Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Implementation Attacks against QKD Systems

Document History

Version	Date	Description
0.9	18.09.2023	Initial version
1.0	21.11.2023	Changes after referee's feedback

Authors

(in alphabetical order, with project management listed first)

Prof. Dr. Christoph Marquardt, Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Dr. Ulrich Seyfarth, BearingPoint GmbH, Germany
Sven Bettendorf, TÜV Informationstechnik GmbH, Germany
Dr. Martin Bohmann, Quantum Technology Laboratories GmbH, Austria
Alexander Buchner, Quantum Technology Laboratories GmbH, Austria
Prof. Dr. Dr. Marcos Curty, Universidad de Vigo, Spain
Dr. Dominique Elser, Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Silas Eul, Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Prof. Dr. Tobias Gehring, Danmarks Tekniske Universitet, Denmark
Dr. Nitin Jain, Danmarks Tekniske Universitet, Denmark
Thomas Klocke, TÜV Informationstechnik GmbH, Germany
Marie Reinecke, BearingPoint GmbH, Germany
Nico Sieber, BearingPoint GmbH, Germany
Dr. Rupert Ursin, Quantum Technology Laboratories GmbH, Austria
Dr. Marc Wehling, TÜV Informationstechnik GmbH, Germany
Dr. Henning Weier, Quantum Space Systems GmbH, Germany

Acknowledgements

The Federal Office for Information Security and the authors wish to express their gratitude in particular to Eleni Diamanti, Hoi-Kwong Lo, Renato Renner, and Harald Weinfurter for providing their valuable feedback regarding the analysis of implementation attacks in this document.

We would also like to thank all the other referees for their time and effort in supporting this analysis with their valuable feedback, namely, Davide Bacco, Poompong Chaiwongkhot, Chris Erven, Tobias Fehenberger, Florian Fröwis, Kevin Füchsel, Anqi Huang, Michael Kasper, Imran Khan, Michael Kues, Christian Kurtsiefer, Thomas Länger, John Leiseboer, Charles Ci Wen Lim, Alexander Ling, Marco Lucamarini, Christopher Pacher, Momtchil Peev, Andreas Poppe, Bing Qi, Hao Qin, Joshua A. Slater, Pino Vallone, Nino Walenta, Guntram Wicke, Feihu Xu, Haw Jin Yan, Zhiliang Yuan, and Hugo Zbinden.

BSI Reference

BSI Title: Implementation Attacks against QKD Systems
BSI Project Number: 575

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: quantum@bsi.bund.de
Internet: https://www.bsi.bund.de

Contents

List of Abbreviations

ADC analogue to digital converter

AOPP actively odd-parity pairing

APD avalanche photo detector

BS beamsplitter

CEM Common Criteria Methodology

CfQKD counterfactual quantum key distribution

CHSH Clauser-Horne-Shimony-Holt

COW coherent-one-way

CV-QKD continuous-variable quantum key distribution

CW continuous wave

DI-QKD device-independent QKD

DOF degree of freedom

DPS differential-phase-shift

DV-QKD discrete-variable quantum key distribution

DVFS dynamic voltage and frequency scaling

FM Faraday mirror

FPGA field programmable gate array

FWHM full-width half-maximum

GMCS Gaussian-modulated coherent state

GPU graphics processing unit

HOM Hong-Ou-Mandel

HWP half-wave plate

IM intensity modulator

LDPC low-density parity check

LO local oscillator

MDI measurement-device-independent

MDI-QKD measurement-device-independent QKD

OSSB optical single-sideband modulation

P(I)N positive (intrinsic) negative

PBS polarising beamsplitter

PCCA phase-covariant cloning attack

PM phase modulator

PMT photo multiplier tube

PNS photon-number-splitting

POVM positive operator-valued measure

QBER quantum bit error ratio

QD quantum dot

QKD quantum key distribution

QND quantum non-demolition

QWP quarter-wave plate

RDI receiver-device-independent

RF radio frequency

SD self-differencing

SNS sending or not-sending

SNSPD superconducting nanowire single photon detector
SPD single-photon detector
SPDC spontaneous parametric down-conversion
SVR support vector regression
TES transition-edge sensor
TF twin-field
TF-QKD twin-field QKD
THA Trojan-horse attack
TOE target of evaluation
USD unambiguous state discrimination
VOA variable optical attentuator
WDM wavelength-division multiplexer

1 Introduction

Most key agreement schemes in use today base their security on the assumed hardness of mathematical problems such as those based on prime factorisation or discrete logarithms. However, these problems can be efficiently solved by large-scale quantum computers once they become available. Therefore, new key agreement schemes on classical computers have been developed. These schemes base their security on the assumed hardness of mathematical problems believed to be hard to solve for both classical and large-scale quantum computers. This is the field of post-quantum cryptography.

A different solution proposed for quantum-safe key agreement is quantum key distribution (QKD). In contrast to the conventional methods based on classical and post-quantum cryptographic mechanisms, the theoretical security of QKD is based on principles of quantum physics rather than mathematical complexity assumptions. However, its implementation requires specialised hardware. For more background on the quantum threat, post-quantum cryptography, and QKD, see BSI publication “Quantum-safe cryptography” [**BSI-quantum_safe**].

Practical implementations of QKD have made rapid advances in the last two decades. Besides a rigorous understanding of the theoretical security of QKD protocols, it is crucial to also mitigate attacks that exploit imperfections in practical implementations not covered by the theoretical model. Such attacks on QKD implementations are the focus of this document.

1.1 Definition and Scope

Implementations of QKD, commonly also called QKD systems, are in essence cryptographic systems that solve the task of key agreement. This document carries the term “implementation attacks” in its title as it provides a comprehensive overview of attacks that can be launched against implementations of QKD. A common denominator to all these attacks is the deviation between the theoretical description of the QKD system and the physical implementation. Such deviations might open security loopholes that can be exploited by an attacker to break the security of the key agreement scheme, i.e., allow the attacker to gain information about the key that might be significantly larger than what the QKD users expect, if the attacks are not properly taken into account.

While conventionally used cryptographic technologies such as hardware security modules or secure networking protocols that are a part of the QKD system may also be targeted by an attacker to achieve the same goal, this document exclusively covers attacks on QKD-specific components. From that perspective, for most attacks considered in this document, the attacker interested in gaining knowledge of the key must launch the attack (on the QKD equipment and/or the connecting channels) during the communication phase: Once the keys have been established, the security of the key agreement scheme cannot be broken retroactively.

The document is structured as follows: Chapter 2 contains background material on QKD which includes the relevant devices and components used in typical QKD systems and other specific technical terminology. Chapter 3 outlines the structure and methodology of the analysis to be performed on the implementation attacks. Various factors and how they motivate the derivation of a quantitative comparison between any two given attacks, i.e., attack ratings, are explained. A “template” that tabulates different aspects of a typical attack is also presented. In Chapter 4, which constitutes the core of this document, every attack (or a class of attacks) covered in this study is explained in depth in its respective attack table, formatted according to the template (depicted in Table 3.1). Information about countermeasures, or mechanisms proposed to prevent the attack, is also provided in these tables. A concerted effort was made to confine any expert opinion, namely remarks from the authors of this document that provide information beyond what is contained in the literature, under a 'Remarks' field in each table[1]. The last section of this chapter (Section 4.5) contains a compiled list of countermeasures found to be sufficiently general to be applicable to several attacks. Chapter 5 provides a summary and concludes the analysis.

1.2 Limitations

At the time of the creation of this document, the field of QKD is more under scientific exploration than commercial exploitation. Most of the publications dealing with attacks as well as countermeasures have been proof-of-concept works in one or several ways. Primarily, these attacks have been researched and executed in university laboratories, which can have access to highly specialised equipment but do not necessarily aim (or have the resources) to mount the fastest, cheapest and easiest method to implement the proposed attack[2]. In many cases, the QKD systems—on which the attacks have been proposed and/or implemented—are basic lab setups with only a limited number of functionalities. Furthermore, there are several ways of implementing QKD, and attacks on some categories of QKD systems have been scrutinised far more than others. As a consequence, the implementation attacks covered in this document reflect only the current state of knowledge, and given that the research field is still quite active, no claims of completeness or future predictions are possible.

In particular, there is currently not enough scientific literature to compare the effectiveness of two or more countermeasures proposed to prevent the same attack. This document surveys the various countermeasures that have been proposed in the literature, but an assessment of their effectiveness is beyond its scope and requires more research.

This document makes a first attempt at quantifying the effort required by an adversary to conduct an attack. To this end, an attack rating is provided. Due to the current state of research indicated above, there is still a fair bit of uncertainty in the determination of a rating for most attack classes. Furthermore, the attack ratings are provided independent of the physical implementation of the quantum channel between the QKD transmitter and QKD receiver, as their numerous variations and their individual vulnerabilities would go beyond the scope of the analysis. The ratings also do not take into account any of the countermeasures proposed to prevent that attack, given the current state of the knowledge base on countermeasures and their effectiveness (as highlighted above). To summarise, this document

- surveys countermeasures proposed in the literature, but does not assess their effectiveness,
- provides attack ratings which are not to be taken as authoritative, and
- is not intended to be used for the evaluation of concrete products.

[1] Although in some cases, it was necessary to consciously abandon this guideline to ensure validity and a complete description of the respective attack.

[2] The product cycles of commercial QKD implementations with typical lifetimes of few years paired with high upfront costs for universities to invest in investigating attacks with unknown or poor scientific perspectives make the academic exploitation of implementation attacks unattractive.

2 Background

2.1 Introduction

As one of the most widely used applications of quantum technology today, QKD solves the well-known cryptographic problem of providing keys—sequences of random bits—to users across an insecure communication channel. The keys can later be used for cryptographic tasks such as encryption. Confidential messages can then be securely communicated by the users, i.e., the information content of their messages can be protected from the prying eyes of the adversary. The requirements are that the encryption and decryption algorithms employed by the users are secure, and that the key (used for encryption and decryption of the message) is secret, i.e., not known to anyone except the sender and receiver of the message.

In this chapter, a brief refresher on the main elements of QKD relevant to this document is given. For further details on any of the subtopics below, the reader is referred to several excellent reviews [**Gisin2002**, **Scarani2009**, **Lo2014**, **Pirandola2020**, **Xu2020**, **Portmann2022**]. Since QKD is both a cryptographic and communication application, the terms **Alice** & **Bob** and **transmitter** & **receiver**, respectively, will be interchangeably used for describing QKD users throughout this document. Similarly, the adversary will be addressed as **Eve** or **attacker/eavesdropper**.

2.2 QKD Systems, Protocols, and Channels

The two main ingredients that enable QKD users to obtain identical yet completely random strings of bits, i.e., the symmetric and shared secret keys, are quantum correlations and quantum measurements. The act of a quantum measurement is responsible for the quantum-to-classical transition, yielding Alice and Bob with correlated bit sequences. Eve's attempts to gain any non-negligible knowledge of the secret key (by means of eavesdropping) degrades these correlations. Alice and Bob can quantify these actions by Eve, and the length of the secret key they can eventually obtain can be understood to be proportional to the degraded correlations. In the worst case, the secret key length drops to zero when the amount of eavesdropping exceeds a certain threshold. In that case, Alice and Bob cannot exchange encrypted messages (due to the lack of a key), however, the confidentiality of all of their messages remains intact.

As of today, photons are the only reliable candidates for distributing quantum correlations across long distances. From a physical perspective, the aforementioned insecure communication channel is thus either an optical fibre or an atmospheric/free-space link. The QKD systems connected by such "quantum channels" are physically realised as optical setups that are capable of encoding and decoding quantum-optical information. The coding happens in a certain degree of freedom (DOF) or property of the photons; this is covered in more detail in Section 2.3.

In the terminology of quantum information physics, quantum states of light are prepared, measured, and transmitted over the quantum channel. The most intuitive picture of a QKD scheme is similar to that of a conventional optical communication system, comprising a transmitter and receiver. The correlations in such prepare-and-measure schemes are obtained indirectly by utilising randomness and quantum measurements. Correlations can also be more directly obtained using entangled states of light and quantum measurements in so-called entanglement-based schemes [**Gisin2002**, **Scarani2009**, **Portmann2022**].

