFI.05*

The resulting information that is accessible to an eavesdropper due to spatial distinguishability can be reduced to a necessary level by privacy amplification. The mutual information between basis value $b \in B$ and measured spatial position $x \in X$ can be calculated analogously to equation (6.2):

$$H(B:X) = H(B) + H(X) - H(B,X) \tag{6.6}$$

6.2.2.3 Experimental Estimation

Although the spatial profiles of multiple emitters should perfectly overlap behind a single mode optical fibre in theory, this may not be true in reality. Especially when the fibre is very short (in our case only 6 cm), this should be checked. Yet, we found no significant difference in the spatial profiles of the eight laser diodes behind the fibre above the noise level (Fig. 6.2). The calculated mutual information was on the

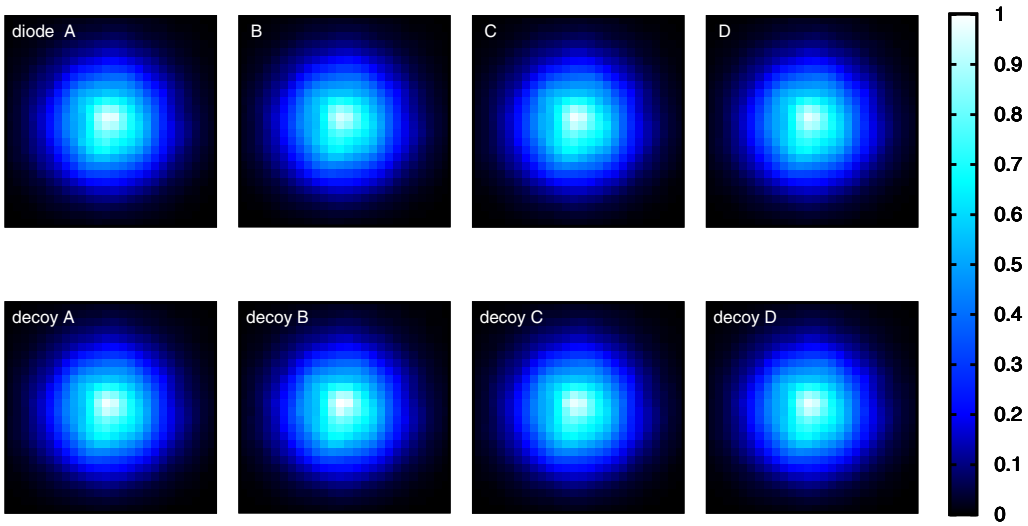

Figure 6.2: Experimental analysis of the spatial emission profiles of the eight laser diodes used in the TOE measured behind the 6 cm long single mode optical fibre. The beam was collimated and then scanned with an APD at a distance of 40 cm. The scanned area was 6.25 mm × 6.25 mm [61].

order of $H(B:X) \sim 10^{-5}$ bit per pulse [61].[3]

6.2.3 Temporal Overlap (TI.A03)

6.2.3.1 Temporal Alignment: SFI.06

The temporal profiles of the different laser diodes have to be overlapped maximally. This can usually be done by delaying the electronic pulses by a suitable amount.

6.2.3.2 Privacy Amplification Against Temporal Distinguishability: SFI.07*

The resulting information that is accessible to an eavesdropper due to temporal distinguishability can be reduced to a necessary level by privacy amplification. The mutual information between basis value $b \in B$ and measured time $t \in T$ can be calculated analogous to equation (6.2):

$$H(B:T) = H(B) + H(T) - H(B,T) \tag{6.7}$$

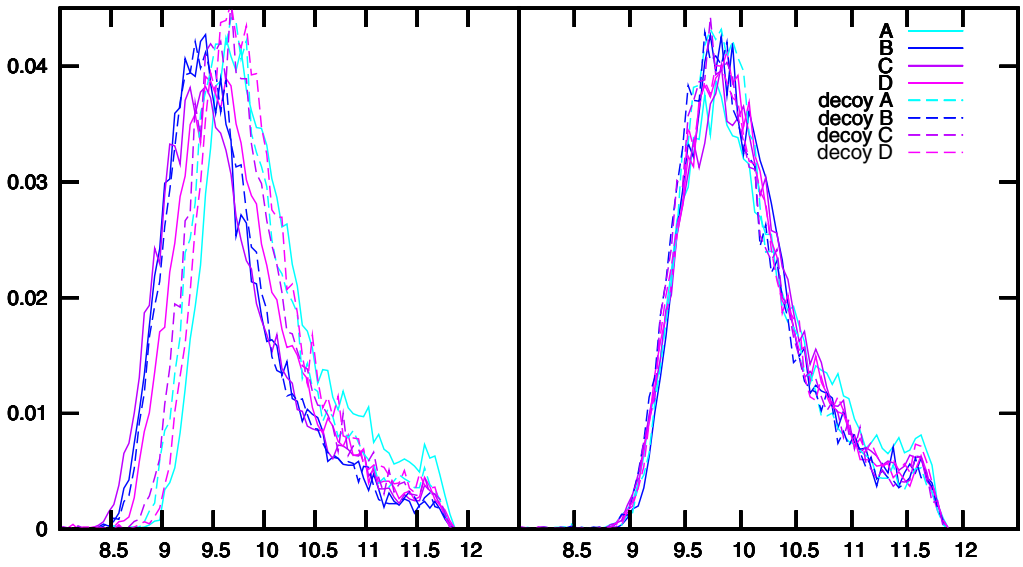

Figure 6.3: Experimental analysis of the emission times of the eight laser diodes used in the TOE before (left) and after (right) maximizing the temporal overlap [61].

6.2.3.3 Experimental Estimation

We measured the distributions of time differences between clock pulse and output pulse of a single APD for the eight laser diodes in the TOE with a fast oscilloscope. The results are shown in Fig. 6.3. After optimization of the overlap (right) by setting the digital delay lines for each laser diode, the resulting mutual information would have been $H(B:T) \leq 3.0 \cdot 10^{-3}$ bit per pulse [61].[4]

6.2.4 Mean Photon Number Mismatch (TI.A04)

6.2.4.1 Mean Photon Number Monitoring: SFI.08*[5]

In order to ensure that the different laser diodes are emitting the same mean number of photons per pulse, the output of the transmitter module is monitored by a calibrated internal APD within the transmitter. The pulse intensities should be

[3] Here it is assumed that the eavesdropper does not block any pulses. He could just let those photons reach the transmitter that allow him to infer as much as possible about the polarisation.

[4] Here it is assumed that the eavesdropper does not block any pulses. He could just let those photons reach the transmitter that allow him to infer as much as possible about the polarisation.

[5] At the moment, the TOE uses a periodic calibration (e.g. every 15 min) to avoid long-term drifts of the mean photon numbers and static mean photon number mismatches. This is not sufficient, though.

controlled in order to optimize the indistinguishability. Since it will have to be a statistical analysis, short-term fluctuations will have to be kept in mind (at least during PA).

6.2.4.2 Privacy Amplification According to Photon Number Mismatch: SFI.09*

The resulting information that is accessible to an eavesdropper due to a mean photon number mismatch can be reduced to a necessary level by PA.

6.2.5 Induced Mean Photon Number Boost or Mismatch (TI.A05)

6.2.5.1 Mean Photon Number Monitoring: SFI.08

See section 6.2.4.1.

6.2.5.2 Privacy Amplification According to Photon Number Mismatch: SFI.09*

See section 6.2.4.2.

6.2.5.3 Monitor Photo Diode: SFI.10*

In order to make sure that bright light cannot enter into the transmitter module unnoticed, one could employ a monitor photo diode to check for this.

6.2.6 Trojan Horse Attack (Transmitter, TI.A06)

6.2.6.1 Monitor Photo Diode: SFI.10*

See section 6.2.5.3.

6.2.7 Photon Number Splitting (TI.A07)

6.2.7.1 Mean Photon Number Optimization: SFI.11a*

In order to reduce the information that is accessible to an eavesdropper, the mean photon number μ can be optimized. Generally speaking, the optimal mean photon number μ_{opt} is on the order of the link transmission: $\mu_{opt} \sim \eta$. The problem with this approach is that the resulting key rate is then (at least over some range) proportional to η^2.

The resulting information that is accessible to an eavesdropper due to a photon number splitting attack can be reduced to a necessary level (shrinking ratio R) by privacy amplification:

$$R = \max\left((1-\Delta_{wcp}) - H_2(\delta) - (1-\Delta_{wcp})H_2\left(\frac{\delta}{1-\Delta_{wcp}}\right), 0\right) \tag{6.8}$$

(see [8]) with

$$\Delta_{wcp} = p_M/p_D = \frac{1}{2\eta}\left(\mu + O(\mu^2)\right). \tag{6.9}$$

p_M is the probability that a multiphoton pulse is emitted, p_D is the probability that an emitted photon is detected. Δ_{wcp} is the fraction of so-called *tagged* photons, i.e. photons that Eve can get full information about during a PNS attack without introducing errors.

6.2.7.2 Decoy State Extension: SFI.11b

In the formula above, without better knowledge, a worst case value for Δ_{wcp} has to be assumed. The so-called decoy state extension to the BB84 protocol [40, 62–64] has introduced a method of reducing the information of a potential eavesdropper, performing a PNS attack. It calculates an upper bound for $\Delta_{decoy} \leq \Delta_{wcp}$, with the result that the optimal μ_{decoy} is approximately independent of the link transmission and hence QKD can be securely used up to a lot longer distances than before [65,66]. Δ_{decoy} can be calculated when at least two different mean photon number μ, μ' are used by the transmitter randomly. Put simple, transmitter and receiver calculate the transmission values separately for each mean photon number and from that they can calculate Δ_{decoy}.
In this case Eqn. (6.8) has to be adpated to use Δ_{decoy} instead of Δ_{wcp}:

$$R = \max\left((1-\Delta_{decoy}) - H_2(\delta) - (1-\Delta_{decoy})H_2\left(\frac{\delta}{1-\Delta_{decoy}}\right), 0\right) \tag{6.10}$$

Δ_{decoy} is calculated according to

$$\Delta_{decoy} = \frac{\mu}{\mu'-\mu}\left(\frac{\mu e^{-\mu}Q'}{\mu' e^{-\mu'}Q} - 1\right) + \frac{\mu e^{-\mu}Q_0}{\mu' Q} \tag{6.11}$$

where Q, Q', Q_0 are measured detection probabilities of pulses with mean photon number $\mu, \mu', 0$, i.e. Q_0 is the background event detection probability.

