TÜV Informationstechnik GmbH

v2.0

MuQuaNet – Infrastructure security analysis

This document is based on information shared under NDA between *ID Quantique*, *TÜV Informationstechnik GmbH* and *Universität der Bundeswehr*. Do not distribute without consent!

Lucie Kogelheide	Project manager and technical expert
Dr. rer. nat. Henning Kerstan	Deputy project management
Thomas Klocke	Technical expert
Sven Bettendorf	Technical expert

March 22, 2023

Abstract

Quantum key distribution (QKD) allows two parties to establish a secret key inherently secure due to the laws of quantum mechanics. In theory, an attacker thus cannot eavesdrop on the communication without being detected. However, security proofs for QKD are based on assumptions that do not take into account imperfections of actual QKD devices. Furthermore, QKD devices have to be integrated into larger networks, resulting in additional challenges.

First commercial QKD solutions have already been developed. In order to gain experience with actual network infrastuctures using QKD, the *MuQuaNet* research project has been established. The *MuQuaNet* is a QKD test infrastructure in the Munich area that aims at connecting various locations using QKD devices from different vendors and based on different protocols. Thus, realistic network scenarios can be explored.

In the context of this report, *TÜV Informationstechnik GmbH* conducted a theoretical analysis of a certain communication scenario relevant in the *MuQuaNet*. As a result, this document sums up attack vectors relevant not only for the QKD devices themselves but also additional (classical) components of the network.

In order to use QKD in governmental use-cases, certified and tested solutions are required. As a pre-requisite, a precise understanding of network components and their interaction is required. This report aims at identifying areas for future research regarding attacks on QKD, so that remaining loopholes might be identified and closed.

Zusammenfassung

Quantenschlüsselaustausch (QKD) kann genutzt werden, um einen sicheren Schlüssel zwischen zwei Kommunikationsparteien zu etablieren. Eingeschränkt durch die Gesetzmäßigkeiten der Quantenphysik kann ein Angreifer die Kommunikation nicht abhören, ohne selbst bemerkt zu werden. Praktische Implementierungen von QKD resultieren jedoch in Abweichungen von den theoretischen Annahmen, durch die sich neue Sicherheitslücken ergeben können. Zusätzlich müssen QKD-Geräte in existierende Netzwerke integriert werden.

Erste kommerzielle QKD-Produkte sind bereits auf dem Markt verfügbar. Im Rahmen eines Forschungsprojektes wird im Raum München das *MuQuaNet* aufgebaut, eine Testinfrastruktur, in der QKD-Geräte verschiedener Hersteller zum Einsatz kommen. Ziel des Projektes ist es, QKD in einem realistischen Netzwerkszenario einzusetzen und zu testen.

Im Rahmen dieses Dokuments analysiert die *TÜV Informationstechnik GmbH* auf theoretischer Ebene ein Kommunikationsszenario, das im *MuQuaNet* Anwendung findet. Als Resultat werden mögliche Angriffsvektoren sowohl auf die QKD-Geräte selbst als auch auf andere Komponenten aufgeführt.

Um QKD auch in einem behördlichen Umfeld einsetzen zu können, ist ein genaues Verständnis des Zusammenspiels der Komponenten sowie Zertifizierung und Evaluierung einzelner Komponenten vonnöten. Dieser Bericht soll einen Beitrag dazu leisten, noch offene Handlungsfelder zu identifizieren und Angriffspfade zu schließen.

Contents

1 Introduction

1.1 About TÜV Informationstechnik GmbH

TÜV Informationstechnik GmbH (TÜViT), with registered office in Essen, is a company of *TÜV NORD GROUP*, which is one of the largest technical service providers with more than 10,000 employees and business activities in 70 countries worldwide. The IT business unit is represented by the companies TÜViT and the consulting company *TÜV NORD IT Secure Communications GmbH & Co. KG* with headquarters in Berlin.

TÜViT performs evaluation and certification activities in various national and international schemes, e.g. *Common Criteria* (CC) and corresponding ISO/IEC standards up to an *Evaluation Assurance Level* (EAL) 7.

The *Hardware Evaluation Department* of TÜViT is located in Essen. It has one of the largest hardware testing laboratories in Europe, especially focusing on performing side-channel analysis and fault injection attacks on cryptographic hardware. Trained staff and state-of-the-art lab equipment (e.g. laser fault injection stations) allow for in-depth independent security testing.

"Evaluation of quantum resistant cryptography" is a focus topic of the hardware evaluation department since 2019 with the aim of establishing procedures and updating lab equipment in such a way that quantum resistant cryptographic solutions can be tested for their physical security in commercial high security evaluations.

1.2 Implementation security for classical cryptography

Even if a cryptographic algorithm is considered secure from a theoretical viewpoint taking into account all theoretical attack vectors, actual implementations of said algorithm can suffer from additional vulnerabilities that are caused by the way the scheme is implemented. A famous example in the field of classical cryptography is Bleichenbacher's attack on the RSA encryption standard #1 v1.5 from 1998. The underlying scheme itself is not broken by the attack as it exploits an implementation error in the protocol. [1]

Furthermore, even if an implementation correctly implements a standard that is considered secure, additional attack paths open up, especially when

an attacker has physical access to the device performing the cryptographic operations. Physical attacks can largely be divided in two categories: (passive) *side-channel attacks* and (active) *fault injection attacks*.

Side-channel attacks focus on monitoring channels like timing behavior, power consumption or emanation in the electromagnetic field – although these channels are not intended to carry data-dependent information they often nonetheless do. Thus, an attacker that monitors these side-channels can obtain information about the processed secrets without interfering with the performed operations.

On the contrary, fault injection attacks describe techniques for which an attacker deliberately interferes with the performed operations, resulting in erroneous behavior that can either lead to revelation of secrets or allow an attacker to gain access without knowledge of the required secrets.

In the context of classical cryptography, security against physical attacks is a well-known prerequisite for cryptographic hardware used in a high-security context with an attacker having physical access. Typical countermeasures against side-channel attacks are masking of security-critical operations or hiding the respective operations by additional noise. Fault injection attacks can be detected by sensors or counteracted by redundant calculations and additional checks.

1.3 Implementation security for quantum resistant cryptography

When classical algorithms are replaced by *Post-Quantum Cryptography* (PQC) algorithms, comparable effort is required to secure an implementation against physical attacks. It has been shown that PQC implementations are vulnerable against side-channel and fault injection attacks just like their classical counterparts with countermeasures from classical cryptography also being applicable to PQC (for a summary see [2]).