The reason why an eavesdropper cannot simply obtain the same correlations as the transmitter and receiver is due to the non-orthogonality property of quantum states and the no-cloning theorem. The non-orthogonality property brings in a fundamental indeterminacy in being able to successfully distinguish between two unknown quantum states. And given a randomly chosen quantum state from a set of non-orthogonal quantum states, the no-cloning theorem prohibits Eve from creating perfect clones of that quantum state.

The steps of preparation and/or measurement of quantum states constitute the first stage of a "QKD protocol". Typical optical and optoelectronic hardware needed for this purpose is described in Section 2.4. The next stage of the QKD protocol, following the quantum measurement (which happens at the quantum-classical interface), involves the establishment and processing of the classical correlations, i.e., correlations of bit sequences. In the information reconciliation step, Alice and Bob correct for errors that may have occurred due to loss and/or noise (either of which could also be controlled by Eve) on the quantum channel. Alice and Bob quantify correlations between themselves and with Eve by means of the parameter estimation step[1], which involves evaluating the actual loss and noise in the quantum stage of the protocol. At this stage, Alice and Bob possess identical bit sequences which are, however, not completely private: in order to ensure that Eve's knowledge of their semi-secret bit sequences is reduced to something insignificant, they perform hashing using special mathematical functions. This step is known as privacy amplification. More information regarding these steps in the classical stage can be obtained from several of the reviews mentioned at the beginning of this chapter.

In order to communicate during information reconciliation, parameter estimation, and privacy amplification, Alice and Bob exchange messages that must fulfil the requirement of being authentic, though the message content need not be confidential. For this, QKD systems require an authenticated connection [**Scarani2009**, **Portmann2022**], typically realised using another physical channel or through multiplexing on the quantum channel. Several cryptographic methods (including those based on pre-shared symmetric keys that can offer information-theoretic security [**Carter1979**, **Wegman1981**]) can be used for the creation of such an authenticated channel.

2.3 Discrete and Continuous Variables

Variables refer to the (quantum) properties or DOFs used for information coding. QKD schemes are realised as quantum-optical setups that are capable of processing these variables. The most frequently used DOFs in QKD systems are polarisation, amplitude, phase, and time.

The first generation of QKD systems and protocols is based on discrete variables (DV), which means that measurement outcomes (or detection events) exhibit a discrete nature. This is in contrast to continuous variable (CV) systems and protocols where the detection outcomes are continuously distributed. In this section, these two main branches of QKD are briefly described.

2.3.1 DV-QKD Systems & Protocols

Typically, the number of possible measurement outcomes explored in discrete-variable quantum key distribution (DV-QKD) protocols ranges from two to six for a two-dimensional system [**Scarani2009**, **Pirandola2020**]. Since the inception of the first QKD protocol, published in 1984 by Charles H. Bennett and Gilles Brassard [**Bennett2014**], many other DV protocols and variants have been proposed. Nonetheless, BB84 is the most well-known and widely implemented protocol across QKD systems as of today. Below, a short technical summary of how this protocol works using polarisation, is provided.

2.3.1.1 BB84 Protocol

BB84 is a prepare-and-measure type of protocol. As the first step, the transmitter prepares a random sequence of quantum states, choosing one out of four possible states in each instance.

[1] From a sequential point of view, this step has traditionally been performed before information reconciliation.

These states can be represented in two complementary bases, such as the horizontal/vertical and diagonal/antidiagonal polarisations (phase encoding can be also used equivalently). Both QKD users randomly choose one of the two bases, and the transmitter chooses one of the two states in a basis, associating bit values 0 and 1, respectively. The non-orthogonality of the states guarantees that the eavesdropper cannot clone or measure the prepared states with perfect fidelity. If, for a particular state, the transmitter and receiver have chosen the same basis for their measurement, their bit value will be identical. If the bases are different, the bit will be random.

After this quantum stage of the protocol, Bob notifies Alice over the authenticated channel about his basis choice for each detected signal state. Alice reports back her bases and they discard all bits in which their choices of bases do not match. Provided that no errors occurred or no one manipulated the photons, the users should now both have an identical string of bits which is called the "sifted key". Alice and Bob test the existence of errors in their key by agreeing on a random subset of the bits to compare their results via the authenticated channel. Eve is able to take note of these bits but is unable to use this information because these no longer secret bits are discarded from use. If the exchanged bits align, Alice and Bob are able to use the remaining bits to form their shared secret key. In the absence of noise or measurement errors, a disagreement in any of the compared bits would indicate the presence of an eavesdropper on the quantum channel. For practical applications some noise and measurement errors are expected and need to be taken into account in security proofs and aforementioned post processing procedures.

2.3.2 CV-QKD Systems & Protocols

In continuous-variable quantum key distribution (CV-QKD), the quantum correlations between Alice and Bob are established using a continuous-variable property, usually the amplitude and phase quadratures of the electromagnetic field of light. In that sense, CV-QKD setups share a lot of similarity with "coherent" optical communication/telecom systems [**Kikuchi2015**]. This is especially true for the case of measurement where the (quantum-) information-carrying optical signal is interfered with a reference light field called the local oscillator (LO). The LO is typically a known bright coherent signal, such as the output of a laser, and aids in the phase alignment of the transmitter and receiver. It has an intensity much higher than that of the quantum signal: In fact, the quantum signal field in CV-QKD contains just a few photons on average in order to guarantee non-orthogonality of the quantum states (see Section 2.2).

From the viewpoint of a prepare-and-measure scheme, information is encoded at the CV-QKD transmitter in the amplitude and phase quadratures of the laser field, for example by modulating the optical signal field which is in a coherent state[2]. A constellation of states is produced, which is attenuated sufficiently to yield the quantum signal before being transmitted on the quantum channel. After having suffered loss and gained noise on the channel, this quantum signal is measured by a coherent detector as described above.

Measurements of vacuum noise (also called quantum noise or shot noise) play a central role in the security and performance of CV-QKD systems: Eve's actions result in the total observed noise to exceed the vacuum noise. Alice and Bob are thus required to calibrate their QKD devices to have an accurate knowledge of the vacuum noise. During the execution of the QKD protocol, they evaluate Eve's information by estimating two channel parameters: the "excess noise" which is the difference between the total observed noise and vacuum noise, and the "transmittance" of the quantum channel.

2.3.2.1 Gaussian/Discrete Modulation

In Gaussian modulation, the encoding variables are regarded as Gaussian random variables. Gaussian modulation with coherent states has been the workhorse, both from a theoretical and

[2] Alternatively, squeezed states can also be used.

experimental perspective, of CV-QKD systems since the advent in 2003 of what is now the Gaussian-modulated coherent state (GMCS) protocol [**Grosshans2003**].

However, in reality, there always is some discretisation in the modulation process as physical devices cannot produce truly continuous outputs. Furthermore, the dynamic range of these devices is also not infinite, whereas a truly Gaussian distribution is unbounded. Due to this, there has been a concerted effort in the CV-QKD community to implement discrete modulation protocols, where only a handful of states (typically a number equal to 2^M with $1 \leq M \leq 8$) are actually modulated.

2.4 QKD Devices and Components

2.4.1 Single-Photon Detectors

As mentioned in Section 2.1, QKD relies on photons as carriers of quantum information. In order to decode this information, a QKD system needs to be able to perform a quantum measurement which necessarily involves the detection of photons. The quintessential devices that register the presence of an optical signal consisting of a single photon (or few photons) through detection events called "clicks" are single-photon detectors. These photodetection devices are used in the receivers of DV-QKD systems described in Section 2.3.1.

The two most prominent types of single-photon detectors are avalanche photo detectors (APDs) and superconducting nanowire single photon detectors (SNSPDs). The properties and functionalities of these photodetection devices relevant to this study are described below.

2.4.1.1 Single-Photon Avalanche Diode

An APD that is used as a single-photon detector is also called a single photon avalanche diode. APDs are solid-state devices that generate charge carriers upon photoexcitation. Since the "bias" or the voltage applied across the APD is above the breakdown voltage V_b of the APD, such carriers are quite energetic and ionise additional carriers in the junction area. Such repeated ionisation events lead to an avalanche of charge carriers.

Linear and Geiger Mode The output photocurrent of an APD is proportional to the input optical intensity when the voltage applied across the APD is below the breakdown voltage of that APD. In such cases, the APD is in the "linear mode". An APD operating at a voltage that is higher than the breakdown voltage becomes highly sensitive to extremely low optical intensities: In fact, even a single photon can trigger an avalanche. The flow of these charge carriers constitutes a measurable current that is then interpreted as a detection event. This is known as the "Geiger mode" operation of an APD, and is instrumental in usage of APDs as single-photon detectors.

Active and Passive Quenching The avalanche produced in Geiger mode is self sustaining, i.e., the current does not stop on its own unless the availability of charge carriers is limited or quenched. In the passive variant of quenching, a rather large resistance is placed in series with the APD to restrict the flow of charge carriers into the device. Essentially, the APD can be seen as a capacitor that is slowly (reverse) charged through the resistor. When it is charged, a photon triggers the avalanche that discharges the device: Due to the limited charge carriers being re-supplied to the APD, the avalanche rapidly stops, and the charge process begins again. On the other hand, in active quenching, the APD discharge is stopped by sensing the rise of an avalanche and actively lowering the bias voltage below V_b. Afterwards, the charging process is started. By replacing the passive resistor with an active circuit, the charge current can be regulated at higher values in a more controlled way, leading to a significantly faster charging process.

Gating APDs can be operated in Geiger mode continuously or they can be gated, meaning that they are activated for certain, usually periodic, time windows. During the time window the APD is activated, the bias voltage is increased above V_b, thus arming it to detect photons. At present, gated APDs form one of the most common photodetection devices for QKD systems.

Afterpulsing A common but usually unwanted feature of operating APDs in Geiger mode is called afterpulsing. This means that there is an increased probability of a second detection event shortly after a first one. The second click is therefore not caused by an actual new photon, and is thus noise. This detection event is usually attributed to charge carriers that get trapped during the first avalanche and subsequently trigger secondary avalanches when they become free. The afterpulsing probability depends on multiple parameters, including the material of the APD and the type of quenching implemented.

Backflash or Breakdown Flash Another undesired feature produced as a result of the avalanche is the emission of (secondary) photons. Such an event, occurring due to the recombination of a conduction-band electron with a valence-band hole, is known as the breakdown flash or backflash. The spectral distribution and the emission probability characteristics of a backflash depend on the material of the APD as well as the operating parameters such as temperature, width of gate (if gated), rate, and mean photon number of the incoming optical signal.

2.4.1.2 Superconducting Nanowire Single-Photon Detector

In this type of detector, the absorptive element is a nanowire that is patterned by electron-beam lithography in superconducting film and biased just below its critical current, which is the point at which the nanowire changes its behaviour from resistive to superconducting. If an incoming photon now hits the nanowire, its temperature increases, thereby introducing a perturbation to the current distribution which in turn causes a fast voltage-pulse that can be amplified and measured as a count. Subsequently, the electric circuit tries to counter the increased resistance by diverting current from the nanowire to the transmission line (electrothermal feedback), allowing for a cooling of the superconducting film. During the (brief) time period the nanowire takes to cool down below the critical temperature, called dead time, the detector is not able to detect any further photons. Furthermore, the chosen bias point can have an effect on the detection efficiency and the dark count rate.

Latching Normally, after a photon hits the nanowire, electrothermal feedback resets the device back to the superconducting state. In an effort to increase the count rate of the detector, the magnetic inductance or the load impedance of the underlying electrical circuit has to be adjusted in a way that the reset time of the nanowire decreases. However, if the reset time becomes too short, the detector “latches” into a state in which a stable resistive hotspot is formed. In this latched state, the detector is unable to detect any further incoming photons.