6.2.8 Correlated Radiation (Transmitter, TI.A08)

6.2.8.1 Shielding SFI.12*

Like in classical cryptography systems, the transmitter module has to be shielded and decoupled from the environment so that it doesn't emit any electromagnetic radiation.

6.2.9 Random Number Generator (TI.A09)

6.2.9.1 Quantum Random Number Generator (QRNG): SFI.13*[6]

In order to close the loop-hole of in principle predictable pseudo-random numbers and hence predictable basis and bit value choices made by Alice, a true random number generator should be used, for example [67]. An obvious choice could be to employ a random number generator based on a quantum process (QRNG)[7]. If there is an imbalance between the number of 0s and 1s (a so-called bias), this can be treated analogously to the mismatch of mean photon numbers. Usually this bias can be made very small, though.

6.2.10 Temporal Detection Efficiency Mismatch (TI.B01)

6.2.10.1 Equalization of Path Lengths: SFI.14

The best possible (but probably never sufficient) way of treating this is to maximize the temporal overlap of all detector signals. That starts with the optical path lengths and stops at the digitization of the event times. If this is not done (and instead e.g. only the following step), there may be the risk that e.g. different optical path lengths could be used in connection with the breakdown flash to gain more information.

6.2.10.2 Hardware/ Software Delay: SFI.15

In the TOE, there is no hardware time window that determines whether a detection event is treated as background or signal. This is done in software here. So one can either add an electronic delay in the signal pulse paths or add some delays in software before the time window is applied (as it is done at present).

[6] At the moment, the TOE uses stored random numbers from a QRNG.

[7] A rather high flux of random numbers is necessary. For each pulse, an average value of 5 random bits is used, since not only basis and bit value have to be chosen, but also to which of the three pulse classes (decoy, signal, background) it belongs and they do not occur with the same probability.

6.2.10.3 Privacy Amplification: SFI.16*

Remaining differences in the temporal detection efficiency have to be taken into account during PA. This has been examined in [17, 48, 49] for systems with two detectors. To this end the corresponding properties of the TOE have to be known well.

6.2.11 Spatial Detection Efficiency Mismatch (TI.B02)

6.2.11.1 Maximization of Spatial Overlap: SFI.17

In order to maximize the spatial overlap of the APDs, it should be attempted to equalize the spatial efficiency distribution of the four detectors[8]. In the TOE this can be done by rotating and tilting the beam splitter (BS) and polarizing beam splitters (PBSs) in the receiver module. There will always be a remaining difference, of course.

6.2.11.2 Reduction of the Field of View: SFI.18

In order to further reduce the impact of this effect, it can be ensured that the field of view of the receiver is not defined by the active area of the APDs. In other words it should be impossible to shine light onto the outskirts of their active areas, where the detection efficiency mismatch is presumably worst.

6.2.11.3 Privacy Amplification: SFI.19*

Remaining inhomogeneities have to be taken care of during PA as in SFI.16. This has been discussed for two-detector setups in [17], too.

6.2.12 Spectral Detection Efficiency Mismatch (TI.B03)

The spectral detection efficiency mismatch is presumably rather small, since the spectral efficiency differences of the detectors are comparably small. But the passive optical components inside the Bob module also have to be taken into account.

6.2.12.1 Selection of APDs with Regard to Spectral Efficiency: SFI.20*

To start from the best possible situation, one should try to select APDs with a maximum overlap of their efficiency in the important spectral area (see SFI.21).

[8] This procedure will usually be performed anyway to maximize the total efficiency of the system

6.2.12.2 Spectral Filtering: SFI.21

Since the relative spectral efficiency mismatch is usually maximal far away from the design wavelength of the TOE, a narrow band pass filter[9] can be introduced at the entrance of the detector module. In the TOE there is an interference filter used with a width of 3 nm FWHM.

6.2.12.3 Privacy Amplification: SFI.22*

Like in the previous cases, the remaining differences have to be addressed in the PA process. This can be handled like in SFI.19 and SFI.16. For two-detector setup this is shown in [17].

6.2.13 Constant Detector Efficiency Mismatch (TI.B04)

6.2.13.1 Adjustment of the Detector Efficiencies: SFI.23*

After applying SFI.17, SFI.18, SFI.20 and SFI.21, there may still be some constant detector efficiency mismatch. This could be optimized by adjusting the bias voltage of the APDs themselves, since that affects the detection efficiency of each APD separately. This method should be used very carefully, though, since other properties of the APD (like dead time, timing jitter and signal pulse height) may be affected by this change, too.

6.2.13.2 Privacy Amplification: SFI.24*

The resulting information that is accessible to an eavesdropper due to a detector efficiency mismatch can be reduced to a necessary level by privacy amplification [8, Theorem 7]. If the total efficiency is described by $\eta = (1 - \eta_{ind})(1 - \eta_{dep})$, where η_{ind} and η_{dep} are basis independent and dependent efficiencies, the shrinking ratio is

$$R = \max\left(1 - H_2(\delta) - H_2\left(\delta + \frac{\eta_{dep}}{1 - \eta_{dep}}\right), 0\right) \tag{6.12}$$

where δ is the standard QBER.

6.2.14 Trojan Horse Attack (Receiver, TI.B05)

So far it seems that a Trojan horse attack is not feasible, since there are no actively switched components in the detector module. Spectral filtering (SFI.21) and bright light detection (SFI.25) would be effective countermeasures against such an attack.

[9] Such a filter is already used in the TOE for background suppression.

6.2.15 Detector Dead Times (TI.B06)

6.2.15.1 Bright Light Detection: SFI.25*

Attacks on detector dead times using bright light pulses (TI.B06b) can be detected by introducing a standard photo detector that monitors the amount of light at the entrance of the Bob module (behind all filters) [68][10] or measuring the APD current [54]. When a reasonable level is exceeded (even for short times) the respective events could be discarded. This would not prevent TI.B06a, though, but may be interesting against other attacks, too.

6.2.15.2 APD Bias Monitoring: SFI.26*

One way to rule out an attack aimed at the dead time of (ungated passively quenched) APDs is to sense whether all (at least all (!) APDs are active and allow clicks to be recorded or processed only when this is the case. One possibility for such an implementation would be to measure whether the voltages at the anodes of all APDs are sufficiently high (so that a detection event would definitely trigger the discriminator). For more details see the following chapter. This will also counteract the effect that for high clock rates (periods smaller than the dead time), the resulting keys can show anti-correlations [53]. In order to make sure that this countermeasure does not limit the sifted key rate unnecessarily, the transmitted photon intensity can be optimized [53].

6.2.15.3 Privacy Amplification: SFI.27*

It will have to be investigated whether or not SFI.26 can successfully negate all possible dead time attacks. It may turn out that there will still remain some need for additional PA. On the other hand it is clear that software methods alone (e.g. PA or checking whether some detector has fired shortly before the current event [53]) will not suffice.

6.2.16 Thermal Dependency of Breakdown Voltage (TI.B07)

6.2.16.1 Bright Light Detection: SFI.25*

Since this attack requires very bright, but potentially short pulses, this can be detected by a photo diode (see 6.2.15.1). Signal events should be discarded when a bright light pulse is detected before or at the same time.

[10] This idea was not so explicitly mentioned in the finally submitted version [54].

6.2.17 Insufficient Gating (TI.B08)

This attack is currently not applicable to the TOE. Still, SFI.26* (section 6.2.15.2) would prevent this attack efficiently, too.

6.2.18 Correlated Radiation (TI.B09)

6.2.18.1 Shielding SFI.28*

Like in classical cryptography systems, the detector module has to be shielded and decoupled from the environment so that it does not emit any (security relevant) electromagnetic radiation.

6.2.19 Breakdown Flash (TI.B10)

6.2.19.1 Spectral Filtering Inside the Detector Module: SFI.21

Since the spectrum of the breakdown flash is relatively broad [60], its effect can be reduced significantly by using a narrow filter. In order to suppress the information leakage due to this effect, one can utilize a narrow spectral filter close to the detector module, so that Eve cannot access the space between the APDs and the filter.

6.2.19.2 Spatial Filtering at the Detector: SFI.29*

To further reduce the effect of breakdown flashes, the optical path from the APDs to the environment (outside the secured area) can be blocked as well as possible. (This may already be sufficiently done by SFI.18 (see 6.2.11.2).)

6.2.19.3 Privacy Amplification: SFI.30*

The breakdown flash can be treated analogously to the multi photon pulses and its countermeasure by privacy amplification. When the rate of photons emitted this way is known, a Δ_{bdf} can be calculated that has to be added to Δ_{wcp} or Δ_{decoy}.

$$R = \max\left((1-\Delta') - H_2(\delta) - (1-\Delta')H_2\left(\frac{\delta}{1-\Delta'}\right), 0\right) \tag{6.13}$$

with $\Delta' = \Delta_{wcp} + \Delta_{bdf}$ or $\Delta' = \Delta_{decoy} + \Delta_{bdf}$, depending on the treatment of multi photon events.

6.2.20 Coincidence Detection (TI.B11)

6.2.20.1 Random Bit Attribution: SFI.31*

When a coincidence (two events inside one signal time window) is detected, a random single detection event has to be assigned to the event in order to prevent an attack described in the QKD security proofs [8, 14]. It goes without saying that the source of randomness should be quantum.

6.2.21 Finite Key Length (TI.S01)

6.2.21.1 Privacy Amplification: SFI.32*

The statistical fluctuations that happen because of finite key lengths can be treated during privacy amplification. This is a topic of current research [69–71].

6.2.22 Correlated Radiation over the Classical Channel (TC.01)

6.2.22.1 Separation of Circuits: SFC.01*

Careful separation of internal and external circuits should suppress the transmission of signals that may not leave the secured area. Since the classical channel ideally does not convey any sensitive information itself, it has only to be ruled out that sensitive information that should not be on the classical channel at all, gets out via this. One possibility of doing this could be to use completely separated circuits (e.g. with optocouplers) to transfer information from one circuit to the other. In such a way, power supply lines and even ground potentials should be decoupled. This will also address TC.03, where this is used to manipulate rather than read information.

6.2.23 Software Design Flaws (TC.02)

6.2.23.1 Code Review: SFC.02*

In order to rule out that sensitive information is accidently transmitted via the classical channel, the software has to be reviewed for security loopholes.