Quantum Key Distribution (QKD) protocols are considered physically secure against eavesdropping due to the quantum-mechanical properties used in these protocols. Thus, such protocols are promising candidates for new key exchange schemes that are secure even against attackers with capabilities only limited by the laws of quantum mechanics. However, even if theoreti-

cal security of a protocol has been shown an actual implementation has to be carefully checked for flaws that open up new attack paths targeting an imperfect implementation and not the underlying protocol itself.

As QKD relies on new hardware components, research of physical attack vectors as well as appropriate countermeasures is less mature than for classical cryptography. Both fault-injection attacks as well as side-channel monitoring are valid attack paths, however, the targeted components are QKD specific, thus, attacks and countermeasures can differ from classical cryptography (and PQC).

Both passive and active attack vectors might be counteracted by mitigation techniques like filters, monitoring of components etc. Furthermore, the performed attacks might not result in a full break of the system, thus, an appropriately increased level of privacy amplification can cover up for vulnerabilities.

To further improve maturity of QKD, it is of uttermost importance to consider not only theoretical security of QKD protocols but also take into account existing imperfections of real-world implementations and devices. In order to benefit from QKD in a network scenario, potential attack paths have to be understood and evaluated. This work therefore aims at classifying vulnerable components in an exemplary QKD infrastructure, especially focusing on the QKD parts that might require different treatment than classical components.

2 The MuQuaNet

The *MuQuaNet* is a quantum communication test infrastructure in the Munich area. It aims at establishing a QKD connection between various locations.

2.1 Communication scenario

In this report, a specific communication scenario is considered. This scenario corresponds to an exemplary use-case for QKD in remote maintenance. In a real-world application this might e.g. correspond to a military use-case involving both fiber and free-space QKD connections.

At the time of writing this report, the considered connections are fiber-based QKD between the research institute *CODE* and two locations at the campus of the *Universität der Bundeswehr* as well as a free-space QKD link to *Airbus*. At this last location, a robot is located. Using QKD, a secure connection shall be established between *CODE* and *Airbus* in order to remote-control the robot.

Figure 1 depicts the considered communication scenario.

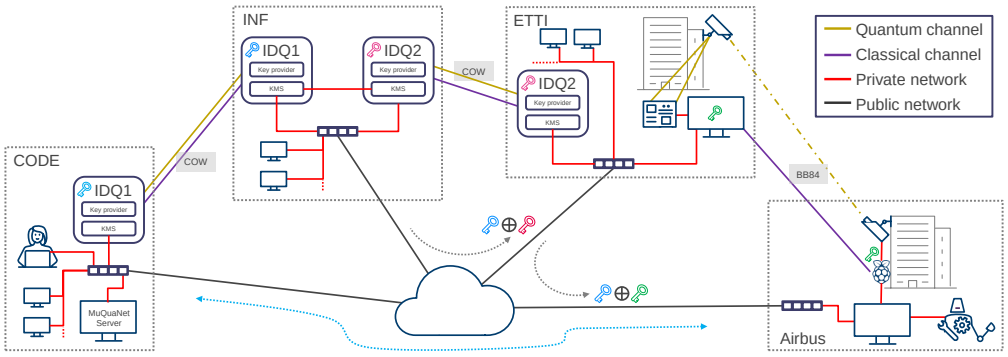

Figure 1: Schematic overview of the considered communication scenario

Adjacent locations are connected by a QKD link with both a quantum and a classical service channel. The fiber-based connections are based on the *Coherent One-Way* (COW) protocol, the free-space link uses the BB84 protocol. At the time of writing this report, all devices using COW are manufactured by ID Quantique (Clavis3). This report is centered on the examination of

devices manufactured by ID Quantique (IDQ). The operating MuQuaNet part investigated in this research exclusively employed IDQ devices, and IDQ products are also suitable due to the abundance of available literature. Moreover, IDQ provided additional information to the project collaborators during the study, enabling a comprehensive analysis. Clavis2 systems will be used as a comparison. There is already a new generation of devices called Cerberis XG(R), which are not used in the MuQuaNet. The free-space link is provided by the *Ludwig Maximilian University of Munich* (LMU).

QKD devices by ID Quantique contain both a "key provider" and an integrated *Key Management System* (KMS). The term "key provider" refers to the actual QKD part of the system providing keys derived by means of QKD. The role of the KMS is to handle interaction with the outside world, thus, addressing key management. In case of the free-space connection, control PCs used for post-processing take on the role of the KMS already integrated in ID Quantique devices. [3, p. 10]

All QKD components deliver key material according to the ETSI 014 REST-based API, a first standard for interoperability of QKD key delivery (compare Section 3.2).

For the sake of clarity, network layer 2 and 3 are not explicitly depicted in Figure 1. Each location has a *private network*, and connections to the outer world are gated by encryptors. Thus, applications within a private network as well as QKD devices have to connect to some kind of centralized controller responsible for higher layer encryption. However, in a simplified infrastructure focusing on direct data transfer, applications directly connect to the QKD devices. Both variants have been proposed for the *MuQuaNet*. [4]

QKD is used to exchange key material between the different locations, with the aim of establishing a secure communication path. Then, the robot can be remote-controlled sending commands secured by symmetric encryption with session keys derived using QKD.

As described in [5], QKD keys can be propagated through a system of trusted nodes by encrypting one key (blue key) with the next one (pink key), then sending the encrypted key over the public network. The intermediate receiver can decrypt and re-encrypt with the next QKD key (green key). This procedure is repeated until the initial QKD key has reached the final recipient. Please note that QKD channels are never used to transmit encrypted keys.

The key (= payload) is transmitted via the classical public network once it is encrypted with the derived QKD keys.

3 Protocols

3.1 Classical communication

The QKD connection is part of a larger network containing various classical connections.

It is noteworthy mentioning that classical connections require quantum resistant cryptography in order to ensure authenticity and confidentiality of data, most probably by integration of post-quantum cryptography. Integrity protection is less of a concern, as the underlying cryptographic primitives are not affected by Shor's algorithm threating classical asymmetric cryptography.