2.4.1.3 Characteristics of Single-Photon Detectors

Here, some of the main characteristics of APD- and SNSPD-based single-photon detectors that are relevant to this study are discussed.

Dead Time After a photon detection event, a detector may be unable to reliably detect additional photons for a time interval τ. This could be due to the intrinsic nature of the detector and/or a limitation of the circuit that records the detection events. As a consequence, the dead time sets a limit to the maximum count rate $1/\tau$ of the detector.

Detection Efficiency The detection efficiency is defined as the probability of registering the arrival of a photon at the detector. This could be measured as the ratio of the count rate registered by the detector and the rate at which photons arrive at the detector. In an experimental scenario, however, the overall detection efficiency of the whole receiver is also affected by coupling losses through free-space optics and/or optical fibres, which occur before the photon impinges on the photosensitive portion of the detector.

Dark Count Probability The probability of the detector registering false counts, i.e., detection events without any optical input, is described by the dark count probability. Dark counts represent noise and occur due to both internal and external factors, including material properties, biasing conditions, and ambient thermal noise. In QKD, it is usually not possible to differentiate between the noise counts incurred as a result of any eavesdropping activity or dark counts.

Spectral Range The wavelength of the photons arriving at the QKD receiver needs to be carefully considered, as single-photon detectors are normally only sensitive to a certain range of wavelengths, i.e., exhibit poor detection efficiencies for photons at wavelengths outside this range. The spectral range of a given detector is mainly a function of the material properties.

Timing Jitter The variation in time delay between the absorption of a photon and the generation of an output (such as a voltage pulse) that qualifies the registration of that photon is called timing jitter. Since the maximum clock rate of the photon counting module is also dependent on this variation (counts can stray into neighboring clock cycles), timing jitter has to be taken into account when designing QKD applications.

Photon Number Resolution A detector that is able to distinguish whether one or more photons are present (which can be the case, e.g., using weak-coherent lasers) are called photon number resolving detectors. This feature can be achieved through spatial or time multiplexing of conventional APDs and SNSPDs, or through the use of superconducting transition edge sensors, which intrinsically produce a signal proportional to the number of absorbed photons.

2.4.2 Other Detectors

Single-photon detectors (covered in the previous section) enable the quantum measurement of discretely varying properties of the photons. A quantum measurement may, however, require being able to discern continuously varying properties such as the amplitude and/or phase of the optical signal. Alternatively, practical QKD systems may need to make classical measurements, such as the intensity or power of a bright optical signal, which may contain millions of photons on average. For these purposes, the most common photodetection devices are made of positive (intrinsic) negative (P(I)N) photodiodes.

Just like APDs (refer to Section 2.4.1.1), P(I)N photodiodes, or simply photodiodes, are also solid-state devices that generate a current when light is absorbed in the depleted region of the P(I)N junction of the semiconductor material. Therefore, some of the properties described in Section 2.4.1.3 are applicable to photodiodes as well.

In QKD implementations, photodiodes are used (typically together with electronic amplifiers) in the construction of coherent receiver circuits, such as homodyne detectors for measuring the electromagnetic quadratures, as well as power monitoring and optical synchronisation circuits. Below, two such photodetection devices that are relevant to this study are described.

2.4.2.1 Coherent Detectors

Coherent detectors employed in CV-QKD receivers implement techniques such as a homodyning, intradyning or radio frequency (RF) heterodyning [**Kikuchi2015**, **Pirandola2020**] to infer the amplitude and phase information coded in the quantum-optical signal, which is interfered with the LO. As elaborated in Section 2.3.2, the LO is typically a bright coherent signal, such as the output of a laser, with an intensity much higher than that of the quantum signal. All of these techniques essentially involve measuring the output of the interference on a photodiode (or a pair of photodiodes) and electronic processing, including filtering, subtraction, etc. of the corresponding photocurrent(s).

While coherent detectors are used very frequently in classical optical communications, for quantum communications, or specifically CV-QKD, they need to satisfy certain extra conditions. For instance, they need to be able to resolve the vacuum noise (see Section 2.3.2) over the entire quantum signal bandwidth. The amplification produced by a coherent detector needs to be able to preserve the linear relationship of the variance of the vacuum noise with the LO power (at least over a certain range), as this is how CV-QKD systems calibrate the vacuum noise level.

More specifically, by having a vacuum state on the signal port of the coherent detector, by blocking the (signal) light from entering the receiver, the calibration can be performed. Practical coherent detectors also suffer from electronic noise, for instance, due to thermal effects in the electronic amplifiers. In order to subtract this noise component (and obtain the ‘true’ vacuum noise), the calibration procedure therefore may involve another stage where the LO input to the detector is switched off as well.

2.4.2.2 Watchdog Detectors

As the name conveys, these detectors are used for guarding a device, e.g., a QKD transmitter, against undesired intrusions through the quantum channel. A typical example of an undesired intrusion is bright light launched by Eve into the device for exploiting imperfections of the realistic components which could allow the eavesdropper to remain undisclosed: Several such exploits and attacks are described in Chapter 4. While P(I)N photodiodes are generally more suited for implementing watchdog detectors, one can also use APDs in the linear regime.

Typically, these detectors are installed at locations close to where the device under protection connects to the quantum channel, so as to be effective in raising an alarm early enough in case of an attack. The detector can then trigger an automated mechanism such as (the burning of) an optical fuse or call for manual intervention (human operator) to ensure disconnection of the device from the channel and protection against future attacks.

However, the watchdog detector circuitry responsible for raising alarms needs to be carefully implemented in order to reduce the chances of getting triggered by false positives, i.e., legitimate signals from the other QKD subsystems, while simultaneously succeeding to catch any actual intrusion. For this, one recommendation is to use an array of such watchdog detectors having different response times and sensitivities in different spectral regions, together with a careful analysis of all their outputs to determine the conditions for raising an alarm. Lastly, the watchdog detector itself may need protection from a (sudden) strong light injection by Eve that could damage it functionally, i.e., render it useless.

2.4.3 Optical Sources

Implementing QKD protocols the way they are proposed or intended imposes specific requirements on the optical sources used in the QKD system. Lasers are the underlying optical source used for creating quantum “signal” states in prepare-and-measure QKD transmitters. Lasers are also used directly for implementing the LO in CV-QKD systems (see Section 2.3.2). This is inter alia due to various properties of lasers including coherence, single-mode nature, as well as stability in the frequency and power of operation.

A laser can be operated either in the continuous wave (CW) mode, providing a steady stream of photons, or in pulsed mode, which is characterised by short bursts of energy. In the latter case, the output of the laser is determined by pulse duration (time the laser is on) and repetition rate (number of on and off cycles per second).

2.4.3.1 Weak-Coherent States

The output state of a laser itself in a given mode is (in ideal cases) described by a coherent state. This coherent state, in the absence of a reference phase, can be described by a Poissonian superposition of photon number states. In the case of a pulsed laser, each individual pulse contains multiple photons at the direct output of the laser. In the context of QKD, one attenuates the laser output so that on average a pulse would contain just a few photons. The quantum state describing such an attenuated laser output is that of a weak-coherent state, and due to the Poissonian nature, many of the weak-coherent pulses actually do not contain any photons, while the probability of having more than one photon per pulse is low but not zero.

2.4.3.2 Single-Photon Sources

Compared to attenuated lasers, single-photon sources (or more generally sub-Poissonian sources) can be advantageous as the probability of emitting multiple photons is smaller (theoretically zero). The basis of most sub-Poissonian sources is the optical excitation or pumping (via lasers) of materials endowed with special properties. The two most prominent sub-Poissonian sources used in QKD implementations are based on (heralded) spontaneous parametric down-conversion (SPDC) and semiconductor quantum dots (QDs). SPDC requires a nonlinear medium for conversion of a higher-energy pump photon to two lower-energy photons, one of which is then detected to "herald" the presence of the other photon. QDs exhibit atom-like discrete energy levels, i.e., individual optical transitions involving electrons, which are used for realising single-photon emission.

2.4.3.3 Entangled Sources

Entangled states refers to a composite system whose description cannot be broken into its elementary component states. To elaborate with an example of an entangled state with two quanta, a full description of one quantum particle is not (mathematically) possible without a reference to the state of the other quantum particle. Entanglement is a uniquely quantum mechanical resource and can occur in different DOFs (e.g. polarisation, frequency, time, photon number, amplitude and phase quadratures). In QKD implementations of entanglement-based schemes (see Section 2.2), the photons used for sharing correlations between Alice and Bob are entangled states. Sources based on SPDC and QDs (see Section 2.4.3.2) are capable of producing highly entangled states with two quantum particles.

2.4.4 Other Components

Besides detectors and optical sources, other optical components used typically across most QKD setups (and which are also relevant to this study) are described below. It is worth noting that the behaviour of some of these components is usually limited to a certain spectral range.

2.4.4.1 Beamsplitters

A beamsplitter (BS), or more appropriately a non-polarising BS, is a passive unitary device that performs a linear transformation on one or more input fields to produce one or more output fields. Although there exists a variety of different configurations of BSs, the most common type used in QKD setups has two inputs and two outputs, frequently called "ports". From a classical physics perspective, such a four-port BS splits the intensity of an incident beam of light into two. In the case of a single photon at the input, the field amplitudes are replaced by probability amplitudes. Assuming a pair of ideal single photon detectors (introduced in section 2.4.1) at the two output ports, a balanced or symmetric BS ensures that the single photon is registered with an equal probability of 0.5 in either of the two detectors randomly. Beamsplitters, especially symmetric ones, play an important role in realising quantum communication.

2.4.4.2 Optical Attenuators

Optical attenuators serve to reduce the optical power transmitted through them, and are used in several QKD applications. For instance, they can be used in the preparation of weak-coherent states in both CV-QKD and DV-QKD transmitters (see Section 2.4.3). They can also be used as countermeasures, e.g., as part of the watchdog detector assembly (see Section 2.4.2.2), to prevent attacks by Eve. They can be categorised into fixed optical attenuators, with a fixed attenuation level, and variable optical attentuators (VOAs) that are able to control the attenuation level (in a specified range and with a specified step) on demand.

2.4.4.3 Polarisation-based Components

In the context of QKD, the property of polarisation is sometimes used as DOF to encode information. In addition, polarisation is frequently used in realising different functionalities, such as (de-)multiplexing or selective attenuation in both QKD transmitters and receivers. Below, the three most common polarisation-based components used in QKD setups are described:

Polarisers Polarisers (or more precisely, polarising filters) are devices that enable a selective transmission of light, i.e., photons with only a specific polarisation pass through them.

Polarising Beamsplitters As the name suggests, a polarising beamsplitter (PBS) is a type of BS (see Section 2.4.4.1) where the transmission/reflection of photons is dependent on the polarisation state of the incident photon; for instance, photons with a horizontal polarisation get transmitted, while photons with a vertical polarisation get reflected.

Waveplates Due to the properties of the underlying birefringent material, waveplates introduce a relative phase-shift between the horizontal and vertical component of the polarisation. Half-wave plates (HWPs) [Quarter-wave plates (QWPs)] introduce a phase-shift of π [$\pi/2$], changing the polarisation state.

2.5 Basic Implementation Attacks on QKD

The ultimate objective of an attack on a practical QKD implementation is to be able to obtain a non-negligible amount of information about the secret key (see Section 2.2) without alerting Alice and Bob. For this, it is generally assumed that Eve has an inexhaustible number of ways to attack at her disposal. Her “attack path” could be generally described as a series of actions performed while Alice and Bob execute the QKD protocol and generate keys—without however realising that Eve has obtained a partial or even complete knowledge of those keys. The first action could be for instance (remotely) characterising the QKD systems and their operation, with the motivation of spotting one or more security vulnerabilities. The next step is to exploit these vulnerabilities, i.e., actually performing the attack that ends up with Eve having the non-insignificant correlations to the bitstrings held by Alice and Bob (see section 2.2).