6.2.24 Insufficient Decoupling (TC.03)

6.2.24.1 Separation of Circuits: SFC.01*

See 6.2.22.1.

6.2.25 Man-in-the-Middle-Attack

6.2.25.1 Authentication: SFH.01

A man-in-the-middle-attack can only be opposed by authentication of the legitimate parties. Suitable ways to do this securely are Wegman-Carter message authentication [7] or some standard HMAC routines.

6.2.26 Summary

Threat	SFR	Description
TQ.01	SFQ.01	Privacy amplification for ideal quantum channel
TI.A01	SFI.01	Spectral Selection of Laser Diodes
	SFI.02*	Spectral Filtering
	SFI.03*	Privacy Amplification
TI.A02	SFI.04	Spatial Filtering
	SFI.05*	Privacy Amplification
TI.A03	SFI.06	Maximizing temporal overlap
	SFI.07*	Privacy Amplification
TI.A04	SFI.08*	Mean Photon Number Monitoring
	SFI.09*	Privacy Amplification
TI.A05	SFI.08*	Mean Photon Number Monitoring
	SFI.09*	Privacy Amplification
TI.A06	SFI.10*	Optical Isolator
TI.A07	SFI.11a*	Mean Photon Number Optimization
	SFI.11b	Decoy State Extension
TI.A08	SFI.12*	Electromagnetic Shielding
TI.A09	SFI.13*	Quantum Random Number Generator
TI.B01	SFI.14	Equalization of Path Lengths
	SFI.15	Hardware/ Software Delay
	SFI.16*	Privacy Amplification
TI.B02	SFI.17	Maximization of Spatial Overlap
	SFI.18	Reduction of Field of View
	SFI.19*	Privacy Amplification
TI.B03	SFI.20*	APD Selection for Efficiency
	SFI.21	Spectral Filtering
	SFI.22*	Privacy Amplification
TI.B04	SFI.23*	Adjustment of the Detector Efficiencies
	SFI.24*	Privacy Amplification
TI.B05	N/A	(Trojan Horse Attack Ineffective)
TI.B06a	SFI.25*	Bright Light Detection
	SFI.26*	APD Bias Monitoring
	SFI.27*	Privacy Amplification
TI.B06b	SFI.26*	APD Bias Monitoring
	SFI.27*	Privacy Amplification
TI.B07	SFI.25*	Bright Light Detection
TI.B08	N/A	(No Hardware Gating Implemented)
TI.B09	SFI.28*	Electromagnetic Shielding
TI.B10	SFI.21	Spectral Filtering

Threat	SFR	Description
	SFI.29* SFI.30*	Spatial Filtering (/SFI.18) Privacy Amplification
TI.B11	SFI.31*	Random Bit Attribution
TI.S01	SFI.32*	Privacy Amplification
TC.01	SFC.01*	Separation of Circuits
TC.02	SFC.02*	Code Review
TC.03	SFC.01*	Separation of Circuits
TH.01	SFH.01	Authentication

7 Eavesdropping without Interception: A New Dead Time Attack

Contents

7.1 Introduction

In Chapter 5 I have listed a number of attacks that can possibly be launched on real implementations of QKD systems similar to the one we have developed. In this section I want to examine one of these attacks (TI.B06a, see 5.2.4.2) more carefully. It exploits the so-called dead time of single photon counting detectors, i.e. the time a detector needs to recover from a detection event. We have experimentally demonstrated such an attack and propose an effective countermeasure [72].

7.2 Prerequisites for the applicability of this attack

Two characteristic features of many demonstrated QKD systems enable this particular attack: The first is the fact that when an SPD registers a photon, there usually follows a period of time during which it will not be able to output a second detection event. This period (called dead time) can range from less than a nanosecond to

some tens of microseconds, depending on the specific SPD. In our system, we use passively quenched Silicon avalanche photodiodes (SiAPDs)[1], with a particularly long dead time of about 0.5 μs (see Fig. 7.1). The second feature is the periodic operation. This means, there are well defined times when the transmitter emits a signal. Consequently the receiver accepts detection events only during narrow time windows – all events outside these time slots are discarded. For this attack it is ideal if this gating is done on the output signal of the SPD (e.g. in software) rather than by controlling the sensitivity of the detector[2]. The presence of these two properties, the dead time of the SPD and a (software) time window that determines whether a detection event is considered background or signal are necessary requirements for this particular attack, that we describe below.

7.3 The model QKD system

For reasons of simplicity and because it fits to our setup, the QKD device shall in principle employ a BB84 protocol with the polarization of single photons as qubits. The detector part shall be designed as shown in Fig. 7.2: The first non-polarizing 50/50 BS serves as a random basis switch, if the incident photon is reflected, a PBS together with two SiAPDs will analyse the photon's polarization in the H/V basis. However, if the photon is transmitted, the half-wave plate will rotate its polarization by 45° and the remaining PBS together with the two SiAPDs will analyse the photon's polarization in the ±45° basis. I also assume that no hardware gating is used, i.e. the SPDs are in principle always active. A time window to discriminate signal from background counts is applied on the output logic signal (either in hardware or software). Suppose that the transmitter (Alice) sends the i-th qubit at time $t_i = i \cdot T$ with the period T and the receiver (Bob) expects the i-th qubit between $t_i - \Delta_{tw}/2$ and $t_i + \Delta_{tw}/2$, so that the time window has a width of Δ_{tw}. In this experiment the period was $T = 4$ μs and $\Delta_{tw} = 5$ ns (see fig. 7.1).

7.4 The attack

At least one attack has already been proposed by V. Makarov and co-workers [54], that makes use of the dead time of SPDs. Similar attacks have been proposed in [55–58], all using some kind of intercept-resend strategy. The one described here is different in this way. To perform this attack, the eavesdropper (Eve) simply sends in light pulses of one of the four polarizations used in the protocol (H, V, +45° or

[1] We are using the commercially available PerkinElmer C30902S.

[2] When sensitivity gating is applied, the timing of the attack is getting crucial. If it is possible to trigger an avalanche around the start of the gate interval without triggering a signal pulse at the output of the SPD, this attack will still be feasible. Since our system does not use hardware gating, we do not investigate this any further.

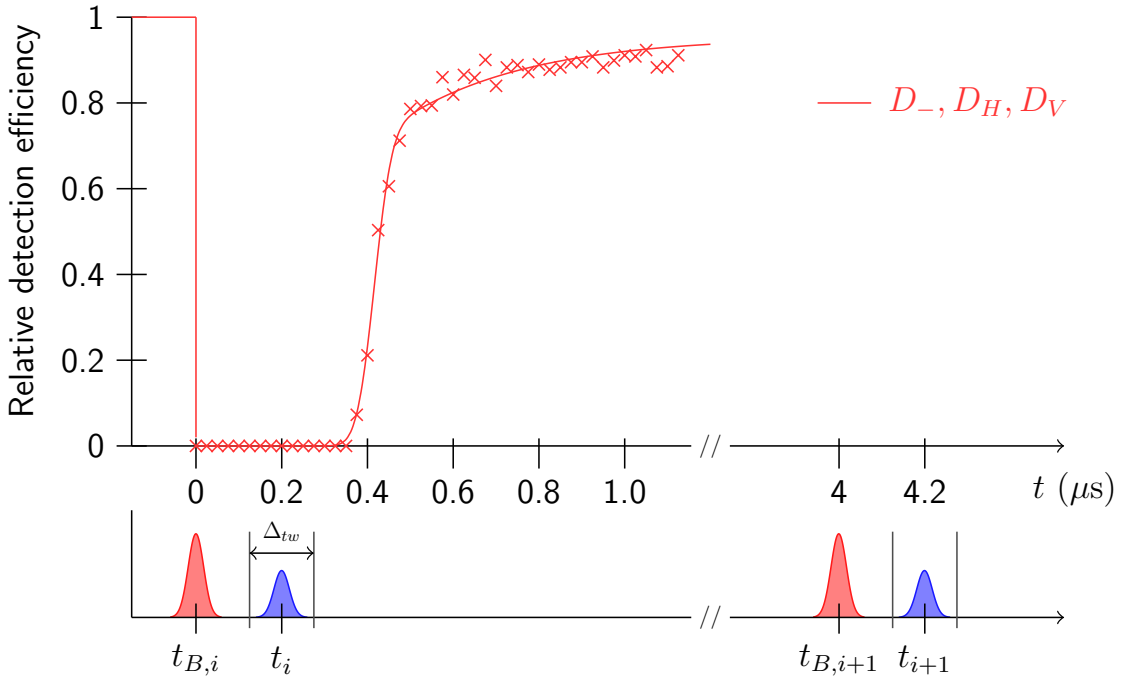

Figure 7.1: Probability for a detection event (normalized to the value after 3.5 μs after a detection at $t = 0$). SiAPDs exhibit a detection efficiency which depends on the overbias voltage applied. After a detection, depending on the electronics, it takes some time until the detector regains full efficiency. Due to additional threshold circuits, there is also a time where the detector does not output a click at all. For the characterization of the detector's dead time, we illuminated it by two consecutive faint laser pulses. The delay between the first and second pulse has been tuned and the corresponding relative detection efficiency was recorded. The line is a fit using the function $E(t) = \frac{A}{2}\left(1 + \mathrm{erf}\left(\frac{t-\tau_D}{\tau_2}\right)\right) \cdot \left(1 - e^{-\frac{t}{\tau_3}}\right)$ with fit parameters $A, \tau_D, \tau_2, \tau_3$. For the attack, the eavesdropper sends sufficiently bright pulses onto Bob's detectors just before the regular pulses from Alice arrive, in this case we used a time difference $t_i - t_{B,i} =$ 200 ns. Pulse and gate widths are not to scale, both are typically on the order of 1 ns.