In the context of the MuQuaNet, we would like to list the following components that are specific for a network including QKD components:

- *Key Management Entity* (KME) (*Key Management System* (KMS)) to application connection ("key consumer"): Fiber-based QKD boxes by ID Quantique come with an integrated KME component, in case of the free-space connection this role is fulfilled by the control PC. The KME delivers QKD keys according to the ETSI API (see 3.2), so that applications can use these keys. [6]
- Communication between KMS nodes relies on TLS 1.2 or TLS 1.3. [7, p. 47]
- MuQuaNet server: The MuQuaNet server configures QKD devices in the network. Although no key material is directly transferred to the server, there might be the need of authenticating commands send from the MuQuaNet server to the QKD boxes.
- Service channel authentication: The service channel has to be authenticated, this is initially achieved using pre-shared keys. [8]
- Communication via the service channel is done using a proprietary ID Quantique protocol. [9]
- Various guidance documents of ID Quantique mention the use of SSL/ TLS certificates for remote configuration and maintenance of QKD systems. [7], [8], [10]

Other components of the network (e.g. classical connections to other devices

like office laptops) are not explicitly considered in this report, though they also require quantum resistant cryptographic solutions if not fully located within a secure site.

3.2 ETSI standard for key delivery

The *ETSI Industry Specification Group* (ISG) "Quantum Key Distribution" provides first standards for QKD systems, specifying interfaces and protocols.

[11] is a compact standard defining an *Application Programming Interface* (API) for creating key streams within a QKD network. This standard is "implementation agnostic", meaning that it does not depend on specific programming languages or libraries. In contrast, [12] specifies the use of the HTTPS protocol and the JSON data format. Thereby, implementation of [12] is simpler but comes with certain constraints.

Both standards serve the aim of standardizing the API between a QKD KME and applications using QKD keys.

[11] states that the API might be implemented using "secure communication methods like SSL/TSL tunnels". However, quantum resistant authentication and encryption methods between QKD link and requesting application are not demanded yet.

[12] assumes the existence of trusted nodes that are "securely operated and managed" with the API used "within a security boundary".

Considering real-world applications, additional security measures are recommended – especially in order to strengthen the trusted nodes. Potential measures would be quantum resistant authentication between applications requesting keys and the QKD link as well as encryption of the transmitted key material. If this is not provided, then care must be taken that the whole application network is within a secured site.

In order to integrate QKD systems in a classical network, a representation in the management layer is required. [13], [14] describe the information flow between QKD nodes and an *Software-Defined Networking* (SDN) controller (respectively, a subcomponent called SDN orchestrator), resulting in "network-aware QKD systems". Although no key material is transmitted from a QKD system to the controller, security measures like authentication

are required to secure communication between the components. The available ETSI-standard [13] mentions that "some initial steps [need] to be taken for authenticating" while "the description of any particular security implication and the associated solution for each one is out of the scope of the present document". Thus, it has yet to be specified how both the SDN controller and the QKD systems are secured (at the moment, the standard refers to them being installed in a "secure location") and how authentication is performed.

As a general observation, the ETSI standards heavily rely on trusted nodes and implicitly mention that e.g. additional authentication measures are required – potentially involving pre-shared secrets or post-quantum cryptography.

4 Certifiability of QKD systems

In order to enhance trust in QKD systems, a long-term goal is to achieve certifiability of QKD networks. In course of a certification process, several components are usually individually certified, involving precise description and testing of all security relevant features and interfaces.

A potential framework for certification is the *Common Criteria* (CC) framework. This international framework outlines criteria for certification of secure IT products with certificates issued by national certification authorities like the *Bundesamt für Sicherheit in der Informationstechnik* (BSI).

Important part of the required documentation is the so-called *Security Target* (ST) that specifies boundaries and functionalities of the information security system under test. STs can be derived from *Protection Profiles* (PPs) that serve as a generic blueprint of an ST for a certain product category.

4.1 Protection profile for QKD

A first PP for prepare-and-measure QKD distribution modules is available in a draft version. [15]

This PP shall serve as a basis for evaluation of actual QKD modules in the future. Relevant security considerations so far are:

- QKD modules are operated in an access controlled environment,
- Only local users have access (with a tweakable option of including remote access with additional authentication measures),
- Configuration and initialization data of QKD modules are protected by access control measures,
- Authentication of the classical channel is reached using a pre-shared *QKD Authentication Key* (QAK) which can only be (re-)provided by an administrator in a secure environment,
- Resistance against physical attacks like active probing of the QKD link or emanation revealing secret data is required,
- The "secure environment" has to resist high attack potential (detailed in [16]).

5 Potential attack vectors

In order to design and implement secure QKD systems, potential attacks and corresponding mitigation techniques have to be identified.

The following chapter therfore summarizes various attacks targeting components of the QKD infrastructure. First, the QKD device itself is considered with its different subcomponents (e.g. detector, modulator, etc.). Second, interconnections (namely, the QKD channel and the classical channel) are analyzed taking into account differences between fiber-based and free-space connections. Third, classical – but nonetheless QKD-specific – components of the systems (e.g. post-processing units, the MuQuaNet server) are considered.

Attacks on the QKD devices themseves and the interconnections (first and second subsection) are derived based on scientific publications as well as guidance and patent documentation by ID Quantique.

Studying the handbooks by ID Quantique, TÜViT identified further potential loopholes that might require additional consideration and careful choice of configuration parameters, as reported in the third subsection.

Whenever possible, corresponding mitigation techniques for an attack are also described. However, please note that countermeasures are often just proposed in the scientific literature and implementation and evaluation might still be an open action item.

Furthermore, access restriction can already be a successful mitigation for attacks requiring direct physical access to the devices. It then depends on the attacker model and assumptions regarding the secure environment whether certain potential attacks should be considered a threat or not.

Table 1 to 3 summarize the considered attacks, followed by detailed descriptions in the following sections.

QKD systems using the COW (*Coherent One-Way*) protocol are immune against various attacks due to the fact that many of the existing attacks are armed at differences between two or more signal detectors. Generally speaking, decoy-state BB84 is secure against general coherent attacks while COW and Continuous-Variable-QKD are secure against collective attacks. [17]

The crosses ("X") indicate whether an attack is explicitely applicable to

devices or protocols used in the *MuQuaNet*. The last column provides further information about vulnerable components or already included mitigation strategies.

However, please note that TÜViT cannot assess sufficiency of reported countermeasures based on literature research alone. Actual testing – most beneficially in a whitebox scenario with detailed information about the underlying hardware available – would be required to come up with such conclusions. Also, most attacks require certain sets of parameters to work. If the prerequisites are not given, then these attacks are not applicable. Comparison between prerequisites and the *MuQuaNet* infrastructure in this report are drawn based on rather general information. Whether details of the implementation enable or hinder a certain attack remains an open task for future work.