During any of these endeavours, Eve’s hope is to stay concealed. Typically, this implies that Alice and Bob do not observe the operating parameters to be out of some known range during the QKD protocol run. With reference to section 2.3.1.1, for instance, in case the error incurred by Bob crosses a certain threshold, Alice and Bob would attribute this to Eve, and would abort the QKD protocol. That however is not in Eve's interest as she would actually like Alice and Bob to use the keys generated through that protocol. One obvious way that Eve can try to prevent Alice and Bob to abort the protocol is to attack only a fraction of the signals [**Ye2020a**].

Below, some attack strategies that are most relevant to this document in the sense they are extensively mentioned in the attack tables of Chapter 4 are described.

2.5.1 Photon-Number-Splitting Attack

Only a pure single-photon source (see Section 2.4.3.2) is capable of generating quantum states with an exact zero multiphoton probability. In practice, the photon number statistics from heralded SPDC and QD sources mentioned before may also show some multiphoton components. In any case, weak-coherent states (see Section 2.4.3.1), which may be described as the "workhorse" quantum signal states in DV-QKD systems show Poissonian statistics, i.e., some pulses have the possibility to contain more than one photon. This non-zero multiphoton probability results in a vulnerability that can be exploited by so-called photon-number-splitting (PNS) attacks [**Luetkenhaus2000**, **Brassard2000**].

To launch a PNS attack against a QKD system operating the BB84 protocol (see Section 2.3.1.1), the quantum states leaving the transmitter are intercepted on the quantum channel and subjected to a (quantum-non-demolition) photon number measurement. If the outcome of this measurement is one, Eve blocks that quantum state. If it is greater than one, Eve splits that pulse to retain and store only one photon and sends the remaining photons to the receiver (via a low-loss channel). Once Alice and Bob publicly discuss their measurement bases in the sifting/reconciliation step (see Section 2.2), Eve then performs the same measurement on the stored photon in the correct basis. In this manner, she obtains information about the sifted key (and thus the secret key) without disclosing her presence.

2.5.2 Intercept-and-Resend Attack

An intercept-and-resend attack [**Bennett2014**] is a simple attack where the adversary Eve *intercepts* the quantum signal transmitted by Alice on the quantum channel and subjects that to a quantum measurement similar to the one normally performed by Bob. Depending on the outcome she obtains, she then *re*-prepares a suitable quantum state and *sends* it to Bob.

With reference to BB84 (see Section 2.3.1.1), a precondition for the correct operation of the protocol is that whenever the preparation basis of Alice is different than (equal to) the measurement basis of Bob, the corresponding measurement outcome is random (deterministic). In other words, if in the intercept-and-resend attack, Eve chose the other basis than the one in which Alice had prepared her state, her measurement outcome would be random, i.e. either bit "0" or bit "1", each with a probability of 1/2. In such cases, Bob's quantum measurement on the re-prepared state from Eve would yield him a bit that is exactly opposite to that of Alice with a probability of 1/2. During the public communication phase, Alice and Bob would find that their respective bit sequences have a mismatch (on average for $1/2 \times 1/2 = 1/4$ of all events). This then ensures that a plain intercept-and-resend attack would necessarily result in Bob incurring a quantum bit error ratio (QBER) of $\approx 25\%$, which is significantly higher than it would be without the attack.

2.5.2.1 Faked-States Attack

A faked-states attack [**Makarov2005**] is a special kind of intercept-and-resend attack that exploits vulnerabilities in the single-photon detection system of Bob. The initial step is the same: Eve intercepts and measures the state sent by Alice on the quantum channel to Bob. Depending on the measured value of the bit, she prepares a "faked state" which would produce a detection event in a manner controlled by Eve. To obtain this control, Eve may for instance blind Bob's single-photon detectors by shining CW light [Lydersen2010a] from the quantum channel (several of such control strategies are elaborated in Chapter 4). Typically, Eve prepares the faked state using the basis she had employed and the bit she subsequently obtained[3]: and in this case, Bob would register a detection if and only if his measurement basis coincides with that of Eve. This is due to constructive interference that causes all the optical power of the faked state to reach a targeted detector—this can, for instance, increase the detector output voltage beyond the discriminator threshold, thus producing a detection event. Conversely, if the basis choice of Bob and Eve do not coincide, the pulse power is split, and the resulting detector outputs do not cross their respective discriminator thresholds. By choosing the launched power of the faked states carefully, Eve can thus control the detection outcomes in Bob.

In contrast to the (legitimate) few-photon quantum states shared between Alice and Bob, faked states are usually classical states containing many photons, which should normally result in an unusual response from the single-photon detection system. Nonetheless, the faked-states attack exploits certain characteristics of the detection system to provide Eve a significant knowledge of the key without alerting Alice and Bob. Especially, compared to a simple intercept-and-resend attack, the QBER incurred by Bob during a faked-states attack can be almost negligible.

2.6 Attack-Prevention Mechanisms in QKD

Attacks and measures to prevent (or protect against) them go hand in hand in any branch of cryptography. The same is the case with QKD, where extensive research by the QKD community over the last decades has investigated not only attacks, loopholes, vulnerabilities and imperfections but also methods and strategies to counter them and/or their consequences. At times, such countermeasures proposed to prevent an attack, close a loophole, address a vulnerability, or deal with an imperfection, can protect an entire class of QKD protocols or family of QKD implementations from having their security compromised. One such example is the decoy-state method that can be used for detecting the PNS attacks, which were introduced in Section 2.5.1.

2.6.1 Decoy-State Method

Decoy states are quantum states that (in ideal circumstances) have exactly the same characteristics as the quantum signal states except in their photon number statistics. With reference to the explanation in Section 2.5.1, the transmitter *randomly* replaces some of the outgoing quantum signal states with these decoy states. After the quantum measurement, the transmitter discloses to the receiver the instances where the decoy states were used. Based on this information and on the detected statistics corresponding to the different signals, it is possible to obtain a tight estimation of the detection and error rates associated to the single-photon pulses emitted by the transmitter, thus defeating the PNS attacks.

In fact, the decoy-state method, developed from heuristics [Luetkenhaus2002, Hwang2003] to (rigorous) security analysis [Wang2005, Lo2005], is now considered the default method to prevent PNS attacks in practical DV-QKD implementations. Typically, two sets of mean photon numbers, one ideally zero (i.e., always yielding vacuum states) and the other close to zero, are used for preparing decoy states.

2.6.2 Interference-Based QKD

For a class of QKD schemes, quantum-optical interference is at the heart of how quantum correlations are distributed across long distances. This interference involves the measurement of quantum signals prepared by two QKD transmitters in a suitable DOF and sent (on a pair of

[3] In some cases, however, encoding the opposite bit in the opposite basis in the faked state can prove to be a more beneficial strategy for Eve [Makarov2006].

quantum channels) to a so-called relay station, housing the quantum measurement apparatus. For obtaining interference, symmetric beamsplitters (see Section 2.4.4.1) are a primary component of the relay, whose main functionality is to announce or relay the measurement outcomes.

Remarkably, in these type of interference-based QKD schemes, no security assumptions on the measurement apparatus, especially the detectors[4] are required. In fact, the entire relay station can be in full control of Eve. This has significant implications for the practical security of the QKD implementation: Any attack that exploits imperfections in the detection system, such as the faked-states attack introduced in Section 2.5.2.1, cannot provide any advantage to Eve.

The first known interference-based QKD scheme that closes all detection-related loopholes is aptly named measurement-device-independent QKD (MDI-QKD) [**Lo2012**]. In this scheme, the quantum signals from Alice and Bob (who also holds a QKD transmitter now) interfere on a relay; in case of DV-QKD, the correlations are extracted because of two-photon coincidence with polarization and phase as the oft-used DOFs. In case of CV-QKD, homodyne interference and quadrature detection is employed [**Pirandola2015**].

A first-order interference is realized when the DOF is phase, i.e, Alice and Bob prepare phase-encoded optical fields. Whenever these phases—chosen randomly and independently by either party—are near twins, i.e., sufficiently close in their values, the interference at the relay leads to correlations that can be distilled to bit sequences. This is the twin-field QKD (TF-QKD) protocol [**Lucamarini2018**], which is based on single-photon interference (in contrast to MDI-QKD which is based on two-photon interference).

Several variants of interference-based QKD protocols exist today. These include the virtual protocol [**Braunstein2012**], the receiver-device-independent (RDI) family of protocols [**AlDarwbi2022**, **Ioannou2022**] and the prepare-and-measure Bell test protocol [**Tan2016**]. From an implementation point of view, the MDI-QKD and TF-QKD protocols have been the most popular. Theoretical improvements in the security analysis and technical improvements in the practical setups operating the MDI-QKD and TF-QKD protocols have pushed the frontiers on both performance and overall implementation security.

[4] Sections 2.4.1.1 and 2.4.1.2 give a background of detectors used in DV-QKD systems while Section 2.4.2.1 describes the detectors employed in CV-QKD systems.

3 Structure of the Analysis

This document aims to present the current state of scientific literature on the subject of implementation attacks against QKD systems. For this purpose, viable attack paths (see Section 2.5) are first assembled from the literature. Based on the description of these attack paths, the effort an eavesdropper needs to make in order to successfully mount the respective attack is quantified using a best-case scenario from the eavesdropper's perspective, i.e., the easiest attack path is chosen. As explained in Chapter 2.4.4.2, an eavesdropper has an inexhaustible number of ways to attack at their disposal, and thus can combine relevant attacks as needed.

Identification of a complete attack path is, however, not clear for some of the analysed works. To elaborate, for all vulnerabilities presented in Chapter 4.4, it is not exactly clear how to exploit a vulnerability, either due to the lack of equipment or expertise. Thus, in a first step a distinction between attacks (i.e., where the full attack path is known) and vulnerabilities (i.e., where a source of information leakage resulting in a side channel is known but it is not clear whether this is exploitable) is introduced.

3.1 Attack and Vulnerability Tables

To present the details of various implementation attacks togehter with the attack analysis in a concise and organised manner, a tabular approach has been taken. While the tables themselves are presented only in Chapter 4, the basic template that each of them follows can be found below in Table 3.1.

Name	Attack table template		
Category			
Component		**Subcomponent**	
Expertise		**Opportunity**	
Attack Rating		**Attack Type**	
Protocol			
Target(s)			
Short Description			
Precondition			
Equipment			
Description			
Proposed Countermeasures			
Remarks			
Feasibility			
Reference(s)			

Table 3.1: Attack table template

Each such attack table carries a unique "name" that also eventually acts as the caption and identifier of that table.

As a precursor to writing this document, a literature survey of scientific articles such as those published in journals and conference proceedings was done. Based on common themes or elements across different articles, the entire body of the surveyed literature was thereafter categorised into the following attack categories:

- Calibration attack
- Classical side-channel attack
- Degree-of-freedom coupling attack
- Detector-backflash attack
- Detector-control attack
- Excessive-modulation attack
- Laser-damage attack
- Laser-seeding attack
- Non-random phase attack
- Phase-reference alignment attack
- Phase-remapping attack
- Photon-number splitting attack
- Saturation attack
- Timing attack
- Trojan-horse attack
- Wavelength-dependent manipulation attack

The field "Category" is set to one of the options mentioned above. All the remaining fields of Table 3.1 are elaborated further in Table 3.2.

Field	**Details**
Component	This field states which part of the QKD system serves as the point of entry for the attack. This is usually either the transmitter, the receiver, or the post-processing. In rare cases, there are multiple entry points for an attack.
Subcomponent	This field gives the subcomponent targeted by the attack as point of entry. There are many options possible here, with some attacks targeting very specific components, e.g., actively quenched APDs or modulators. This field may be left empty if several subcomponents are affected.
Expertise	This field gives the expertise required for the attack, as defined in Section 3.2.3.
Opportunity	This field states the window of opportunity for the attack, as defined in Section 3.2.5.
Attack Rating	This field gives the calculated attack rating, as described in Section 3.2.7.