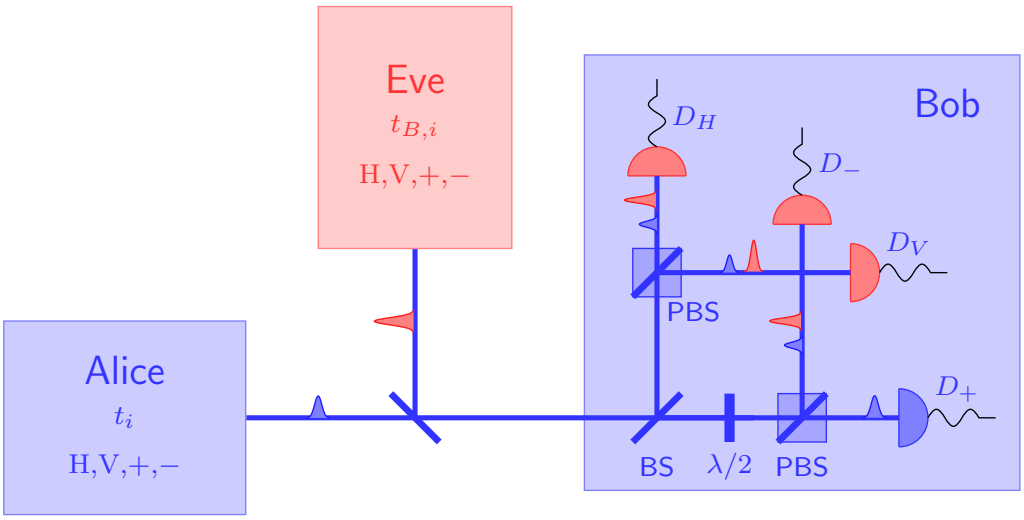

Figure 7.2: Schematic drawing of the setup: The transmitter (Alice) on the left, her pulses marked blue, the eavesdropper (Eve) in the center, her pulses marked red and the receiver (Bob) on the right. When Eve sends a sufficiently intense light pulse polarized in on of the four polarization, up to three of Bob's detectors are inactive with a high probability. Alice's following signal pulse can only be detected in the remaining detector.

$-45°$), outside of Bob's time window. With a certain probability, depending on the intensity of the pulse, three of Bob's SPDs will be inactive afterwards, because they have detected photons and are now recovering. If Eve's timing is good, she can thus manipulate the average detection probability of Bob's SPDs during signal time windows, three of the four values will be decreased, while one (the one belonging to the perpendicular polarization she has used) remains constant. In fact, when passively quenched SiAPDs are used at output rates (at Alice) of some tens of MHz, the SPDs will be inactive for several clock periods. This means that the relative efficiency of one of the SPDs is increased, so that the probability that this detector registers an event is elevated. By increasing the intensity, Eve can make sure that the detection probabilities of three detectors become negligible, so that whenever Bob registers an event during this time, Eve will know that it can only be the one perpendicular to the polarization she had sent in before. She should make sure, of course, not to send in a blinding pulse of a different polarization, before all Bob's detectors are expected to be active again (this effect can also happen when Alice runs at a high repetition rate compared to the dead time [73, 74]).

As long as the polarization of Eve's blinding pulses are perfectly aligned with Bob's polarization measurements, the attack will not introduce any errors between Alice and Bob. The amount of information that Eve will have about the sifted key can be tuned by her, ideally she will get as close to full information as she wants.

If we assume that the delay between two of Bob's signal time slots and hence also Eve's blinding pulses is greater than the average dead time of the SPDs, which itself is longer than a signal time slot, the probability of triggering one of the detectors with a blinding pulse can be calculated. Doing so we can further assume the recovery process to be discrete with a certain dead time, which simplifies the calculations.

7.4.1 Blinding pulse detection probabilities

To evaluate the effect of this attack, one has to calculate the detection probabilities of blinding pulses (those issued from Eve) and signal pulses (emitted by Alice). We start with the blinding pulses. Let $P_p(\mu_B^{\text{eff}})$ and $P_d(\mu_B^{\text{eff}})$ be the probability that a blinding pulse is recognized in the detector parallel and diagonal to the blinding pulse, respectively. The corresponding probability in the orthogonal detector is negligible. They depend on the blinding pulse intensity expressed as their mean photon number per pulse $\mu_B^{\text{eff}} := \eta_B \mu_B$. We define this as the number Eve would have to send in to an ideal detector module (regarding transmission and detector efficiency) built like depicted in Fig. 7.2. Uniform, but non-unity transmission and detector efficiencies can be included therein. If the receiver module used active basis switching (i.e. only two detectors), only half of the blinding pulse intensity would be sufficient.
The probabilities of registering detections in one, two or three of the respective detectors at the same time are:

$$p_p(\mu_B^{\text{eff}}) = \underbrace{P_p(\mu_B^{\text{eff}})}_{\text{parallel detector clicks}} \cdot \underbrace{(1 - P_d(\mu_B^{\text{eff}}))(1 - P_d(\mu_B^{\text{eff}}))}_{\text{both diagonal detectors do not click}} \tag{7.1}$$

$$p_d(\mu_B^{\text{eff}}) = P_d(\mu_B^{\text{eff}}) \cdot (1 - P_p(\mu_B^{\text{eff}}))(1 - P_d(\mu_B^{\text{eff}})) \quad (2\times) \tag{7.2}$$

$$p_{pd}(\mu_B^{\text{eff}}) = P_p(\mu_B^{\text{eff}}) \cdot P_d(\mu_B^{\text{eff}}) \cdot (1 - P_d(\mu_B^{\text{eff}})) \quad (2\times) \tag{7.3}$$

$$p_{dd}(\mu_B^{\text{eff}}) = P_d^2(\mu_B^{\text{eff}}) \cdot (1 - P_p(\mu_B^{\text{eff}})) \tag{7.4}$$

$$p_{pdd}(\mu_B^{\text{eff}}) = P_p(\mu_B^{\text{eff}}) \cdot P_d^2(\mu_B^{\text{eff}}) \tag{7.5}$$

So the probabilities that none, one, two or three detectors fire from a blinding pulse are (theoretically, four detectors do not fire at once, if the polarizations are correctly aligned):

$$p_{(0)}(\mu_B^{\text{eff}}) = (1 - P_p(\mu_B^{\text{eff}})) \cdot (1 - P_d(\mu_B^{\text{eff}}))^2 \tag{7.6}$$

$$p_{(1)}(\mu_B^{\text{eff}}) = p_p(\mu_B^{\text{eff}}) + 2p_d(\mu_B^{\text{eff}}) \tag{7.7}$$

$$p_{(2)}(\mu_B^{\text{eff}}) = 2p_{pd}(\mu_B^{\text{eff}}) + p_{dd}(\mu_B^{\text{eff}}) \tag{7.8}$$

$$p_{(3)}(\mu_B^{\text{eff}}) = p_{pdd}(\mu_B^{\text{eff}}) \tag{7.9}$$

7.4.2 Signal pulse detection probabilities

Using the previous results, the probability that a detector clicks from a signal pulse, depending on the detector's polarization ϕ and the signal pulse's polarization θ with respect to the blinding pulse can be calculated.

$$p^S_{\theta,\phi}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) = (1 - P_\phi(\mu_B^{\text{eff}}))P^S_\theta(\mu_S^{\text{eff}}) \tag{7.10}$$

with $\phi, \theta \in \{p, d, o\}$ meaning parallel, diagonal and orthogonal and $P^x_o(\mu_x^{\text{eff}}) \equiv 0$ and the mean photon number per signal pulse at the receiver $\mu_S^{\text{eff}} := \eta\mu_S$.
From this, the amount of information, an adversary can gain from such an attack, can be estimated: The difference between the maximum (= 1) and the current value of the binary entropy is used as the information gain a potential eavesdropper would have:

$$\begin{aligned} I_{EB} &= 1 - H_2(p(x_{Eve} = x_{Bob})) && (7.11)\\ &= 1 + \Pr(x_{Eve} = x_{Bob}) \log(\Pr(x_{Eve} = x_{Bob})) \\ &\quad + \Pr(x_{Eve} \neq x_{Bob}) \log(\Pr(x_{Eve} \neq x_{Bob})) && (7.12) \end{aligned}$$

With

$$\begin{aligned} p_\parallel(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &:= p^S_{p,p}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) + p^S_{d,d}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \qquad \text{and} && (7.13)\\ p_\perp(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &:= p^S_{o,o}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) + p^S_{d,d}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) && (7.14) \end{aligned}$$

we find:

$$\left.\begin{aligned} p^{0_B}_H(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\parallel(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \\ p^{1_B}_H(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\perp(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \end{aligned}\right\} \quad \text{if Eve sends H} \tag{7.15}$$

$$\left.\begin{aligned} p^{0_B}_V(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\perp(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \\ p^{1_B}_V(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\parallel(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \end{aligned}\right\} \quad \text{if Eve sends V} \tag{7.16}$$

$$\left.\begin{aligned} p^{0_B}_P(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\parallel(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \\ p^{1_B}_P(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\perp(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \end{aligned}\right\} \quad \text{if Eve sends } +45°\text{=P} \tag{7.17}$$

$$\left.\begin{aligned} p^{0_B}_M(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\perp(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \\ p^{1_B}_M(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= p_\parallel(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \end{aligned}\right\} \quad \text{if Eve sends -45°=M} \tag{7.18}$$

It is intuitively clear that for large μ_B^{eff}, i.e. high blinding intensities, all terms with $p^S_{d,d}$ and $p^S_{p,p}$ will become small, because most of the time, all detectors but the one orthogonal to the blinding pulse will be inactive (see Fig. 7.4).
Now the information gain (7.12) can be calculated as:

$$\begin{aligned} I_{EB}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) &= 1 + \frac{p_\parallel}{p_\parallel + p_\perp} \log_2 \left(\frac{p_\parallel}{p_\parallel + p_\perp} \right) \\ &\quad + \frac{p_\perp}{p_\parallel + p_\perp} \log_2 \left(\frac{p_\perp}{p_\parallel + p_\perp} \right) && (7.19) \end{aligned}$$

In the simulation (Fig. 7.3) it is assumed that the photon statistics of signal and blinding pulses are Poissonian and thus $P_p(\mu_B^{\text{eff}}) = 1 - e^{-\frac{\mu_B^{\text{eff}}}{2}}$, $P_d(\mu_B^{\text{eff}}) = 1 - e^{-\frac{\mu_B^{\text{eff}}}{4}}$, $P_p^S(\mu_S^{\text{eff}}) = 1 - e^{-\frac{\mu_S^{\text{eff}}}{2}}$ and $P_d^S(\mu_S^{\text{eff}}) = 1 - e^{-\frac{\mu_S^{\text{eff}}}{4}}$.