Attack	Reference	COW/ IDQ	BB84/ LMU	Note
Photon seeding attack	[18]–[20]		X	Applied to ID300 short-pulse lasers by ID Quantique
Laser-damage attack	[21]	X	X	Commercially available QKD systems use optical isolators that are considered a countermeasure
Selected photon number splitting attack	[22]–[24]		X	
Source flaw	[25], [26]		X	Loss-tolerant protocol suggested as countermeasure has been implemented with an ID Quantique ID-500 plug&play QKD system
Information side-channel leakage	[27], [28]	X	X	
Timing side-channel	[29]		X	
Trojan-horse attack	[30]–[32]	X	X	Performed for Clavis2 receiver module, Clavis3 includes bandpass and isolator as countermeasure
Phase remapping	[33]			Clavis2 by ID Quantique does not contain a phase randomizer yet
Wavelength-dependency of beam splitter	[34]		X	
Superlinearity attack	[35]	X	X	Clavis2 by ID Quantique exhibits superlinear behavior
Faked state attack	[36]	X	X	Theoretical work depicting various attack paths
Efficiency mismatch	[37]		X	
Time shift	[38]		X	
Intercept-resend attack	[39]		X	Applied to Clavis2 by ID Quantique
Exploiting dead time of detectors	[40]	X	X	Countermeasures are introduced for Clavis2 and Clavis3 by ID Quantique
Exploiting detector mismatches	[41]		X	
Backflash attack	[40], [42]–[44]	X	X	InGaAs diodes used by ID Quantique exhibit backflash behavior
Bright illumination	[45]	X	X	
Thermal blinding	[46]		X	Applied to Clavis2 by ID Quantique, still, it is stated that countermeasures are introduced

Table 1: Overview about considered attacks for QKD devices

Attack	Reference	COW/ IDQ	BB84/ LMU	Note
Zero-error attack against COW	[47]–[49]	X		ID Quantique uses four-state COW protocol as a countermeasure
Calibration attack	[50], [51]	X	X	Applied to Clavis2 by ID Quantique, but software countermeasure already proposed
Non-encrypted service channel	[52]	X	X	

Table 2: Overview about considered attacks for connections

Attack	Reference	COW/ IDQ	BB84/ LMU	Note
Classical leakage during post-processing	[53]	X	X	
Updates	[7]	X	X	
Denial of service / login	[7]	X		
Cloud integration	[3]	X		

Table 3: Overview about considered attacks for additional components

5.1 QKD devices

In case of the BB84 free space connection, the source is made up of four laser diodes, a micro-lens array, polarizers and a wave guide circuit. In case of the COW connection using commercially available ID Quantique devices, the source consists of a CW laser, intensity modulator and a variable attenuator.

In case of the BB84 free space connection, the receiver contains several beam splitters and four *Avalanche Photodiodes* (APDs) for detection of incoming photons. In case of the COW protocol, the receiver is made up of two branches, the *computational basis analyzer* and the *phase relation check*, containing couplers, Faraday mirrors and two APDs. As the detector component is made up of several single-photon detectors, the main target of side-channel attacks is to identify which photon detector actually clicked. By doing so, an attacker can recover secret information.

Fiber-based QKD with the Clavis3 by ID Quantique uses the COW protocol. As a theoretical attack ("Zero-error attack against COW protocol", described in section 5.2.1) significantly reduces the range between the QKD modules in which the original protocol can be safely executed, the Clavis3 uses COW 4-states in which an additional vacuum state is added to the protocol. [7, p. 34]

The emitter and receiver station of Clavis3 contain an optical isolator and a bandpass filter as countermeasures against Trojan-horse attacks (described in section 5.1.2). [7, p. 37]

5.1.1 Source

Photon seeding attack

Component: Source

Description: Externally injected photons affect the source and can change the phase and intensity of the resulting laser pulse. Thereby, the attacker can control the phase and intensity of the sender's signal laser. This can both decrease the security of decoy state and *Measurement-Device-Independent* (MDI-QKD) protocols. For the security of protocols that depend on weak coherent pulses and randomized phases it is possible to break the respective prerequisite. [18]–[20]

Countermeasure: Various countermeasures are applicable, however, they do not hinder the attack completely, just make the attack path more challenging:

If an optical isolator is used to prevent reflected photons from reaching the sender, the attacker can counter by increasing the power of their control laser.

An optical frequency filter removes all unwanted wavelengths, but in case that an attacker is using photons with identical wavelength this countermeasure is not effective.

An optical power meter can measure the average power of light reflected back to the sender, with the limitation that an attacker can foil this countermeasure by sending short pulses with low average power. Using a photon detector instead, detection of incident photons would be very sensitive, but this detector can be easily damaged by bright pulses. Therefore, if laser-damage attacks are not excluded, the attacker could perform a two-fold attack and first destroy the monitoring detector.

Incorporating a photon seeding attack in the previous security analysis, a potential countermeasure is reducing the secret key rate [19]

Laser-damage attack

Component: Source

Description: The majority of non-empty pulses contains a single photon that cannot be split off by an attacker and measured separately. Single photons are generated using an optical attenuator combined with a weak coherent laser as a source. If the optical attenuation component itself can be modified, thereby decreasing its attenuation (either permanently or temporarily), this assumption about the mean photon number may be broken. An attacker can then compromise the security of the QKD system. [21]

Countermeasure: The incoming light can be monitored with a separate detector in order to detect the damaging laser pulse. However, this watchdog monitor can also be attacked by laser-damage attacks. [21]

Passive components like optical isolators are reported to be used in commercially available QKD systems. However, these additional compo-

nents again have to be tested for their resistance against laser-damage attacks. [54]

An alternative countermeasure is using an optical fuse at the source output. This fuse only accepts a certain amount of power and permanently shuts off when a threshold is crossed. [21]

Selected photon number splitting attack

Component: Source

Description: Photon number splitting attacks can be countered by QKD systems using decoy states. An important assumption is that signal and decoy state are indistinguishable for an attacker. However, improved attacks can still be applicable as this assumption might be incorrect for practical QKD systems, resulting in a "selected photon-number splitting attack". Thus, although using decoy states closes the multi-photon loophole, other attack paths open up when decoy and signal state can be distinguished using side-channel information.