Attack Type	This field states whether the attack is of passive or active nature, i.e., the attacker has to only listen while the device is working (passive) or needs to alter the device's working conditions in order to successfully attack (active). A combination of passive and active attack type is also possible, this is called "mixed".
Protocol	This field gives the QKD protocols the respective attack can be applied to. The attack may not be exclusive to the protocols mentioned here, as this list is based on the referenced papers.
Target(s)	This field defines the target of the particular attack. While the eventual target for Eve is to gain knowledge about the secret key without getting disclosed to Alice and Bob (see Chapter 2), here the entries can be one or more of the following: - gain partial knowledge of the key agreed upon by Alice and Bob; - gain complete knowledge of the key agreed upon by Alice and Bob; - enable further attacks leading to one of the above scenarios. A target of complete knowledge of the key necessarily includes the target of partial knowledge of the key. A target of partial or complete knowledge of the key can be combined with the target of enabling further attacks.
Short Description	This field gives an overarching condensed explanation of what the attack is about.
Precondition Knowledge about the target of evaluation (TOE)	This field contains information on the level of knowledge about the TOE, as defined in Section 3.2.4, as well as all preconditions, i.e., the elements that need to be present in the QKD system for the vulnerability to be manifested or the attack to work.
Equipment Equipment rating	This field lists information on all necessary equipment for mounting the attack. Moreover, the "equipment rating" as defined in Section 3.2.6, is given under the field name.
Description	This field describes the attack in detail as it is found in the articles relevant to that category. Typically, it starts with some background and general explanation of the principles of the attack, and is followed by a presentation of the information gleaned and compiled from the individual articles.
Proposed Countermeasures	This field gives an overview of countermeasures identified to prevent (or reduce the effectiveness of) the attacks under discussion. It does not, however, give any assessment of how one measure may be better or worse than another (see also the **Disclaimer on Proposed Countermeasures** in Chapter 4). In order to avoid repetition across several tables, the countermeasures applicable to several attacks are grouped together, and presented in Section 4.5.
Remarks	This field is reserved for any additional information, comments or expert opinion from the authors of this document. If there is no further remark to be added, the field only contains a "-".

Feasibility t_{Attack}	This field provides information about (successful) implementations of the attack. This could be for instance the type of QKD system or the subcomponent involved. The value for t_{Attack} below the field name gives the elapsed time, as defined in Section 3.2.2.
Reference(s)	This field contains a list of all publications relevant to the described attack.

Table 3.2: Description of the fields found in the attack table template (Table 3.1).

As mentioned in the beginning of this chapter, a clear attack path does not always manifest completely, even though a vulnerability has been identified. These vulnerabilities might be exploitable by an attacker in the future, assuming that (in most cases) the required equipment has been invented by then. To describe such vulnerabilities, an adjusted table template is used, as shown in Table 3.3.

Vulnerability	Vulnerability table template		
Component		**Subcomponent**	
Protocol			
Short Description			
Precondition			
Description			
Proposed Countermeasures			
Remarks			
Reference(s)			

Table 3.3: Vulnerability table template

3.2 Attack Rating

Based on the described attack path, a measure of how basic or sophisticated an attack is can be evaluated. This is performed by calculating an attack rating, which essentially describes the difficulty in executing the presented attack path correctly in order to successfully implement the attack. It is based on the following aspects:

- **Elapsed time / Feasibility**
  The time needed to mount the attack
- **Expertise**
  The level of knowledge required from the attacker
- **Knowledge of the TOE**
  The extent of information about the QKD system required to mount the attack
- **Equipment**
  The equipment needed for the attack
- **Window of opportunity**
  The accessibility of the device under attack

The above mentioned aspects, as well as the definitions and descriptions of the considered factors (see Subsection 3.2.1 onwards), are adapted from the current version of Common Criteria Methodology (CEM) which proves to be a reliable approach to estimate the attack ratings on cryptographic systems. In the literature, some approaches to combine Common Criteria and QKD have been made for individual attacks such as "saturation attacks“ [**Kumar2021**]. Here, the CEM-approach is applied on a large variety of attacks described in the scientific literature. Since there is no rating system for QKD attacks yet, the Joint Interpretation Library Hardware Attacks Subgroup [**JILHAS**] approach was also followed. There, the attack is divided into two phases: First, the identification phase; second, the exploitation phase. In the attack tables presented in Chapter 4 the categories determined for the exploitation phase are presented. However, for the final attack rating both phases are considered. Details as well as a more profound description can be found in **CEM**.

Due to the academic nature of investigating attacks on QKD systems, it is important to note that a more detailed determination of the attack rating values is only possible with further research and practical experience (for more details, refer to Section 1.2). Thus, it is important to stress the fact that these attack ratings are not authoritative but a first indication in order to distinguish the presented attack paths by means of an attack rating in the Common Criteria context.

The final grouping into the known attack ratings as it is presented here is not definitive. However, in this phase, the entire experience of the authors of this document has been incorporated to ensure a justifiable distinction. Therefore, comparable attacks should also have a similar attack rating. However, the evaluation of attack rating for an attack can change drastically with further research. When calculating the attack rating, all proposed countermeasures and their (possible) influence have not been taken into account due to the lack of knowledge about their effectiveness.

Finally, it should be noted here that attack ratings can be evaluated only when a complete attack path is determined. Due to this, the vulnerability template (Table 3.3) does not contain some fields present in the attack table template (Table 3.1); otherwise the remaining fields carry the same explanation provided in Table 3.2.

3.2.1 Identification of Factors

QKD systems have multiple differences compared to classical key distribution methods. Nevertheless, as a first and simple approach (as in this document), the factors included in the calculation of an attack rating can be assumed to remain the same as the ones presented in CEM. Like within the smartcard community, a differentiation between the cost of “identification” (i.e., demonstration of the attack) and the cost of “exploitation” (e.g., once the correct parameters for a laser damage attack are published on the internet) are made. As both phases together describe the complete attack, the points for each individual phase are added in order to estimate the final attack rating based on the following formula:

$$\text{Attack rating}_{\text{total}} = \text{Attack rating}_{\text{Identification}} + \text{Attack rating}_{\text{Exploitation}} \tag{3.1}$$

while the rating for each phase consists of the sum of all points P assigned in the identified factors:

$$\text{Attack rating}_{\text{Phase}} = P_{\text{Elapsed Time}} + P_{\text{Expertise}} + P_{\text{Knowledge}} + P_{\text{Opportunity}} + P_{\text{Equipment}}. \tag{3.2}$$

In the analysis throughout this document, identical values for the identification and exploitation phases shall be considered given the final verdict for each identified factor (i.e.,"Bespoke“ equipment amounts to seven points in both phases). Accordingly, the final attack ratings given are probably a bit lower than they will realistically be in the end. In the future, a separation of the analysis for the identification and exploitation phases should refine the rating process.

3.2.2 Elapsed Time

The amount of time to mount an attack i.e., “elapsed time” t_{Attack} is divided into the following intervals shown in Table 3.4

Duration	**Rating**	
	Identification	**Exploitation**
< one day	0	0
< one week	1	1
< two weeks	2	2
< one month	4	4
< two months	7	7
< three months	10	10
< four months	13	13
< five months	15	15
< six months	17	17
< nine months	19	19
Not practical[1]	*	*

Table 3.4: Rating for elapsed time

All attacks presented in this document are either trying to force Alice and Bob to agree on a key which is also known to Eve or the attacker tries to read along the secret while it is being agreed upon. In case Eve enters the quantum channel and gains information about the exchanged key bits, that don’t require post-processing, or forces a particular key onto Alice and Bob the actual attack takes less than a day and the elapsed time for such cases is considered to be “< one day”. Please note that this argument applies only to the exploitation phase as the identification of the attack path may take much longer.

3.2.3 Expertise

Expertise levels define the ability of an attacker to implement attacks, devise attack paths, develop attack setups and procedures, as well as the capability to understand the attack concepts. In the following table, the expertise levels ranging from “Laymen” (lowest) to “Multiple experts” (highest) is shown. Every level includes the expertise of the lower levels.

Expertise Level	**Definition**
Laymen	- Is able to perfectly follow (publicly available) instructions. - Has enough practice and knowledge to rely on user manuals for operating off-the-shelf benches and tools.

[1] CEM defines the term *not practical* as “the attack path is not exploitable within a timescale that would be useful to an attacker”.

Proficient	- Has basic knowledge, training, or experience in implemented algorithms, protocols, hardware structures, security behaviour, principles and concepts of security employed. - Is able to conduct previously successful attacks where adjustments of parameters (laser power, timing etc.) need to be done in order to be successful.
Expert	- Is able to understand the concepts of state-of-the-art attacks and attack procedures from either knowledge or extensive training/experience with the following: implemented algorithms, protocols, hardware structures, security behaviour, principles, and concepts of security employed. - Has the ability to operate complex tools and equipment that require expertise beyond what can easily be acquired from user manuals. - Is able to implement newly published attacks (typically based on a paper or a related patent). - Can devise new attack techniques or attack paths which cannot be addressed by off-the-shelf benches and tools and well prescribed and available sets of procedures. This also includes redesigning or implementing attack techniques, attack paths, setups or procedures for well-established complex attacks. Here, well-established considers that the novelty or the need for adaptation is, for example, related to a specific target or implemented countermeasures.
Multiple experts	Multiple experts from different kind of fields (laser physics, cryptography, electronics engineering, etc.). Multiple experts can also be a single person which is an expert in more than one kind of field.

Table 3.5: Distinction of expertise levels

To calculate the attack rating, each expertise level is assigned to a specific rating during each phase emphasised in Table 3.6.

Expertise	**Rating**	
	Identification	**Exploitation**
Laymen	0	0
Proficient	3	3
Expert	6	6
Multiple experts	8	8

Table 3.6: Rating for the expertise level of the attacker

3.2.4 Knowledge about the TOE

Knowledge about the TOE refers to all pieces of information that need to be known from an attacker's perspective. These may include the used protocol, the hardware components of the TOE, as well as their characteristics, e.g., wavelengths or temperature dependencies. The following information distinction is to be used:

Information Distinction	Definition
Public (or none)	Information is considered public if it can be easily obtained by anyone (e.g., from the internet) or if it is provided by the TOE's manufacturer to any customer without further means
Restricted	Information is considered restricted if it is controlled within the developer organisation and distributed to other organisations under a non-disclosure agreement
Sensitive	Knowledge that is only available to discrete teams within the developer organisation
Critical	Knowledge that is only available to teams on a strict need-to-know basis within the developer organisation
Very critical	Knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need-to-know basis and individual undertaking

Table 3.7: Distinction of knowledge about the TOE

In the here presented analysis of the attack rating, the general approach to estimate the knowledge about the TOE follows as: The QKD receiver and transmitter are treated as commercially available products that an attacker can purchase as standalone components. With these devices, the attacker can thoroughly characterize all necessary aspects required to execute the chosen attack. During this process, the attacker gains access to details about the component's architecture, vulnerabilities, and characteristics. These pieces of information are sufficient for conducting the majority of attacks described in Chapter 4 which is why the necessary knowledge of any TOE component has been rated as "public information". If any attack requires information about the actual implementation, the rating of the knowledge about the TOE has been adjusted accordingly. This is because implementation details are typically kept confidential for commercial products. These assumptions remain valid until a fully secure development chain for QKD components and systems is established. Subsequently, the rating of knowledge will need to be adjusted. To calculate the attack rating, specific ratings are assigned to each knowledge level during each phase, as depicted in Table 3.8.

Knowledge	Rating	
	Identification	Exploitation
Public	0	0
Restricted	3	3
Sensitive	7	7
Critical	11	11

Table 3.8: Rating for knowledge about the TOE

3.2.5 Window of Opportunity

The concept of a "window of opportunity" is closely related to the amount of time that has passed (see Section 3.2.2). Taking advantage of a weakness may demand extended access to the TOE, which in turn could raise the chances of being detected. Some attack strategies might necessitate substantial off-line preparation, requiring only short periods of access to the TOE for successful execution. Conversely, access may need to be sustained or spread across multiple sessions to be effective. The QKD receiver and transmitter are considered commercially available products that an attacker might buy in order to “train” for the attack against the actual target. Thus, the window of opportunity in the identification phase is “Unlimited” in all cases that do not include physical access to the actual target. In case the presented attack uses the quantum channel as a point of entry, independent of its implementation (free-space or fibre-based), the window of opportunity is considered “Easy” as lower boundary since no attacks on ‘in field’ QKD implementations are presented in the literature. If physical access to the component is required, the window of opportunity is considered to be ”Difficult“.