7.5 Experimental setup

In order to demonstrate the previously described attack we set up a version of our free space QKD system (see Chapter 4) in the lab. The transmitter (Alice) contains four laser diodes with their beams combined on a set of two conical mirrors, oriented such that their polarizations are at the four necessary polarizations. After a short free space link we placed one of our Bob receiver modules configured as depicted in Fig. 7.2. The Alice module was connected to a standard PC via a USB 2.0 connection, while the Bob module was connected to a home build time tagging unit, connected to another standard PC.
Additionally to this usual setup, we set up a second faint pulse transmitter module (Eve), similar to the Alice module, only with special emphasis laid on the fact that it should emit pulses with comparatively high mean photon numbers. For easier synchronization with Alice and Bob, the four laser diodes inside the Eve module were driven by the four extra laser diode drivers of Alice, usually used for the decoy state protocol extension. The light emitted by Eve was coupled into the free space link using a non-polarizing beam splitter (see Fig. 7.2). The timing was set such that Alice's signal pulses occurred every 4 μs (to allow the SiAPDs to recover with a high probability between two consecutive blinding pulses), preceded by a blinding pulse from Eve, 200 ns before. The value of the delay between blinding and signal pulses was chosen, so that it be longer than the processing time of the timetagging electronics (140 ns), but still within the dead time of the SiAPDs ($\sim$ 500 ns, see Fig. 7.1). The mean photon number μ_B^{eff} of the blinding pulses was controlled by inserting different combinations of neutral density filters. Eve's key was deduced from the classical communication between Alice and Bob. According to the BB84 protocol, Bob communicates to Alice when and in which basis he detected a photon, with Alice returning her basis choice. This information together with the knowledge about the setting of her blinding pulses enables Eve to construct a key which coincides with Alice's and Bob's key in case of equal bases between Alice, Bob and Eve.

7.6 Results

We ran the protocol with different blinding pulse intensities, the results are shown in Tab. 7.1 and Fig. 7.3 (and for illustration Fig. 7.4). As expected, for low blinding pulse intensities, Eve's sifted key was hardly correlated with the ones of Alice and Bob, but the more powerful her pulses got, the better the match between the keys.

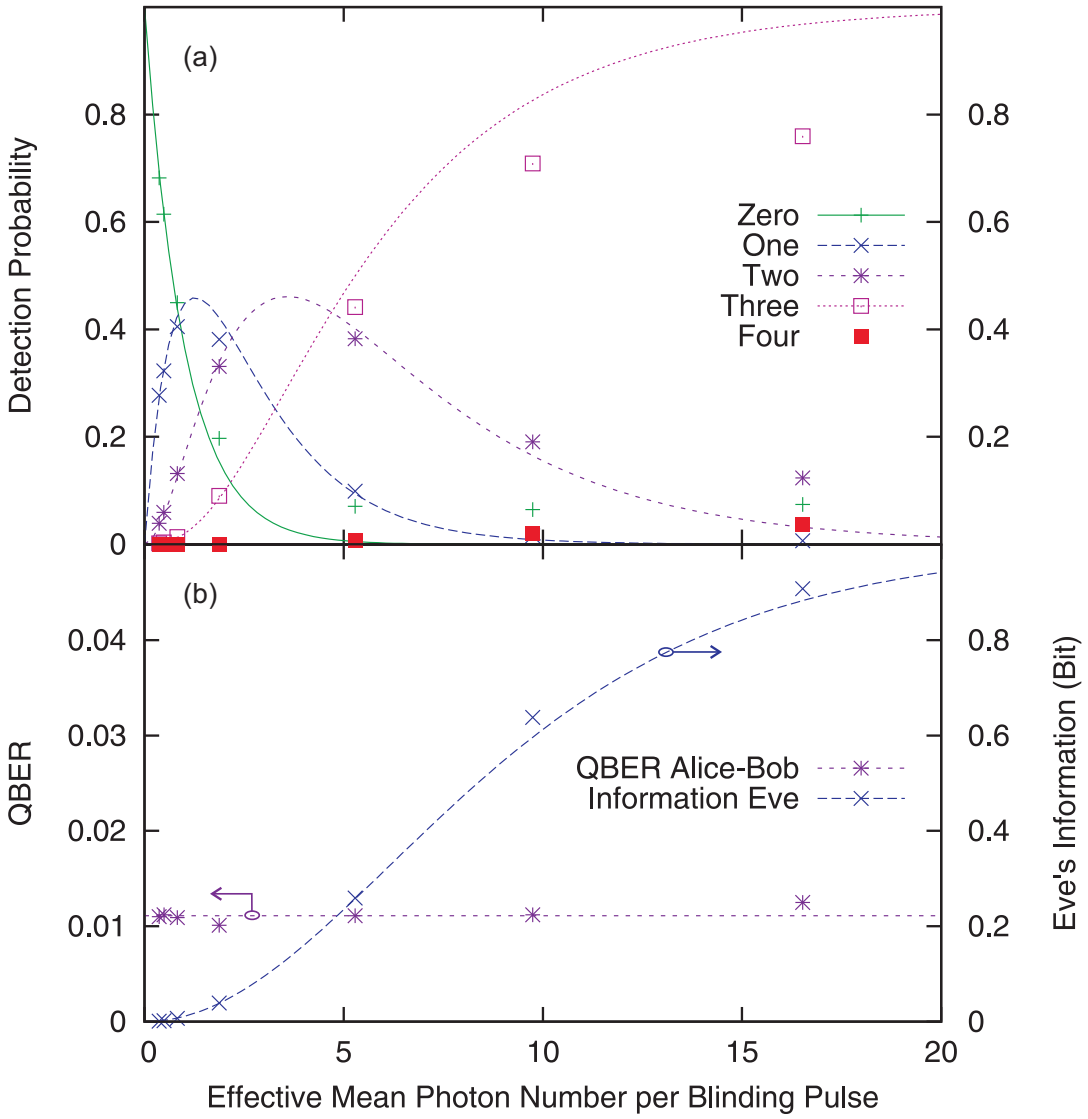

Figure 7.3: Experimental results of the eavesdropping attack (a) showing the probability for detecting blinding pulse photons in zero, one, two, three or four detectors depending on the effective mean photon number per blinding pulse. (b) shows the QBER of Alice's and Bob's key and the information about this key gathered by Eve. By using different combinations of neutral density filters, the blinding pulse intensity was adjusted, while keeping the signal pulse intensity constant. With increasing number of photons per blinding pulse the probability that three detectors are blinded increases rapidly resulting in an information of > 0.9 bit for about 17 photons, while the QBER does not increase and leaves Alice ignorant about the attack.

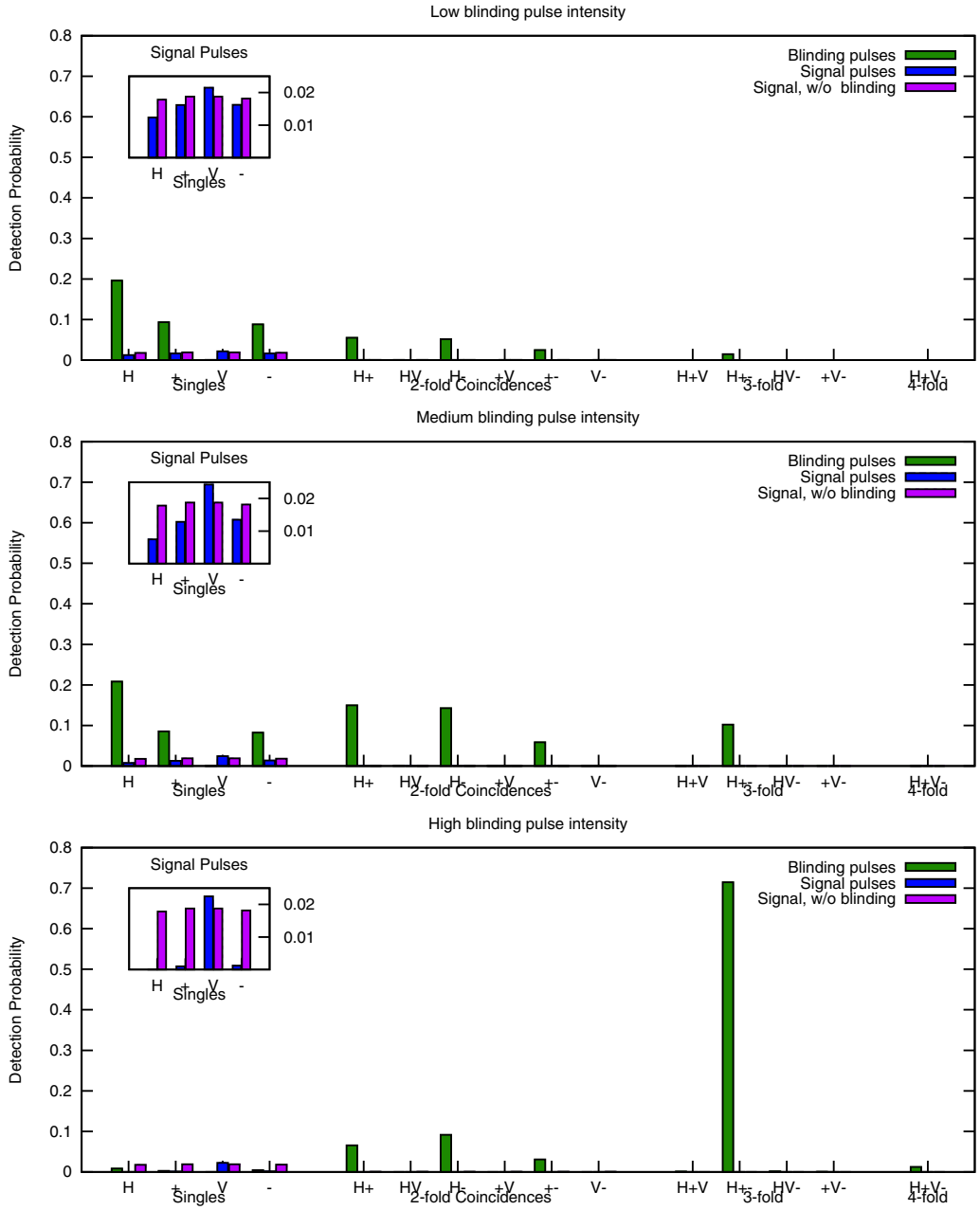

Figure 7.4: Experimental results with only horizontal blinding pulses. This illustrates how the signal pulse detection probabilities (magnified in the inset) of the horizontal and both diagonal SPD are modified with increasing blinding pulse intensity. When the blinding pulse intensity is high, most of the time three detectors are inactive, so that the signal pulse can only trigger the SPD orthogonal to the blinding pulse (lower image).