QKD systems that regulate the intensity of the laser diode by pump-current modulation can exhibit a timing mismatch between signal and decoy states. Therefore, the signal state and the decoy state are distinguishable. [23]

For decoy state plug-and-play QKD systems, the sender uses an intensity modulator to produce different signal strengths, thus randomly modulating the intensity of each light pulse to either the signal state level or decoy state level before sending it to the receiver. There are several kinds of intensity modulators used for decoy state protocols. These intensity modulators can introduce frequency shifts instead of pure intensity modulation under certain conditions, thereby deviating from the model in the security proofs. The decoy and signal states can then be distinguished by wavelength measurements based on wavelength division multiplex technology without error. [24]

In case that bi-directional QKD systems are used (with the receiver sending phtotons back to the sender), an atatcker can actively trigger wavelength shifting by introducing a time shift during the calibration phase. [22], [24].

Countermeasure: A potential countermeasure is monitoring of the arrival times of signal and reference pulse, thereby detecting and adjusting to mismatches introduced due to the presence of an attacker.

On top, privacy amplification reducing the secret key rate is suggested, as well as reducing the transmission range. [23]

Source flaw

Component: Source

Description: Decoy state QKD assumes perfect state preparation, not taking into account imperfections of actual sources. An attacker can deliberately disturb the source, introducing source flaws. [25]

Single laser pulses can be used instead of continuous laser pulses to make the attack less detectable. [26]

Countermeasure: Implementations of loss-tolerant protocols (modifications of BB84 and three-state QKD) have been proposed in [25], taking into account source flaws.

Information side-channel leakage

Component: Source

Description: If there are correlations of spatial, spectral or temporal properties with the actual key bit value encoded by the sender, an attacker can monitor these non-quantum side-channels to gain knowledge about the key without introducing errors. Specific side-channels for free-space BB84 QKD have been studied. [27], [28]

Countermeasure: Side-channel leakage can be reduced when individual components are carefully adjusted and manufactured in such a way that potential differences are evened out.

Timing side-channel

Component: Source

Description: In [29] an attack on entanglement-based QKD is described that exploits timing side-channels. Ideally, timing information about detection events is not correlated to the measurement outcome of a

quantum variable. However, experimental realizations of entanglement-based QKD protocols do show that timing signatures might be present. If the timing side-channel is available to an attacker (e.g. monitoring the service channel on which detection timings are communicated), an attacker can derive knowledge of secret information. In case that the BB84 protocol is used, [29] claim that the attack can be applied to the emitting unit instead.

Countermeasure: Possible countermeasures are delay equalization or delay randomization by artificially inserting wait times. [29]

5.1.2 Phase modulator

Trojan-horse attack

Component: Phase modulator

Description: Using a laser system with a very high wavelength on the quantum channel, reflections of these laser pulses are analyzed by measuring the reflected photons as they provide information about parameters used such as timing and polarization. [30] Using wavelengths outside the range usually used in telecommunication the attack can be improved. [31]

Countermeasure: Potential countermeasures are the use of wavelength filters. These are not present for Clavis2 ID Quantique devices, however, might be part of a later update. [31]

Depending on the protocol used, both sender and receiver might be vulnerable to Trojan-horse attacks (e.g. when using the SARG04 protocol). The receiver's side can be addressed by using a QKD protocol that does not require the receiver's phase modulator settings to be secret, such as BB84 with decoy states. [31], [32]

Phase remapping

Component: Phase modulator

Description: An important assumption for the safety of the BB84 QKD protocol is the absolute randomization of the phase. In practical QKD systems, this is achieved by actively randomizing the phase of the source using a phase modulator.

However, in practice it is difficult to test for the involved parties whether full randomization has been achieved. Commercially available QKD systems by ID Quantique are reported to rely on the assumption that the phase is randomized.

An attacker can intercept all pulses introducing a small timing shift. Then, the phase is no longer absolutely random but only partially modulated in a reduced range. When successful, the attacker can compromise the generated key. [33]

Countermeasure: The receiver can use a pulse homodyne detector to reconstruct the probability distribution of the signal pulse to detect the presence of an attacker.

Phase remapping attacks are applicable to the decoy state QKD protocol. However, the attack cannot be applied to the vacuum+weak decoy state method in which the sender sends three kinds of pulses: the signal state, the decoy state and the vacuum state. [33]

5.1.3 Detector

Wavelength-dependency of beam splitter

Component: Detector

Description: Beam splitters are usually made from fused biconical taper and are therefore wave-length dependent. The attacker must have the same detection setup as the receiver, then, performs a man-in-the-middle attack. The transmitted photons are intercepted, analyzed, remodulated and then retransmitted with a different wavelength. By exploiting the wavelength-dependent behavior of the beam-splitter the attacker gains information about the receiver's detection events (at the cost of an increased quantum bit error rate from 1.3% to 1.4% the attacker has control over the bases the receiver chooses). [34]

Countermeasure: Introducing wave-length filters is not a sufficient countermeasure, as an attacker could react with light pulses of increased intensity.

Using actively modulated phase encoding QKD systems with the receiver actively choosing their measurement basis hinders the attack. [34]

Superlinearity attack

Component: Detector

Description: Most QKD detectors are threshold detectors that can only detect no and "one or more" photons in a pulse. A detector with increased probability to detect multiple photons (instead of single photon events) is called a "superlinear threshold detector". The attacker intercepts the communication and measures the incoming pulse. Then, the attacker resends the pulse but not as a single photon but as a bright "trigger" pulse. Due to superlinearity of the detector, the incoming pulse is detected with nearly 100 % probability if the attacker's base matches the receivers base and not detected when the bases do not match. This behavior can lead to full key recovery. [35]

Countermeasure: It is challenging to counter the attack with additional detectors as the attack can be carried out with as little as 120 photons. The most promising countermeasure is to improve the underlying security models resulting in increased privacy amplification. [35]

Faked state attack

Component: Detector

Description: The attacker exploits imperfections in the detection unit, e.g. imperfections of beam splitters. Thus, the attacker is able to force the detection result of the receiver. The attacker intercepts the communication and resends a light pulse to the receiver that is perceived to be an original quantum state. While detection results seem normal, basis and bit value chosen are controlled by the attacker.

The attack descriptions in [36] come from a theoretical viewpoint and offer a rather generic overview of faked state attacks. Various imperfections can and have been attacked with specifically targeted attacks (described in the following paragraphs).