Window of Opportunity	**Rating**	
	Identification	**Exploitation**
Unlimited	0	0
Easy	1	1
Moderate	4	4
Difficult	10	10

Table 3.9: Rating for the window of opportunity

3.2.6 Equipment

In order to rate the equipment, its price and availability are taken into account. Please note that “Bespoke” equipment also requires an expertise of “Expert” level to operate the system and should lead to at least a moderate attack rating.

Duration	**Rating**	
	Identification	**Exploitation**
Standard	0	0
Specialised	4	4
Bespoke	7	7
Multiple Bespoke	9	9
Non-existent	*	*

Table 3.10: Rating for equipment

This document includes some attacks that are theoretical in nature, as in, the equipment is *non-existent*. Also, as the border between the categories listed in Table 3.10 may not be well defined, a metric to compare and to distinguish equipment based on the acquisition and maintenance costs is introduced as a decision guideline:

Cost	**Equipment Category**
< 10 k€	Standard
< 200 k€	Specialised
> 200 k€	Bespoke

Table 3.11: Equipment categorisation by costs

Table 3.12 provides an exemplary list of equipment categorised by means of Table 3.11.

Tool	**Category**
Polariser	Standard
Beamsplitter	Standard
Optical filter	Standard
Helmholz coils	Standard
Simple laser-diode module	Standard
EM-probe	Standard
Timing generator	Standard
Phase / Amplitude / Intensity modulator	Standard
General optical modulator	Standard
Optical amplifier	Standard
Circulator	Standard
Power meter	Standard
Oscilloscope	Standard
Optical spectrum analyser	Specialised
RF spectrum analyser	Specialised
Fast-optical switch	Specialised
Homodyne detector	Specialised
Wavelength-division multiplexer	Specialised
Single-photon detector	Specialised
Laser	Specialised
QKD receiver module	Specialised
QKD transmitter module	Specialised
QKD receiver module (tweaked)	Specialised
QKD transmitter module (tweaked)	Specialised
Intercept-and-resend apparatus	Specialised
Photon-number resolving detector	Specialised
Laser (custom-made)	Bespoke
Ultra low loss quantum channel	Bespoke
Photon-number QND measurement device	non-existent
High quality quantum memory with long storage times	non-existent

Table 3.12: Categorisation of tools

3.2.7 Attack Rating

The attack rating is determined by adding the cumulative scores for both the identification and exploitation phase of all the categories specified earlier, which include: Elapsed time, level of expertise, knowledge about the TOE, available window of opportunity and the necessary equipment.

Values	**Attack rating required to exploit scenario**
0-13	Basic
14-19	Enhanced-Basic
20-25	Moderate
26-31	High
≥32	Beyond High

Table 3.13: Grouping of attack ratings

Table 3.13 gives the resulting Attack rating based on the calculated scores. The rating corresponds to the amount of effort required by Eve to successfully execute the contemplated attack. It implies that an attacker must possess an attack potential that is at least one level above the calculated rating to initiate the attack. Consequently, the lower the attack rating, the greater the number of potential attackers that must be taken into account.

Two clarifications that may be required in the interpretation of the attack ratings in Chapter 4 are elaborated here. First, it should be noted that in determination of the attack ratings, the fields **Target(s)** and **Proposed Countermeasures** (see Table 3.2) are not taken into account. Neither is the degree to which the respective attack has been demonstrated a factor that could be considered for the given attack rating. Second, a worst-case approach (from the QKD users' perspective) is employed in order to estimate the minimum effort an attacker has to make to successfully breach the security.

This implies that a practically not-so-effective attack that however barely manages to break the security criteria of the QKD system and yields a tiny yet non-negligible information about the key may get a lower rating than an attack that is highly practical, effective with current technology, and perhaps even allows a complete knowledge of the key.

4 Implementation Attacks

The security of a physical implementation of a QKD protocol cannot be ensured merely by evaluating the laws of quantum mechanics. In fact, as a consequence of imperfections in the QKD devices and components and incorrect assumptions in the QKD system model, the QKD implementation may deviate from the theoretical description of the QKD system [**Scarani2009**, **Lo2014**, **Jain2016a**, **Pirandola2020**, **Xu2020**]. An attacker can exploit such deviations to prevent or reduce the degradation of the correlations normally caused by eavesdropping attempts, as explained in Section 2.2. To elaborate further, without these deviations, any eavesdropping would have otherwise resulted in a much smaller secret key length or even complete elimination of the secret key.

The deviations can get manifested in several ways. For instance, during the creation or distribution of the quantum correlations or the act of quantum measurements, information that enhances the eavesdropper's knowledge of the key could inadvertently leak through so-called side channels. If the QKD users are unaware of the existence of such side channels (or are unable to account for them), then the security of the QKD implementation can be compromised.

In this chapter, detailed information about numerous implementation attacks[1] that Eve may use to potentially breach the security of a given QKD system and/or realisation of a QKD protocol is presented. The presentation is done through a series of tables, meticulously compiled using information available in the public domain: The surveyed literature sources include peer-reviewed journal publications and conference proceedings, as well as scientific repositories such as `arXiv.org`[2]. In these tables, wherever possible, countermeasures for the described attack methods have also been identified and linked.

Each table itself follows a template that has been explained in detail in Section 3.1. One of the objectives behind preparing this document was to be able to comprehensively analyse and compare attacks on QKD systems, and this has been done through the assignment of an attack rating (which forms one of the many fields of a typical table). The determination of a rating, however, requires having a clearly defined attack path which is not the case with all the analysed works. As in, some of the works merely focus on security vulnerabilities for which an attack path cannot be identified with the currently available equipment or expertise. A first way of classifying the tables thus has been "attacks" or "vulnerabilities".

With the discrete variable and the continuous variable flavours of QKD being the most prominent as of today (see section 2.3), another natural classification for the attack tables has been to sort them in these two groups (sections 4.1 and 4.2 below, respectively), with any attacks relevant to both relegated to a third, common group (section 4.3). This grouping also allows for easier reference whenever it is necessary to identify and address attacks on a particular QKD system of one of the flavours. A similar classification for vulnerabilities has not been performed due to the smaller number of identified vulnerabilities compared to attacks. Finally, it is re-emphasised that conventionally used cryptographic technologies that are part of the QKD systems and may also be targeted by an attacker to achieve the same goal are not covered in this chapter.

Across the different groups (or even within one), two or more implementation attacks that may otherwise have a common theme, for instance, exploit the same imperfection in the QKD-

[1] The term side channel, which denotes the encoding of critical information in undesired degrees of freedom, is also sometimes used in this chapter, if and when it suitably fits the context.

[2] As arXiv.org is an open-access repository that allows uploading documents after moderation but without completing a peer review, the authors of this document have used their expertise to ensure only pre-prints and papers that comply with common quality standards have been considered.

specific components, or are described by the same modus operandi of the eavesdropper, have been categorised under a common category. Along the same lines, scientific works that share a common element or goal have been grouped together coherently in a single table to present the information in a concise manner. It should be noted that there are multiple ways of performing such grouping, and due to the massive size of the literature[3], a best effort has been made to find the optimal grouping.

Lastly, on the subject of attack ratings, a similar assessment but on a much limited scale—just one class of attack on one specific CV-QKD implementation—has been performed in **Kumar2021**.

Disclaimer on Proposed Countermeasures

As shown in the templates of Table 3.1 and Table 3.3, some details of the countermeasures proposed in the scientific literature to prevent the attack under discussion are also provided in the attack table. In order to be transparent about the effectiveness of countermeasures, i.e., to state that a certain set of countermeasures is more effective than another set, ideally, all of them should be compared and tested on the relevant physical QKD implementation. However, in this regard, as there is an unfortunate lack of literature[4], it is clear that making such statements is well beyond the scope of this document.

The objective for the authors involved in writing of this document was mainly to extensively survey and report their findings regarding countermeasures. For instance, in many cases, it would be observed that the entire chain of claims and counterclaims—on the effectiveness of a proposed measure—has been reported. To summarise, all countermeasures are in essence "proposed" without favouring one over the other. The only exceptions that have been pointed out are cases where it is obvious that a certain countermeasure would be highly impractical to implement, e.g., where it requires physical devices that are at the border of technical feasibility in the foreseeable future.

Finally, when calculating the attack rating (see Section 3.2), the influence of the proposed countermeasures has not been taken into account. The rating is based on the nature of the attack. When evaluating, the attack rating is determined based on the implementation of the TOE. Incorporating specific countermeasures into the implementation could, in theory, increase the attack rating. However, this action might inadvertently create new vulnerabilities or might not have any impact on the rating. By conducting more thorough and comprehensive testing of the countermeasures' limits, the actual effect can be more accurately determined.

[3] More than 300 scientific articles were reviewed for this study.

[4] Amongst the many possible reasons, one could be that the field of implementation attacks is still relatively immature. Or that this sort of research is more fit for engineering disciplines whereas QKD is still overwhelmingly pursued at scientific departments and research institutes.

4.1 DV-QKD Attack Tables

In this section, attack tables for implementation attacks that have been proposed and/or demonstrated against DV-QKD protocols and systems are listed.

Number	Attack Table Name
Table 4.2	Photon-number-splitting attack exploiting multi-photon signals
Table 4.3	Exploitation of double-click events
Table 4.4	Exploitation of breakdown flash (photons)
Table 4.5	Exploitation of detection efficiency mismatch
Table 4.6	Correlations due to dead time of APDs
Table 4.7	Timing attack via detector response time
Table 4.8	Phase-remapping attack
Table 4.9	Source attack of decoy-state QKD using phase information
Table 4.10	Frequency-shift attack
Table 4.11	Partially-random-phase attack
Table 4.12	Detector control of passively-quenched APDs via blinding and faked states
Table 4.13	Detector control of gated APDs via blinding and faked states
Table 4.14	Detector control of actively-quenched APD via blinding and faked states
Table 4.15	Detector control via after-gate pulses
Table 4.16	Detector control by exploiting superlinearity
Table 4.17	Detector control via blinding using dead time without interception
Table 4.18	Detector control by blinding of self-differencing APDs
Table 4.19	Detector control of SNSPD-based receivers
Table 4.20	Detector control of TES-based receivers
Table 4.21	Wavelength-dependent beamsplitter attack
Table 4.22	Passive Faraday mirror attack
Table 4.23	Timing mismatch of pump current modulation generated signal and decoy states
Table 4.24	Wavelength-selected photon-number splitting attack
Table 4.25	Attack on spatial information leakage from misaligned sources

Table 4.26	Free-space QKD system hacking by wavelength control using an external laser
Table 4.27	Exploiting passive side channels from imperfections in the transmitter
Table 4.28	Exploiting frequency side channels in sending or not-sending twin-field QKD with passive frequency-shift attack
Table 4.29	Trojan-horse attack against the SARG04 protocol
Table 4.30	Trojan-horse attack on counterfactual QKD
Table 4.31	Laser-damage attack on detectors in QKD systems
Table 4.32	Laser-damage attack against optical attenuators in QKD systems
Table 4.33	Pulse-intensity-increase in bidirectional QKD configurations
Table 4.34	Variation of laser's characteristics via temperature increase
Table 4.35	Injection-locking attack
Table 4.36	Information leakage through electromagnetic radiation

Table 4.1: List of DV-QKD attack tables

Name	Photon-number-splitting attack exploiting multi-photon signals		
Category	Photon-number-splitting attack		
Component	Transmitter	**Subcomponent**	Quantum signal
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Beyond High	**Attack Type**	Active
Protocol	Applicable to any DV-QKD protocol, except entanglement-based and DPR-type protocols. In the scientific literature referenced in this table, mainly BB84 and B92 protocols have been considered.		
Target(s)	Partial knowledge of the key		
Short Description	Exploiting multi-photon pulses from non-ideal single-photon sources to gain knowledge of the key.		
Precondition Public information	Use of non-ideal single-photon sources (see Section 2.4.3 for details).		
Equipment Non-existent equipment	Depending on the proposed PNS attack, different equipment has to be used: - **Brassard2000** uses a quantum memory, a photon-number quantum non-demolition (QND) measurement device, and a detection module. - The attacks proposed in **Felix2001** do not need a quantum memory. They require a detection module, an optical switch, and a signal state source that can emit arbitrary states at demand.		
Description	A description of the PNS attack is provided in Section 2.5.1. In this attack, first proposed in **Brassard2000** (see **Luetkenhaus2000** as well), Eve exploits multi-photon signals produced by non-ideal single-photon sources. Eve uses a QND measurement to retrieve the photon number of the signals emitted by Alice. Eve's intention is to split all multi-photon signals such that she retains one photon while Bob receives the remaining photons, while ensuring that the encoding remains undisturbed. By storing the photons in a quantum memory and measuring them later (once the bases are publicly announced), Eve obtains full information on the pulses that had contained more than one photon. While no errors are introduced in the sifted key, the photon statistics at Bob is altered. This problem is tackled in **Luetkenhaus2002** by a proposed extension to the PNS attack scheme, which preserves the Poissonian statistics. In **Felix2001**, two weaker and simpler versions of the PNS attack without the use of quantum memories are proposed. The first one is applying an intercept-and-resend strategy exploiting the increased information Eve can get from multi-photon signals. The second one is using a beamsplitter to couple out a fraction of each signal. A simplified single-basis encoding version of the PNS attack without the use of a quantum memory was experimentally shown in **Liu2011**.		