μ_B^{eff}	QBER Alice-Bob / %	QBER Bob-Eve / %	Eve's Information I_{EB}
0.37	1.10	48.17	0.001
0.49	1.12	47.54	0.002
0.83*	1.09	45.24	0.007
1.88	1.01	38.43	0.039
5.29*	1.11	21.00	0.259
9.75	1.12	6.91	0.638
16.52*	1.25	1.17	0.908

Table 7.1: Experimental results of the eavesdropping attack exploiting the dead time of the passively quenched SiAPDs. The datasets marked with a "*" are the ones corresponding to the last three images of Fig. 7.5.

The maximum overlap between Bob's and Eve's sifted keys was 98.83% at a mean photon number per blinding pulse of $\mu_B^{\text{eff}} = 16.52$, corresponding to an information $I = 0.908$ Bit. The QBER between Alice and Bob stayed at a constant level of about 1.1%[3] as shown in Tab. 7.1.
The calculated blinding pulse probabilities are in good agreement with the experimental data when the blinding pulse intensities μ_B^{eff} are rather low. For higher values of μ_B^{eff}, the prediction is considerably higher than what our count rates showed to be. We expect that this is because we have used neutral density filters to set the different intensities and with increasing mean photon number per pulse, the number of background events rises, too. Background events blind the detectors, which in turn leads to a decreased blinding pulse detection probability.
As an illustration we used Bob's sifted key[4] to encrypt the logo of our university using a one-time-pad and decrypted this with Eve's sifted key (see Fig. 7.5).

7.7 Countermeasures

Some countermeasures against the effects of the dead time of passively quenched APDs have already been proposed [54, 73, 75]. We suggest a conceptually very easy and very efficient different method: By monitoring the voltage level at the high voltage pin of the SiAPD, one can make sure that it is charged above the level it

[3] This is true when coincident detection events during the signal time window were discarded. As mentioned in section 5.2.4.2, this generally opens a security loop hole. If the according countermeasure (see 6.2.20) was applied, the QBER between Alice and Bob actually decreases with increasing mean photon number per blinding pulse, since the probability that more than one detector was even active decreased and hence the probability for a coincidence detection as well.

[4] Eve's key is primarily correlated with Bob's sifted key, because she can predict what he will measure. The QBER between Alice and Bob affects the overlap between Alice's key and Eve's key.

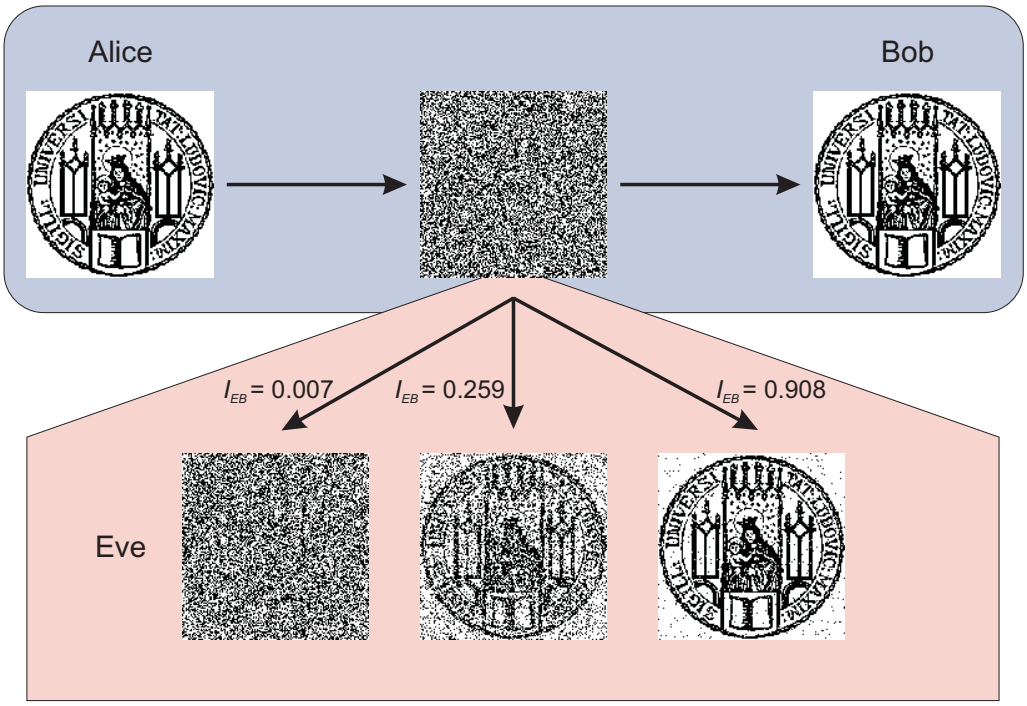

Figure 7.5: Application of the results obtained in the experiment. Alice uses her (error corrected) key to encrypt the original image (top left corner) and sends the ciphertext (top center) to Bob, who uses his (error corrected) key to decrypt the image (top right corner). The three images below are decrypted using Eve's deduction of the sifted key, emitting blinding pulses with a mean photon number of $\mu_B^{\text{eff}} = 0.83$, $\mu_B^{\text{eff}} = 5.29$ and $\mu_B^{\text{eff}} = 16.52$, respectively.

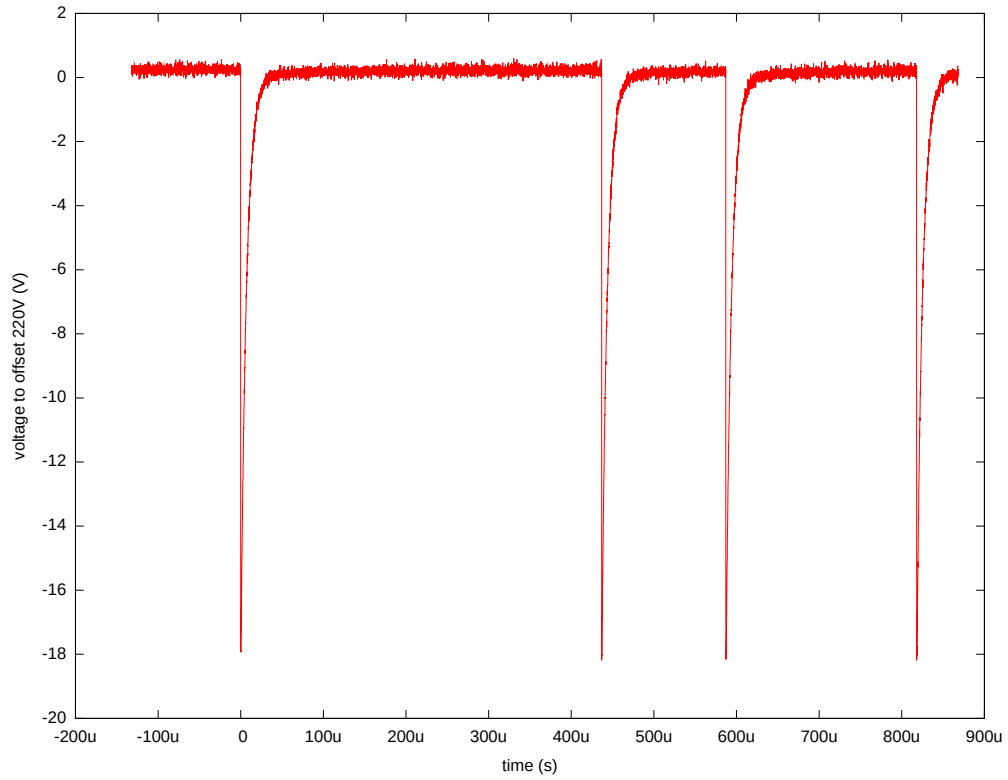

Figure 7.6: Bias voltage at the SiAPD. After a detection event, the voltage drops measurably. This can be used to decide whether or not all SPDs are active. The voltage has been recorded with a fast oscilloscope at the cathode of the SiAPD.

needs so that a detection will generate an electronic pulse above the discriminator threshold (see Fig. 7.6 and Fig. 7.7). Now only those detection events shall be used for the key generation where all four detectors were active in this sense, rendering such an attack useless. It also overcomes the problem of correlations in the sifted key because of detectors being inactive from a previous signal event as mentioned in [73]. This has been further investigated in [74], which proposes some methods and proves their validity, but there, a fixed dead time was assumed. Still, they also mention an idea similar to ours. Furthermore it is technically easier than holding all detectors inactive while one of them is within the dead time as proposed in [75]. A more complex technique, partly involving our idea, has recently been published in [76]. It uses hardware gating, randomly switched hardware and software bit mapping (while the hardware mapping is switched for all detectors simultaneously during the time when all detectors are fully sensitive) and the measurement of voltage at and current through the SiAPD.

It is obvious that the signal rate (and hence the sifted key rate, too) drop when

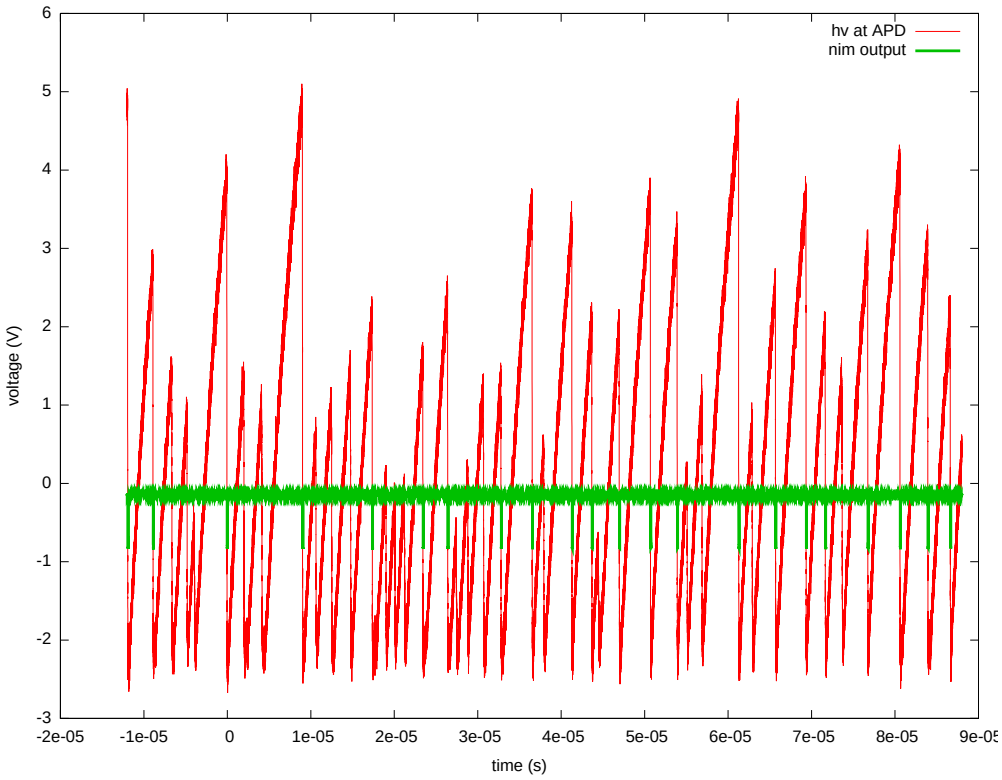

Figure 7.7: Bias voltage at the SiAPD together with the output NIM pulses measured at a high incident photon rate. This also illustrates that no NIM pulse is triggered when the SiAPD is not sufficiently charged.