Countermeasure: In principle, faked state attacks can be countered by careful monitoring of the detector components. Furthermore, additional design and manufacturing steps can reduce imperfections of the detector that are a pre-requisite for the attack. [36]

Efficiency mismatch

Component: Detector

Description: For free-space QKD, an important assumption is the symmetry of detection efficiency between all received quantum states in the receiver's detector. However, practical implementations of free-space QKD might suffer from efficiency mismatches, opening up an attack path (compare *Faked state attack*).

An attacker sending light pulses under specific angles exploits different click probabilities of the detectors. Thereby, as an attacker can control the spatial mode of the incoming photons, the receiver's measurement results are influenced in such a way that they match the attacker's basis choice. [37]

Countermeasure: Additional detectors can reduce the probability of undetected light injection. However, this does not fully hinder the attack, just increases the effort for the attacker. [37]

Time shift

Component: Detector

Description: The time-shift attack exploits the detection efficiency mismatch between two detectors in a QKD system in the time domain. The detection window for bit "0" is different to the detection window for bit "1". With a timing bias introduced by the attacker the incoming pulses are manipulated towards one outcome at the receiver. [38]

Countermeasure: Further manufacturing steps can reduce timing differences between individual detectors. [38]

Intercept-resend attack

Component: Detector

Description: [39] reports an experimental realization of faked state attacks targeting a Clavis2 by ID Quantique. The attacker sends irregular bright light pulses to the receiver that trigger detection events outside the activation window with only a slight increase in the quantum bit error rate.

Considering the long path from the free-space receiving unit to the detectors (from the rooftop to the lower parts of the building) it might be feasible to inject light pulses directly in these fiber connections in the specific build-up of the MuQuaNet, especially as these four fiber connections hold a single detectors basis each. Therefore, the quantum mechanical security would not be given any more.

Countermeasure: The attack can be detected by analyzing the statistics of the detection events. As the bright light pulses are applied outside the detection windows, closely related detection events (smaller than the dead time) indicate that an attack took place.

If detection events within the dead time are rejected, the attack gets more complicated but is still applicable.

Using a watchdog detector, bright pulses can be detected. However, when the incoming fake pulses have low intensity, this countermeasure is not sufficient. [39]

Exploiting dead time of detectors

Component: Detector

Description: After a detection event, single-photon detectors exhibit a dead time in which no detection can occur. An attacker that knows that one detector is within its dead-time can apply fault injection to manipulate the generated secrets. Information about the inactive detector might be gained from the service channel waiting for the device announcing that a qubit has been received.

Countermeasure: Commercially available ID Quantique devices (Clavis2, Clavis3) apply the same dead-time to all detectors, i.e. when one detector clicks, the dead-time has to pass by before another photon can be detected. [40]

If external detectors are used with potentially unknown or uncontrollable dead-times, then a wait time (buffer unit) can be artificially introduced to incorporate dead-times. [40]

5.1.4 Detector / optical path to detector

Exploiting detector mismatches

Component: Detector / optical path to detector

Description: Due to small differences in path length as well as imperfections in detector manufacturing two photodiodes or detection windows might have different detection characteristics. This allows an attacker to mount a variant of the faked state attack forcing their states on the receiver without being detected. [41]

Countermeasure: The attack can be countered by monitoring detector characteristics, such as the sensitivity. Furthermore, timing of the incoming pulses at the receiver can be checked.

Another countermeasure is to add random delays ("jitter") to lower the mismatch between individual detectors by artificially introducing a much larger timing effect.

Additional privacy amplification might be required.

Not all protocols are affected, e.g. the B92 protocol that only uses one individual detector is not vulnerable, as well as modifications of the BB84 protocol using only one individual detector. [41]

5.1.5 Avalanche photodiode (APD)

Backflash attack

Component: Avalanche photodiode

Description: With certain probability, APDs used for detection emit photons back into the channel (*backflashed photons*). By measuring the backflashed photons, an attacker can identify which single-photon detector clicked. This behavior has been experimentally studied in [42], [43] for silicon avalanche diodes. For QKD devices, InGaAs diodes are more common (e.g. used by IDQuantique according to [40]). It has been shown in [44] that these kinds of detectors exhibit the same behavior.

Countermeasure: The probability of backflash events can be reduced using spectral and spatialmode filtering [42][43][44]).

There are detectors that are less likely to emit backflash light at all (e.g. superconducting-nanowire single-photon detectors according to [44] – these, however, require cryogenic cooling).

Measurement-device-independent QKD protocols (MDI-QKD) are not vulnerable to this attack – however, these are challenging to implement at least for free-space QKD connections due to atmospheric turbulences [43].

Bright illumination

Component: Avalanche photodiode

Description: APDs are operated in Geiger mode to detect single photons. By applying bright light pulses they are forced into their linear regime in which an attacker can eavesdrop on the communication. [45]

Countermeasure: Additional detectors can be used to detect bright light pulses (according to [45], ID Quantique devices implement countermeasures against bright light attacks).

Thermal blinding

Component: Avalanche photodiode

Description: Bright illumination can be used to heat up detector componentes, resulting in so-called *thermal blinding*. Commercially available QKD-systems like Clavis2 have been subject of the respective attack. [46]

Countermeasure: Countermeasures like an additional detector or monitoring the APD parameters are deemed insufficient in [46]. A possible solution is the use of quantum detectors which are operated in the linear regime. According to [46], IDQuantique implemented countermeasures against the attack.

5.2 Connections

5.2.1 Quantum channel

Zero-error attack against COW

Component: Quantum channel

Description: Zero-error attacks do not alter the optical mode of the transmitted signal, thus, this kind of attack does not introduce errors. The attacker intercepts the quantum channel and uses unambiguous state discrimination (USD) measurements to analyze the received pulses. Not all pulses are resend, but replaced by vacuum states when a measurement outcome received by the attacker is inconclusive. As a result, security proofs for COW based on coherence analysis have to be adjusted. [47] describes an improved zero-error attack against the COW protocol that significantly limits the maximum achievable distance for secure key exchange to 22 km.

Countermeasure: The attack is possible because the receiver can only check coherence of adjacent pulses. As a countermeasures, the receiving side could be modified in such a way that it can also measure coherence between nonadjacent pulses.