Description	Exploiting channel losses, Eve can block single-photon pulses and use a superior quantum channel, such that the number of non-empty signals received by Bob stays unchanged and Eve's information gain increases, as shown in **Felix2001** and **Liu2011**. **Mailloux2016** studies the use of quantum teleportation as a lossless channel and its improvement by entanglement purification. Additionally, the detectability of the PNS attack is examined with respect to both QBER and the decoy state protocol.
Proposed Countermeasures	The most effective and widely known countermeasure against PNS attacks is the decoy-state method (see Section 2.6.1). **Hwang2003** introduces the concept of using decoy states as a countermeasure to the PNS attack on BB84. Alice randomly replaces the quantum signal pulses with pulses of different intensities (decoy pulses). Then, Alice and Bob check the yield of the decoy pulses. If the yield of decoy pulses is abnormally high compared to that of other signal pulses, the whole protocol is aborted. **Lo2005** further improves the decoy-state method and gives a rigorous security analysis. In **Wang2005**, a modified decoy-state method using two weak-coherent states as signal pulses and vacuum for the decoy states is presented while considering non-asymptotic effects, thus changing the bounds on the security of the protocol. In **Liu2011** and **Mailloux2016**, it was shown via a proof-of-concept experiment and simulation, respectively, that the decoy-state method is able to discover the PNS attack effectively. Since the use of active intensity modulation for the production of decoy states is vulnerable to Trojan-horse attacks, passive decoy-state methods have been proposed and experimentally shown, using heralded single-photon sources in **Sun2014a**, or two local detectors inside the QKD transmitter [**Yu2022**]. Other specific countermeasures: - Use heralded SPDC photons to get sub-Poissonian photon statistics [**Brassard2000**] (see Section 2.4.3). - Use quantum repeaters to reduce channel loss and minimise the possibility of Eve blocking signals [**Brassard2000**]. - Reduce the mean photon number per pulse such that the amount of multi-photon pulses is reduced accordingly[5] [**Brassard2000**]. - Incorporate PNS attacks in the security proofs and in the calculation of the secure key rate leading to a proper amount of privacy amplification [**Gottesman2004**]. - Encoding on the phase of a weak-coherent pulse relative to a strong reference pulse [**Koashi2004**, **Tamaki2009**]. Using a strong pulse prevents Eve from blocking the entire signal without causing errors, and is expected to be robust against channel loss. - Using a modified BB84 protocol with non-orthogonal states proposed in **Scarani2004**. It differs only in the classical sifting procedure. Instead of revealing the basis, Alice announces one of four pairs of non-orthogonal states. - Using a frequency coding scheme [**Gabdulkhakov2018**] can partially inhibit the PNS attack.

[5] However, this also leads to an overall reduction of the secure key rate and/or the transmission distance.

Remarks	The attack paths presented in **Brassard2000** and **Felix2001** require equipment that is not available today, namely quantum memory in **Brassard2000** and signal state source that can emit arbitrary states at demand as well as perfectly number-resolving detectors in **Felix2001**. Also, we note that the attack presented in **Felix2001** is a much simpler and weaker version than the original PNS attack. Furthermore, the attack described in **Liu2011** is only a simplified proof-of-principle version of the PNS attack.
Feasibility $t_{Attack} < 1$ day	None of the proposed PNS attacks have been fully demonstrated on a working QKD system due to the need for future technologies. A simplified one-basis encoding version of the PNS attack without the use of a quantum memory was experimentally shown in **Liu2011**.
Reference(s)	**Brassard2000**, **Luetkenhaus2000**, **Felix2001**, **Luetkenhaus2002**, **Hwang2003**, **Gottesman2004**, **Koashi2004**, **Scarani2004**, **Lo2005**, **Wang2005**, **Tamaki2009**, **Liu2011**, **Sun2014a**, **Mailloux2016**, **Gabdulkhakov2018**, **Yu2022**

Table 4.2: Photon-number-splitting attack exploiting multi-photon signals

Name	Exploitation of double-click events		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Detection module
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to BB84 but the attack should also be applicable to non-MDI-type prepare-and-measure QKD protocols using 2 or more detectors.		
Target(s)	Partial knowledge of the key		
Short Description	Exploiting double-click events at the receiver to gain knowledge of the key.		
Precondition Public information	Bob discards all double-click events during sifting.		
Equipment Specialised equipment	Detection module, source, and state preparation module to perform an intercept-and-resend attack.		
Description	A double click refers to an event where there is a (simultaneous) click in both detectors of a given basis. In a double-click attack, Eve chooses an intercept-and-resend strategy (see Section 2.5.2), with the re-sent state being a relatively intense pulse containing multiple photons. If Bob chooses a basis compatible with that of the re-sent state, he obtains a definite measurement outcome. If not, a double-click event occurs with a probability close to 1. With this, if double clicks are simply discarded by the QKD system, all the remaining clicks are those that were fully controlled by Eve and therefore she can get information about the complete key [**Luetkenhaus1999**, **Luetkenhaus2000**].		
Proposed Countermeasures	Incorporate the effect of multiple clicks and detector dead-time at Bob's side in the QKD security proof. For example, one could randomly assign multiple clicks to single-click events before applying the security proof [**Beaudry2008**, **Fung2011**], or monitor the rate of multiple click events observed [**Koashi2008**]. Importantly, multiple clicks cannot be simply discarded.		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.		
Reference(s)	**Luetkenhaus1999**, **Luetkenhaus2000**, **Beaudry2008**, **Koashi2008**, **Fung2011**		

Table 4.3: Exploitation of double-click events

Name	Exploitation of breakdown flash (photons)		
Category	Detector-backflash attack		
Component	Receiver	**Subcomponent**	APD
Expertise	Proficient	**Opportunity**	Moderate
Attack Rating	Basic	**Attack Type**	Passive
Protocol	BB84 with polarisation encoding is explicitly mentioned. Others (e.g. BBM92, Ekert91) are vulnerable as well.		
Target(s)	Partial knowledge of the key		
Short Description	Eavesdropping on photons that get emitted as a result of detection events in Bob and travel out to the quantum channel.		
Precondition Public information	- The receiver uses APDs in Geiger mode. - Photons from the breakdown flash carry information about the encoding, such as timing directly (e.g. in time-bin encodings) or by traversing a characteristic optical path (e.g. with polarising elements in polarisation enconding). - Imperfect pointing of the receiver towards the QKD transmitter [Kepferman2018, Arnon2019].		
Equipment Standard equipment	- Device to gain access to backflash photons (e.g., circulator). - Receiver module, similar to that of Bob.		
Description	The phenomena of breakdown flash (also called backflash) in APDs described in Section 2.4.1.1 can result in a security vulnerability. By observing the photons emitted in the breakdown flash, as they leak back to the quantum channel, Eve can obtain information about the settings of the QKD system that may enhance her knowledge of the secret key [Kurtsiefer2001]. To elaborate, Eve may be able to identify which detector the backflash photons originated from by extracting polarisation and timing information. Notably, this attack can be done without alerting the QKD users. In Kurtsiefer2001, light emission from a free-space Si APD (C30902-SDTC from PerkinElmer; now Excelitas Technologies) was analysed with respect to absolute number of photons and spectral, spatial, and temporal distribution. For instance, the authors reported (among other results) that on average 1.3×10^{-3} photons were found to be coupled back into the single spatial mode of the quantum channel. In Meda2017, Meda2018 and Shi2017, InGaAs/InP APDs were analysed in a similar manner. In Meda2017, Meda2018, two gated, fibre-coupled detectors, one a home-built prototype and another a commercially available model (ID201 from ID Quantique), were evaluated quantitatively. An average backflash photon number of 0.04 was the main result obtained in Shi2017 (on ID220 from ID Quantique). It was shown in Pinheiro2018 that > 6.5% of detection events in an actively quenched free-space Si APD module (from Excelitas)		

Description	resulted in a backflash. A proof-of-concept setup using a polarisation analyser for eavesdropping on these backflash photons was also implemented here, and an information leakage was 4.5×10^{-3} was experimentally quantified. The authors also investigated a photo multiplier tube (PMT) (from Hamamatsu) and found that no significant backflash emission could be registered. A special case (of a free-space QKD link) in which backflash photons are not always directed back towards the transmitter telescope due to non-ideal pointing is investigated in **Kepferman2018** and **Arnon2019**. This can get manifested when the receiver is mounted on a vibrating platform (e.g., a satellite).
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using optical isolation **(C1)** and spectral filtering **(C4)**. For instance, in **Kurtsiefer2001**, it is estimated that a commercial 1 nm full-width half-maximum (FWHM) wide interference filter could reduce the intensity of the backflash by a factor of 170. In **Meda2017** and **Meda2018**, the usage of an isolator is recommended to bring down the intensity of backflash by 30 dB. - Using newer QKD protocols **(C9)**. Specific countermeasures include: - Lowering the parasitic capacitance of the APDs [**Kurtsiefer2001**]. - Spatial filtering in case of free-space APDs, since the emission is not assumed to be directed [**Kurtsiefer2001**]. - **Shi2017** conjecture that SNSPDs do not exhibit this property of backflash. - Using directional coupler or narrow filter [**Arnon2019**]. - Usage of PMTs instead of APDs [**Pinheiro2018**] though this measure has limitations (as also mentioned by the authors).
Remarks	If Eve does not know the chosen basis beforehand, a polarisation analysis of the (single) backflash photons yields her only partial information, except when she has a quantum memory to store the photons (and perform measurements on them during the classical phase of the protocol).
Feasibility $t_{Attack} < 1$ day	This vulnerability has been shown to manifest on both research and commercial APD modules. It is expected to work on similar implementations. An attack path has been presented in **Pinheiro2018** via proof-of-concept experiments.
Reference(s)	**Kurtsiefer2001**, **Shi2017**, **Meda2017**, **Meda2018**, **Pinheiro2018**, **Kepferman2018**, **Arnon2019**

Table 4.4: Exploitation of breakdown flash (photons)