such an attack is launched. When Eve uses high blinding pulse intensities, only one detector should be active, so the total rate will be decreased to 25 % of the undisturbed case (see insets in Fig. 7.4). One could have the idea to monitor the signal rate in order to detect such an attack, but this is not recommended. First of all, one would need to know the attenuation of the optical channel without Eve present. But Eve could be in there right from the start, so this is almost impossible to determine. Furthermore Eve could replace the quantum channel with one that has less attenuation (using quantum teleportation). This is theoretically no problem, although technically difficult. One more reason is that in free space QKD signal rate fluctuations are rather normal, since the attenuation changes with weather conditions etc.

8 Conclusion and Outlook

In this thesis I have reported on progress concerning two of the most important aspects of current QKD research. The first part describes concepts and our contribution to the heterogeneous QKD network installed in Vienna within the EU project SECOQC. In this network, six different QKD implementations cooperated to connect six locations via eight QKD links. Seven of them were implemented using optical fibres, while ours was the only free space optical connection, linking the building hosting the exhibition with the QKD backbone. It produced average sifted key rates of 40 kbit/s and secure key rates of 14 kbit/s with 2.3% QBER over a distance of 80 m, and ran even during daylight.
The project was part of the ongoing effort to migrate QKD systems from the researchers' labs towards real-life networks and applications. To this end the limits in link distance, secure key production rate and interoperability are still being pushed to new records. Free space optical QKD links are especially interesting when global connections are to be secured. QKD between satellites and the earth have been shown to be well within reach [65, 77], so that it appears to be feasible to connect most parts of the world by QKD. Different projects worldwide are aiming to bring quantum communication technology into space, either onto the ISS or small low-earth-orbit satellites.

The second part of this thesis deals with the security assessment of real QKD systems, in particular the one that we have developed. We could show that there was a loophole in our system that would have allowed an eavesdropper to gain almost complete knowledge of the sifted key even with today's technology. The remaining error between the eavesdropper's key and the legitimate receiver's key got as low as 1.17%, without increasing the QBER between Alice and Bob significantly. We also proposed a simple technical countermeasure against this loophole, preventing other possible attacks, too: Bob needs to make sure that all of his detectors are ready to register photons if he wants to use the detection for his sifted key.
In a similar fashion, other attacks can be tackled, too, for instance by an additional measurement or careful parameter optimization. One has to be careful, of course, not to open new loopholes by changing the protocol. In general it appears to me that QKD research will have to focus intensely on the implementation-specific problems even more in the future. Real systems can of course never be provably secure, these proofs only work for theoretic models. The important task is to bring model and implementation closer together, and there certainly has been some progress

recently [74, 76]. The deviation between theory and implementation is a problem that is common to classical and quantum cryptography, so it might be helpful if there were more communication between those two communities in the near future. In my opinion it is the clear advantage of QKD that the theoretical models are provably secure. This is in general not true for classical cryptography.

Publications

Publications related to the presented work:

- H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth and H. Weinfurter.
  Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors.
  New Journal of Physics, **13**:073024, (2011).

- M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter.
  High speed optical quantum random number generation.
  Opt. Express, **18**:13029–13037, (2010).

- S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier and H. Weinfurter.
  Information leakage via side channels in freespace BB84 quantum cryptography.
  New Journal of Physics, **11**:065001, (2009).

- M. Peev, C. Pacher, R. Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Furst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hubel, G. Humer, T. Langer, M. Legre, R. Lieger, J. Lodewyck, T. Lorunser, N. Lutkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger.
  The SECOQC quantum key distribution network in Vienna.
  New Journal of Physics, **11**:075001 (37pp), (2009).

- T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A. Zeilinger and H. Weinfurter.
  Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km.
  Phys. Rev. Lett., **98**:010504, (2007).

- R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. G. Rarity, Z. Sodnik, C. Barbiere, H. Weinfurter and A. Zeilinger.
  Entanglement-based quantum communication over 144 km.
  Nature Physics, **3**:481–486, (2007).

- H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer and H. Weinfurter.
  Free space quantum key distribution: Towards a real life application.
  Fortschritte der Physik, **54**:840–845, (2006).

- K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter and A. Zeilinger.
  Distributing entanglement and single photons through an intra-city, free-space quantum channel.
  Opt. Express, **13**, 202–209, (2005).

- H. Weier.
  Experimental Quantum Cryptography.
  Diplomarbeit, Technical University Munich, (2003).

Danksagung

Diese Arbeit wurde teilweise durch die Projekte SECOQC and QAP finanziert.

Mein persönlicher Dank gilt allen, die mich in der Zeit begleitet und unterstützt haben, insbesondere:

- Prof. Dr. Harald Weinfurter für die Möglichkeit, an diesem spannenden Projekt zu arbeiten und die Freiheiten, die ich dabei genießen durfte.
- Prof. Dr. Christian Kurtsiefer, der mir am Anfang meiner Zeit in der Arbeitsgruppe viel beigebracht hat, bevor er leider (aus meiner Sicht viel zu früh) nach Singapur wechselte.
- Tobias Schmitt-Manderbach, Martin Fürst, Sebastian Nauerth und Markus Rau, mit denen ich viele Messkampagnen auf Inseln, Bergen und Dächern in verschiedenen Ländern erleben durfte.
- Carsten Schuck, Gerhard Huber, Magdalena Kaminska, Witlef Wieczorek und Fredrik Hocke, zu denen ich während und nach ihrer Zeit in der Arbeitsgruppe auch im echten Leben einen guten Draht hatte und bis auf eine sehr traurige Ausnahme weiterhin habe.
- meinen Büroabschnittsgefährten Jürgen Volz, Chunlang Wang, Johannes Schachaneder, Daniel Schlenk und Asli Ugur für ein stets angenehmes Raumklima.
- allen weiteren (zum Teil ehemaligen) Mitgliedern der Arbeitsgruppe: Mohamed Bourennane, Manfred Eibl, Florian Henkel, Juliane Hermelbracht, Julian Hofmann, Nikolai Kiesel, Harald Krauss, Roland Krischek, Michael Krug, Davide Marangon, Yousef Nazirizadeh, Ivan Ordavo, Norbert Ortegel, Nadja Regner, Daniel Richart, Wenjamin Rosenfeld, Karen Saucke, Christian Schmid, Christian Schwemmer, Pavel Trojek, Oliver Schulz, Markus Weber und Patrick Zarda für die gute Zusammenarbeit und das nette Arbeitsumfeld.
- meiner Familie und meinen Freunden für alles, was das Leben außerhalb der Uni lebenswert macht.

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden.
Quantum cryptography.
Rev. Mod. Phys., **74**:145–195, (2002).

[2] C. H. Bennett and G. Brassard.
Quantum Cryptography: Public Key Distribution and Coin Tossing.
Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (1984).

[3] G. Brassard and L. Salvail.
Secret-Key Reconciliation by Public Discussion.
Advances in Cryptology - Proceedings of Eurocrypt'93, (1993).

[4] C. H. Bennett, G. Brassard and J.-M. Robert.
Privacy Amplification by public discussion.
SIAM J. Comput., **17**:210–229, (1988).

[5] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer.
Generalized Privacy Amplification.
IEEE Transaction on Information Theory, **41**:1915, (1995).

[6] J. L. Carter and M. N. Wegman.
Universal Classes of Hash Functions.
Journal of Computer and System Sciences, **18**:143–154, (1979).

[7] M. N. Wegman and J. L. Carter.
New Hash Function and Their Use in Authentication and Set Equality.
Journal of Computer and System Sciences, **22**:265–279, (1981).

[8] D. Gottesman, H. K. Lo, N. Lütkenhaus and J. Preskill.
Security of quantum key distribution with imperfect devices.
Quantum Information & Computation, **4**, 5:325–360, (2004).

[9] **On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols**, London, UK, (1995). Springer-Verlag.

[10] H.-K. Lo and H. F. Chau.
Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances.
Science, **283**:2050–2056, (1999).

[11] D. Mayers.
Unconditional security in quantum cryptography.
J. ACM, **48**, 3:351–406, (2001).

[12] H. F. Chau and H.-K. Lo.
Making an Empty Promise with a Quantum Computer.
Fortschritte der Physik, **46**:507–519, (1998).

[13] P. W. Shor and J. Preskill.
Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.
Phys. Rev. Lett., **85**:441–444, (2000).

[14] H. Inamori, N. Lütkenhaus and D. Mayer.
Unconditional security of practical quantum key distribution.
Eur. Phys. J. D, **41**:599–627, (2007).

[15] C. Branciard, N. Gisin, B. Kraus and V. Scarani.
Security of two quantum cryptography protocols using the same four qubit states.
Phys. Rev. A, **72**, 3:032301, (2005).

[16] Y. Zhao, C.-H. Fung, B. Qi, C. Chen and H.-K. Lo.
Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems.
Phys. Rev. A, **78**:042333, (2008).

[17] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma.
Security proof of quantum key distribution with detection efficiency mismatch.
Quantum Information and Computation, **9**:0131–0165, (2009).

[18] V. Scarani and C. Kurtsiefer.
The black paper of quantum cryptography: real implementation problems.
arXiv:0906.4547v1 [quant-ph], (2009).