As the attacker does not resend all pulses, monitoring the detection rates for irregularities can lead to detection of the attack. [47]

Increasing the number of signal states emited by the sender reduces the success probability of the attack. [47], [48]

Since Q4 2021, ID Quantique devices use 4-state COW protocol, which extends the secure range to medium distances (100 km). [49, p. 49]

Calibration attack

Component: Quantum channel

Description: This man-in-the-middle attack focusses on the calibration phase between two QKD devices, thus hindering secure establishment of the QKD channel. The attacker intercepts all calibration signals and resend fake calibration signals. [50]

Feasibility of this attack has been experimentally verified [51]

Countermeasure: Intercepting the quantum channel changes arrival time for pulses. Thus, careful monitoring of detector activation timings and signal arrival timing can serve as a countermeasure. [50]

ID Quantique suggested a (software) modification that fixes the calibration routine of the Clavis2 QKD system. [51]

5.2.2 Service Channel

Non-encrypted service channel

Component: Service channel

Description: QKD protocols contain of a quantum communication phase followed by a classical post-processing phase. As part of this post-processing phase, integrity of the messages transmitted on the classical channel is performed. The standard approach of ensuring integrity of messages is to use *Message Authentication Codes* (MAC). These MACs are transmitted as tags together with the messages and then checked for correctness.

MACs have a non-zero collision probability, thus, an attacker that is able to find collisions can replace messages in the classical channel. [52]

Countermeasure : As the service channel is only authenticated but not encrypted, the attacker can intercept and analyze messages and corresponding MACs. A potential countermeasure is encryption of the service channel. Another countermeasure is to use more sophisticated, two-step authentication methods thereby increasing the computational effort for the attacker. [52]

5.3 Additional Components

5.3.1 Classical Hardware

Various components used to perform the QKD protocol are classical hardware, e.g. the control PC performing pre- and post-processing.

Classical leakage during post-processing

Component: Unhardened classical hardware

Description: An example for a successful side-channel attack is described in [53]. The attacked post-processing step is the final key reconciliation involving a syndrome computation. By measuring the power consumption of the involved classical hardware, an attacker can recover the sifted key.

Countermeasure: Classical countermeasures like randomization of the performed calculation apply. Furthermore, adding noise to the power side-channel by running other components during sensitive operations can decrease the attack success probability.

5.3.2 MuQuaNet Server

Updates

Component: MuQuaNet server

Description: To exclude that compromised software updates of server components are accepted – e.g. compromised docker images [7, p.26] – integrity of update files has to be fulfilled and checked.

Countermeasure: Signature-based update mechanisms like Docker Content Trust (DCT) can be used.

Denial of service / login

Component: MuQuaNet server

Description: User accounts are locked after providing an incorrect password three times [7, p.41]. Therefore, it might be possible for an attacker to lock out all users so that no user is left who can remotely reboot the system and reset the console. As a result, a manual reboot would be required.

Countermeasure: Instead of a strict user login ban after three incorrect login attempts brute force attacks can also be countered by an increasing dead time after each incorrect login attempt. This would not lock the whole login system completely.

Cloud integration

Component: MuQuaNet server

Description: According to the IDQ User Guide, the QNET.WebAPI, which acts as a QKD network controller, report their logs, instruments and events to *Microsoft Azure Monitor* (only if activated explicitely), which in certain configurations hosts that data externally. This could be a security issue if logs contain sensitive data. Furthermore, activating the KMS/QKD log forwarding to *Syslog Server* could open a similar loophole. [3, p.28, 31]

6 Conclusion

The overview provided in this report shows that attacks against practical implementations of QKD are a concern with currently available countermeasures often not completely hindering an attack. Thus, detailed modelling of real-world devices is required in order to incorporate implementation flaws in security proofs. Considering commercial devices by ID Quantique, most attacks have been carried out on the Clavis2 platform with the claim that countermeasures are already introduced in the Clavis3. It could be a focus of future research to repeat older attacks on the Clavis3, verifying that countermeasures are indeed sufficient or deriving additional improvements or to repeat them for other systems in the MuQuaNet by other vendors, to see whether they are secured against these attacks.

As trusted nodes are needed to build a QKD network (at least until quantum repeaters are available) it is advisable to make the boundary of said node as small as possible (e.g. excluding office laptops but only including the server room). Access control measures have to be implemented to hinder physical access to the QKD devices. Furthermore, hardware-hardening techniques from classical cryptography also seem to be applicable against various QKD attacks. Such countermeasures from classical cryptography include – but are not limited to – the use of additional detection mechanisms for tamper-resistance or further manufacturing steps to even out side-channel characteristics. As side-channel attacks like monitoring the power consumption are already well-studied for implementations of classical algorithms it is advisable to study mitigation techniques that are used in this field. By doing so, countering an attacker with limited physical access becomes possible, thus, leading to more realistic assumptions about attack potential.

In the context of governmental or critical infrastructure the use of tested and certified components is required. However, standardization efforts are still in progress and currently available schemes like *Common Criteria* have not been extended yet. It is also noteworthy to mention that security testing in such evaluation processes is usually conducted in a whitebox scenario taking into account an attacker with high attack potential and knowledge about details of the product they are attacking. This would require not only hardened products but also more detailed information about implementation characteristics in constrast to the already available documentation studied for this report.

Reviewing current ETSI standards as well as the available *Protection Profile* draft it becomes evident that huge assumptions are placed on the environment in which devices are operated, often excluding physical access. When these assumptions could be lifted due to better countermeasures, challenges in securely operating devices could be overcome.

Another important aspect in a heterogeneous infrastructure is the question of how to secure classical connections within one local site or between different sites in a quantum resistant manner. Some connections might only require authentication and integrity of data, but when keys are transferred to applications using them, confidentiality is a concern, too. Therefore, it can be expected that in the long run QKD systems are going to be integrated in combination with post-quantum cryptography. For non-proprietary protocols, e.g. TLS, implementation of PQC surely is not going to be the sole concern of QKD developers alone. However, as also proprietary protocols are used (e.g. for the service channel) QKD developers might face the challenge of additionally having to implement PQC in their products.

A References

[1] D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1," in *Advances in Cryptology — CRYPTO '98*, H. Krawczyk, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 1–12.

[2] TÜV Informationstechnik GmbH, "Whitepaper Post-Quantum Security," 2020.

[3] ID Quantique SA, "Cerberis3, Clavis3, Cerberis XG – QNET User Guide," 2021, Version 1.6.

[4] U. M, "MuQuaNet – The quantum network in the Munich area," 2022, Presentation.

[5] S. Kastrup, "Ende-zu-Ende-Verschlüsselung unter Nutzung des Quantenschlüsselaustauschs," *Master Thesis*, 2021.