[19] C. H. Bennett.
Quantum cryptography using any two nonorthogonal states.
Phys. Rev. Lett., **68**, 21:3121–3124, (1992).

[20] V. Scarani, A. Acín, G. Ribordy and N. Gisin.
Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations.
Phys. Rev. Lett., **92**, 5:057901, (2004).

[21] A. K. Ekert.
Quantum Cryptography Based on Bell's Theorem.
Phys. Rev. Lett., **67**, 6:661–663, (1991).

[22] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt.
Proposed experiment to test local hidden-variable theories.
Phys. Rev. Lett., **23**, 15:880–884, (1969).

[23] C. H. Bennett, G. Brassard and N. D. Mermin.
Quantum cryptography without Bell's theorem.
Phys. Rev. Lett., **68**, 5:557–559, (1992).

[24] F. Grosshans and P. Grangier.
Continuous Variable Quantum Cryptography Using Coherent States.
Phys. Rev. Lett., **88**, 5:057902, (2002).

[25] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri and P. Grangier.
Field test of a continuous-variable quantum key distribution prototype.
New Journal of Physics, **11**, 4:045023 (14pp), (2009).

[26] C. Silberhorn, T. C. Ralph, N. Lütkenhaus and G. Leuchs.
Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit.
Phys. Rev. Lett., **89**, 16:167901, (2002).

[27] M. Heid and N. Lütkenhaus.
Security of coherent-state quantum cryptography in the presence of Gaussian noise.
Phys. Rev. A, **76**, 2:022313, (2007).

[28] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych and G. Leuchs.
Feasibility of free space quantum key distribution with coherent polarization states.
New Journal of Physics, **11**, 4:045014 (13pp), (2009).

[29] M. Peev, C. Pacher, R. Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Furst,

J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hubel, G. Humer, T. Langer, M. Legre, R. Lieger, J. Lodewyck, T. Lorunser, N. Lutkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger.
The SECOQC quantum key distribution network in Vienna.
New Journal of Physics, **11**, 7:075001 (37pp), (2009).

[30] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin.
"Plug and play" systems for quantum cryptography.
Appl. Phys. Lett., **70**, 7:793–795, (1997).

[31] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden.
Quantum key distribution over 67 km with a plug & play system.
New Journal of Physics, **4**, 41:1–8, (2002).

[32] D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden.
Fast and simple one-way quantum key distribution.
Applied Physics Letters, **87**, 19:194108, (2005).

[33] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel and H. Zbinden.
High speed coherent one-way quantum key distribution prototype.
arXiv:0809.5264v1 [quant-ph], (2008).

[34] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery and S. Ten.
High rate, long-distance quantum key distribution over 250km of ultra low loss fibres.
arXiv:0903.3907v1 [quant-ph], (2009).

[35] R. T. Thew, D. Stucki, J.-D. Gautier, H. Zbinden and A. Rochas.
Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths.
Applied Physics Letters, **91**, 20:201114, (2007).

[36] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe and A. J. Shields.
Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate.
Opt. Express, **16**, 23:18790–18979, (2008).

[37] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorunser, E. Querasser, T. Matyus, H. Hubel and A. Zeilinger.
A fully automated entanglement-based quantum cryptography system for telecom fiber networks.
New Journal of Physics, **11**, 4:045013 (19pp), (2009).

[38] F. Grosshans and P. Grangier.
Reverse reconciliation protocols for quantum cryptography with continuous variables.
arXiv:quant-ph/0204127v1, (2002).

[39] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier.
Quantum key distribution using gaussian-modulated coherent states.
Nature, **421**, 6920:238–241, (2003).

[40] W.-Y. Hwang.
Quantum Key Distribution with High Loss: Toward Global Secure Communication.
Phys. Rev. Lett., **91**:057901, (2003).

[41] H. Weier.
Experimental Quantum Cryptography.
Diplomarbeit, Technical University Munich, (2003).

[42] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer and H. Weinfurter.
Free space quantum key distribution: Towards a real life application.
Fortschritte der Physik, **54**:840–845, (2006).

[43] Common criteria for information technology security evaluation, part 1: Introduction and general model, version 3.1, revision 1, (2006).

[44] Common criteria for information technology security evaluation, part 2: Security functional components, version 3.1, revision 1, (2006).

[45] Common criteria for information technology security evaluation, part 3: Security assurance components, version 3.1, revision 1, (2006).

[46] M. A. Nielsen and I. L. Chuang.
Quantum Computation and Quantum Information.
Cambridge University Press, (2001).
ISBN 0-521-63503-9.

[47] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu and A. Peres.
Qptimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy.
Phys. Rev. A, **56**, 2:1163–1172, (1997).

[48] V. Makarov, A. Anisimov and J. Skaar.
Effects of detector efficiency mismatch on security of quantum cryptosystems.
Physical Review A, **74**, 2:022313, (2006).

[49] V. Makarov and J. Skaar.
Faked states attack using detector effciency mismatch on SARG04, phase-time, DPSK, and Ekert protocols.
Quantum Information & Computation, **8**:0622, (2008).

[50] A. Lamas-Linares and C. Kurtsiefer.
Breaking a quantum key distribution system through a timing side channel.
Opt. Express, **15**, 15:9388–9393, (2007).

[51] C.-H. F. Fung, B. Qi, K. Tamaki and H.-K. Lo.
Phase-remapping attack in practical quantum-key-distribution systems.
Phys. Rev. A, **75**, 3:032314, (2007).

[52] V. Makarov and D. R. Hjelme.
Faked states attack on quantum cryptosystems.
J. Mod. Opt., **52**:691, (2005).

[53] D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu and C. W. Clark.
Detector dead-time effects and paralyzability in high-speed quantum key distribution.
arXiv:0706.1449v1 [quant-ph], (2007).

[54] V. Makarov.
Controlling passively quenched single photon detectors by bright light.
New Journal of Physics, **11**:065003, (2009).

[55] V. Makarov, A. Anisimov and S. Sauge.
Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve.
arXiv:0809.3408v2, (2009).

[56] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov.
Perfect eavesdropping on a quantum cryptography system.
arXiv:1011.0105v1, (2010).

[57] L. Lydersen, C. Wiechers, C. Wittman, D. Elser, J. Skaar and V. Makarov.
Thermal blinding of gated detectors in quantum cryptography.
arXiv:1009.2663v1, (2010).

[58] L. Lydersen, W. Carlos, C. Wittmann, D. Elser, J. Skaar and V. Makarov.
Hacking commercial quantum cryptography systems by tailored bright illumination.
Nature Photonics, **4**:686–689, (2010).

[59] C. Wiechers, L. Lydersen, C. Wittman, D. Else, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs.
After-gate attack on a quantum cryptosystem.
arXiv:1009.2683v1, (2010).

[60] C. Kurtsiefer, P. Zarda, S. Mayer and H. Weinfurter.
The breakdown flash of Silicon Avalanche diodes - backdoor for eavesdropper attacks?
Journal of Modern Optics, **48**:2039–2047, (2001).

[61] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier and H. Weinfurter.
Information leakage via side channels in freespace BB84 quantum cryptography.
New Journal of Physics, **11**:065001, (2009).

[62] H.-K. Lo, X. Ma and K. Chen.
Decoy State Quantum Key Distribution.
Phys. Rev. Lett., **94**:230504, (2005).

[63] X. Ma, B. Qi, Y. Zhao and H.-K. Lo.
Practical decoy state for quantum key distribution.
Phys. Rev. A, **72**, 1:012326, (2005).

[64] X.-B. Wang.
Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography.
Phys. Rev. Lett., **94**:230503, (2005).

[65] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A. Zeilinger and H. Weinfurter.
Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km.
Phys. Rev. Lett., **98**:010504, (2007).

[66] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam and J. E. Nordholt.
Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber.
Phys. Rev. Lett., **98**:010503, (2007).

[67] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter.
High speed optical quantum random number generation.
Opt. Express, **18**:13029–13037, (2010).

[68] V. Makarov.
Exploiting saturation mode of passively-quenched APD to attack quantum cryptosystems.
arXiv:0707.398v1 [quant-ph], (2007).

[69] T. Meyer, H. Kampermann, M. Kleinmann and D. Bruß.
Finite key analysis for symmetric attacks in quantum key distribution.
Phys. Rev. A, **74**, 4:042340, (2006).

[70] M. Hayashi.
Upper bounds of eavesdropper's performances in finite-length code with the decoy method.
Phys. Rev. A, **76**, 1:012329, (2007).

[71] R. Y. Q. Cai and V. Scarani.
Finite-key analysis for practical implementations of quantum key distri.
New Journal of Physics, **11**:045024, (2009).

[72] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth and H. Weinfurter.
Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors.
New Journal of Physics, **13**:073024, (2011).

[73] D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu and C. W. Clark.
Detector dead-time effects and paralyzability in high-speed quantum key distribution.
New Journal of Physics, **9**, 9:319, (2007).

[74] V. Burenkov, B. Qi, B. Fortescue and H.-K. Lo.
Security of high speed quantum key distribution with finite detector dead time.
arXiv:1005.0272v1 [quant-ph], (2010).

[75] H. Xu, L. Ma, J. C. Bienfang and X. Tang.
Influence of Avalanche-Photodiode Dead Time on the Security of High-Speed Quantum-Key Distribution Systems.
In: *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies*, Seite JTuH3. Optical Society of America, (2006).

[76] L. Lydersen, V. Makarov and J. Skaar.
Secure gated detection scheme for quantum cryptography.
arXiv:1101.5698v1 [quant-ph], (2011).

[77] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. G. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter and A. Zeilinger.
Entanglement-based quantum communication over 144 km.
Nature Physics, **3**:481–486, (2007).

Acronyms

APD avalanche photon detector

BRT Breitenfurterstrasse

BS beam splitter

CC Common Criteria

COW coherent one way system

CV continuous variable

ERD Erdberger Lände

FOR Siemens Forum

GUD Gudrunstrasse

ITS information theoretically secure

OSP organisational security policies

PA privacy amplification

PBS polarizing beam splitter

PNS photon number splitting

PP protection profile

QBER quantum bit error rate

QCS quantum channel switching

QKD quantum key distribution

QRNG quantum random number generator

SFR Security Functional Requirements

SiAPD Silicon avalanche photodiode

SIE Siemensstrasse

SMF single mode fiber

SPD single photon detector

ST security target

STP St. Pölten

TOE target of evaluation

TR trusted repeater