[6] ID Quantique SA, "Cerberis3 & Clavis3 – KMS Configuration Guide," 2020, Version 1.7.

[7] ID Quantique SA, "Quantum Key Distribution System Clavis3 – User Guide," 2021, Version 2.8.

[8] ID Quantique SA, "QNET shell User Manual," 2021, Version 1.3.

[9] ID Quantique SA, "Quantum Key Distribution Training CerberisXG," 2021, Version 3.0.3.

[10] ID Quantique SA, "IDQ QKD – QMS User Guide," 2021, Version 1.1.

[11] ETSI Group Specification QKD 004, "Application Interface," 2020, Version 2.1.1.

[12] ETSI Group Specification QKD 014, "Protocol and data format of REST-based key delivery API," 2019, Version 1.1.1.

[13] ETSI Group Specification QKD 015, "Control Interface for Software Defined Networks," 2022, Version 2.1.1.

[14] ETSI Group Specification QKD 018, "Orchestration Interface for Software Defined Networks," 2022, Version 1.1.1.

[15] ETSI Group Specification QKD 016, "Common Criteria Protection Profile Pair of Prepare and Measure Quantum Key Distribution Modules," 2021, Version 0.6.2.

[16] Joint Interpretation Library, "Minimum Site Security Requirements," 2019, Version 2.2.

[17] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 16025, 2016.

[18] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," *Physical Review A*, vol. 92, no. 2, p. 022 304, 2015.

[19] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," *Physical Review Applied*, vol. 12, no. 6, p. 064 043, 2019.

[20] X.-L. Pang, A.-L. Yang, C.-N. Zhang, *et al.*, "Hacking quantum key distribution via injection locking," *Physical Review Applied*, vol. 13, no. 3, p. 034 008, 2020.

[21] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, "Laser-damage attack against optical attenuators in quantum key distribution," *Physical Review Applied*, vol. 13, no. 3, p. 034 017, 2020.

[22] M.-S. Jiang, S.-H. Sun, C.-Y. Li, and L.-M. Liang, "Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states," *Physical Review A*, vol. 86, no. 3, p. 032 310, 2012.

[23] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, "Quantum key distribution with distinguishable decoy states," *Physical Review A*, vol. 98, no. 1, p. 012 330, 2018.

[24] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ""Plug and play" systems for quantum cryptography," *Applied physics letters*, vol. 70, no. 7, pp. 793–795, 1997.

[25] F. Xu, K. Wei, S. Sajeed, *et al.*, "Experimental quantum key distribution with source flaws," *Phys. Rev. A*, vol. 92, p. 032 305, 3 2015.

[26] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 92, 2015.

[27] 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*, vol. 11, no. 6, p. 065 001, 2009.

[28] A. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, "Experimental side channel analysis of BB84 QKD source," *IEEE Journal of Quantum Electronics*, vol. 57, no. 6, pp. 1–7, 2021.

[29] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Express*, vol. 15, no. 15, pp. 9388–9393, 2007.

[30] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New Journal of Physics*, vol. 16, no. 12, p. 123 030, 2014.

[31] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, "Invisible Trojan-horse attack," *Scientific Reports*, vol. 7, 2017.

[32] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[33] S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, "Partially random phase attack to the practical two-way quantum-key-distribution system," *Phys. Rev. A*, vol. 85, 2012.

[34] H.-W. Li, S. Wang, J.-Z. Huang, *et al.*, "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," *Physical Review A*, vol. 84, no. 6, 2011.

[35] L. Lydersen, N. Jain, C. Wittmann, *et al.*, "Superlinear threshold detectors in quantum cryptography," *Physical Review A - PHYS REV A*, vol. 84, 2011.

[36] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

[37] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," *Physical Review A*, vol. 91, no. 6, 2015.

[38] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A*, vol. 78, no. 4, 2008.

[39] C. Wiechers, L. Lydersen, C. Wittmann, *et al.*, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, no. 1, p. 013 043, 2011.

[40] ID Quantique SA, "Detector dead time effect in qkd systems," European Patent 3562088A1, Okt. 2017, Withdrawn.

[41] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022 313, 2 2006.

[42] C. Kurtsiefer, P. R. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?" *Journal of Modern Optics*, vol. 48, pp. 2039–2047, 2001.

[43] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, *et al.*, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," *Opt. Express*, vol. 26, no. 16, pp. 21 020–21 032, 2018.

[44] A. Meda, I. Degiovanni, and A. e. a. Tosi, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," *Light: Science & Applications*, vol. 6, e16261, 2017.

[45] L. Lydersen, C. Wiechers, and C. e. a. Wittmann, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, 2010.

[46] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," *Opt. Express*, vol. 18, no. 26, pp. 27 938–27 954, 2010.

[47] R. Trényi and M. Curty, "Zero-error attack against coherent-one-way quantum key distribution," *New Journal of Physics*, vol. 23, no. 9, p. 093 005, 2021.

[48] R.-Q. Gao, Y.-M. Xie, J. Gu, *et al.*, "Simple security proof of coherent-one-way quantum key distribution," *Optics Express*, vol. 30, no. 13, pp. 23 783–23 795, 2022.

[49] ID Quantique SA, "Security Analysis of QKD: From Qubits to Secure Keys," 2021, Presentation MuQuaNet Seminar.

[50] Y.-Y. Fei, X.-D. Meng, M. Gao, H. Wang, and Z. Ma, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," *Scientific Reports*, vol. 8, no. 4283, 2018.

[51] N. Jain, C. Wittmann, L. Lydersen, *et al.*, "Device Calibration Impacts Security of Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 107, p. 110 501, 11 2011.

[52] C. Pacher, A. Abidin, T. Lorünser, *et al.*, "Attacks on quantum key distribution protocols that employ non-ITS authentication," *Quantum Information Processing*, vol. 15, no. 1, pp. 327–362, 2016.

[53] D. Park, G. Kim, D. Heo, S. Kim, H. Kim, and S. Hong, "Single trace side-channel attack on key reconciliation in quantum key distribution

system and its efficient countermeasures," *ICT Express*, vol. 7, no. 1, pp. 36–40, 2021.

[54] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Phys. Rev. X*, vol. 5, p. 031 030, 3 2015.

[55] A. Klee, "Schlüssel-Management und Verschlüsslungsverfahren im Kontext eines Quantenkommunikationsnetzwerks," *Master Thesis*, 2021.

[56] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Physical Review Letters*, vol. 85, no. 6, pp. 1330–1333, 2000.