Name	Exploitation of detection efficiency mismatch		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any QKD protocol where the detector(s) exhibit a mismatch in some property of the optical signals on the quantum channel that Eve can access. Investigated so far on BB84 (both with and without decoy states) [**Makarov2006**, **Qi2007**, **Fei2015**], energy-time entanglement protocol [**Makarov2005**], SARG04, DPSK and Ekert protocols [**Makarov2008a**].		
Target(s)	Complete knowledge of the key Enabling other attacks		
Short Description	Enabling and exploiting side channels that allow Eve to discriminate between the detectors of Bob (and thus control them) using polarisation, spatial, and temporal DOFs.		
Precondition Public information	Detection efficiency mismatch may exist as a function of - Polarisation, e.g., in the passive basis choice using PBS [**Makarov2005**], - Time, e.g., in gated detectors (more than one, but possibly also time-multiplexed [**Makarov2006**]), - Angle at which the beam impinges on free-space detectors [**Rau2015**, **Sajeed2015a**], or it can be induced, e.g., by exploiting a flaw in the calibration routine of the detection system [**Jain2011**].		
Equipment Specialised equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - Pulsed lasers for preparing faked states (Faked-states generator) [**Liu2014**]. - Possibly (for decoy state BB84) photon-number resolving detectors [**Fei2015**].		
Description	Any DV-QKD receiver that decodes a secret bit by assigning the detection outcome to a unique detector (or unique set of detectors) needs to ensure operational indistinguishability between all the detectors. When this is not the case, the QKD system suffers from detection efficiency mismatch. If Eve can additionally exploit the distinguishability, then the security of the QKD system can be compromised. Several such attacks have indeed been performed using the temporal, spatial, and polarisation DOFs. A temporal detection efficiency mismatch could occur, e.g., due to small differences in the optical path lengths to the detectors [**Makarov2006**]. In case of gated APDs (see Section 2.4.1.1), this results in the gating windows to not completely overlap, i.e., one (or more) detector(s) become active slightly before or after		

Description	the other one(s). A detector-control attack using faked states (see Section 2.5.2.1 for more details) can then completely break the security of the QKD system [**Makarov2005**, **Makarov2006**]. In **Qi2007**, the authors proposed a time-shift attack (experimentally demonstrated in [**Zhao2008**] on a modified ID-500 QKD setup by ID Quantique), where, by temporally delaying or advancing the quantum signals from Alice to Bob, Eve controllably addressed only one of the two gated APDs. The efficiency mismatch in **Zhao2008** was, however, neither too severe nor constant or deterministic—it fluctuated, and in a way that was beyond Eve's control. In **Jain2011**, a strategy to induce a large and predictable mismatch was outlined and experimentally demonstrated, together with simulating the performance of a faked-states attack. The demonstration exploited a flaw in the calibration routine[6] running on the ID Quantique Clavis2 QKD system. In the case of free-space QKD setups, the detection efficiency of the different single-photon detectors can depend on the spatial mode of the incident light. Such a spatial detection efficiency mismatch was experimentally investigated in **Rau2015** and **Sajeed2015a**, with the authors of the latter also evaluating the angles that maximised the detection efficiency mismatch to simulate the faked-states attack that minimises the QBER incurred by Bob. The results from **Sajeed2015a** were extended to a more realistic domain in **Chaiwongkhot2019** where the authors emulated atmospheric turbulence using a spatial light modulator. For efficiency mismatch in the polarisation domain, Eve's task is to find the critical states of polarisation that help her discriminate among the detectors in Bob. As shown in **Makarov2005**, if the basis choice in Bob is implemented in a passive manner, e.g., using a PBS (see Section 2.4.4.3), Eve could launch faked states containing polarised photons that produce a click in the detector she desires. The natural polarisation sensitivity of a SNSPD with meander-type geometry was shown in **Wei2019a** to create grounds for attacks exploiting a polarisation-dependent mismatch.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent attacks that exploit detection efficiency mismatch or those that induce this vulnerability. These include: - Incorporating the flaw in the security analysis **(C5)** or using newer QKD protocols **(C9)**. - Using wavelength filters **(C4)** to minimise vulnerabilities arising from the wavelength-dependence of components. - Using the technique of bit-mapped gating **(C12)**. - Randomly assigning each detector to different bit values per received quantum signal [**Qi2007**, **Silva2015**]. However, this detector-scrambling countermeasure requires a phase modulator [**Qi2007**] or detectors [**Silva2015**] which, apart from being extra hardware, may actually prove ineffective [**Makarov2008a**, **Fatin2021**], e.g., due to

[6] Similar attacks on the calibration sequence exploiting additional vulnerabilities such as the wavelength dependence of beamsplitters [**Fei2018b**] are reported in Table 4.21.

Proposed Countermeasures	the possibility of Trojan-horse attacks on DV-QKD receivers [**Jain2014**] (also see Table 4.29). Specific measures against the mismatch in temporal DOF: - Introducing an intentional random jitter in the detector synchronisation. Active protection can be achieved through random shifting of the receivers detection time window [**Makarov2006**]. - Monitoring QBER and coincidence statistics [**Makarov2008a**]. It is mentioned that this countermeasure could make the attack more difficult but not impossible. - Applying additional randomised phase shifts at the entry of the QKD receiver is expected to inhibit this attack from being successful [**Qi2007**]. Specific measures for the mismatch in spatial DOF: - Both **Sajeed2015a** and **Rau2015** propose using a single-mode spatial filter, e.g., pinhole, as a countermeasure to block unwanted spatial modes from an attacker. However, this is not immune to a laser-damage attack: A pinhole was thermally damaged with a high-power laser and rendered useless in **Makarov2016**. Specific measures against the polarisation-dependent mismatch: - Implementing active polarisation state scrambling inside the QKD receiver [**Makarov2005**, **Wei2019a**]. - Developing polarisation-insensitive SNSPDs [**Wei2019a**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work in laboratories and on commercially available systems. It is expected to work on similar implementations.
Reference(s)	**Makarov2005**, **Makarov2006**, **Qi2007**, **Zhao2008**, **Makarov2008a**, **Jain2011**, **Jain2014**, **Liu2014**, **Fei2015**, **Sajeed2015a**, **Rau2015**, **Silva2015**, **Makarov2016**, **Fei2018b**, **Wei2019a**, **Chaiwongkhot2019**, **Fatin2021**

Table 4.5: Exploitation of detection efficiency mismatch

Name	Correlations due to dead time of APDs		
Category	Timing attack		
Component	Receiver	**Subcomponent**	APD[7]
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Basic	**Attack Type**	Passive
Protocol	Applicable to QKD protocols that use free-running APDs for single-photon detection[8]. Specifically, BB84 [**Xu2006**, **Rogers2007**] and B92 [**Xu2006**] are discussed.		
Target(s)	Partial knowledge of the key		
Short Description	The imposition of dead times across multiple APDs can induce correlations in the sifted key, especially when the detection rates are high.		
Precondition Public information	- Free-running APDs that exhibit a dead time. - More than one APD is used in the detection process, possibly one detector per bit value in each basis [**Rogers2007**]. - Increased impact, if repetition rate is higher than the inverse dead time [**Rogers2007**].		
Equipment Standard equipment	None		
Description	In this table, the focus is on passively quenched APDs, which are described in Section 2.4.1.1. There, the term dead time is also defined. The theoretical maximum event rate an APD based single photon detector can register is the inverse of the dead time. When one APD is inactive due to the dead time, only the other one(s) can detect a photon. In high repetition rate scenarios, this can lead to (anti-)correlations of the sifted key, since the detector(s) that lead to the opposite sifted key bits of the previous detection are active, while that one is not. As shown in **Xu2006**, the B92 protocol is especially vulnerable: The probability that the neighboring bits are different ought to be 0.5, but at high repetition rates, this can surpass 0.9. A BB84 protocol implementation with 4 detectors similarly approaches a probability of 0.62. This has been shown in a simulation with experimental verification of data points [**Xu2006**, **Rogers2007**]. It is assumed (as usual in scientific QKD scenarios) that the eavesdropper has full read access to the classical channel and thus has at least some information about the detection times and basis choices later on during the post-processing phase. This information only is used for this attack.		

[7] Effectively, all threshold (i.e., binary) single-photon detectors have some sort of dead time. So, this attack will also be applicable to other types of detectors to some degree.

[8] See previous footnote.

Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using newer QKD protocols (**C9**). Other specific countermeasures include: - All detectors shall be held off, while one is inactive. They call this simultaneous hold-off of APDs [**Xu2006**]. - Self-disabling detector by time-multiplexing the different bit values in each basis on one physical detector [**Rogers2007**].[9] - Modified sifting algorithm: Whenever there are detection events closer in time than the dead time, only the first detection event is considered [**Rogers2007**].
Remarks	It is theoretically possible to design a QKD system with only one APD. Such a system would not necessarily suffer from this vulnerability, but a tailored security analysis would be needed. Hence the added assumption, that the device has to be comprised of more than one APD. The authors assume that the dead time is fixed and not extendable and hence cannot be paralysed with the exception of "twilight counts" (see reference 16 in **Rogers2007**). This assumption is not necessarily tenable for passively-quenched APDs where the APD is slowly charged and a discharge can be triggered, although there is no detection event, because the smaller electrical pulse will not switch the state of the discriminator that usually follows. Other types of detectors might also be affected by this attack.
Feasibility $t_{Attack} < 1$ day	This attack is of theoretical nature and has not been demonstrated on a working device.
Reference(s)	**Xu2006**, **Rogers2007**

Table 4.6: Correlations due to dead time of APDs

[9] Time-multiplexed detectors exhibit other vulnerabilities though, see 4.5.

Name	Timing attack via detector response time		
Category	Timing attack		
Component	Receiver	**Subcomponent**	Detector
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Passive
Protocol	The scientific literature has considered the BB84 and BBM92 protocols. The attack could potentially also be applied to other non-MDI-type QKD protocols that exchange detectors' timing information.		
Target(s)	Partial knowledge of the key		
Short Description	Achieving partial knowledge of "which detector clicked" using the publicly communicated detection times.		
Precondition Public information	There must be a difference between the detector response times and the timestamps have to be published.		
Equipment Standard equipment	Equipment to get access to the timing information of the detectors by accessing the classical communication channel.		
Description	The timing attack was proposed by **LamasLinares2007**. The identification of a signal photon from background noise is achieved through the measurement of its arrival time at one of the detectors. However, in QKD implementations, correlations between such timing information (which is publicly exchanged) and the resulting measurement outcomes can occur owing to differences in the detector response times or optical path length differences. These correlations can be exploited by Eve to obtain the secret (which detector clicked) information about the key.		
Proposed Countermeasures	- Timing information should be properly characterised, delays equalised, and publicly exchanged information should be randomised or truncated in precision to limit the information leakage [**LamasLinares2007**]. Only Alice should share the timestamps and deployed bases info on the public channel and Bob should minimise distinguishability in his detection system. - Arbitrarily increasing the time bin width is also proposed in **LamasLinares2007** as a countermeasure. However, **Pahali2022** have shown that this countermeasure can lead to an increasing mutual information. It is important to use the right values for time bin width and start time of binning to successfully decrease the mutual information to a minimum. - Using newer QKD protocols (**C9**).		
Remarks	-		
Feasibility $t_{Attack} < 1$ month	A proof-of-concept version of this attack has been shown to work in laboratories [**LamasLinares2007**]. It is expected to work on similar implementations.		

Reference(s)	**LamasLinares2007**, **Pahali2022**

Table 4.7: Timing attack via detector response time

Name	Phase-remapping attack		
Category	Phase-remapping attack		
Component	Transmitter	**Subcomponent**	Optical modulator
Expertise	Expert	**Opportunity**	Difficult
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to certain QKD protocols that use phase coding. For illustration purposes, so far the scientific literature has mainly considered the BB84 and the SARG04 protocols.		
Target(s)	Complete knowledge of the key		
Short Description	Tampering the quantum signal encoding process in Alice to enforce the prepared states to deviate from those of the ideal protocol, which can be exploited by Eve in an intercept-and-resend attack.		
Precondition Public information	- Operating QKD protocol in a bidirectional configuration, or phase calibration through active phase compensation in a unidirectional configuration. - Use of optical modulators (e.g., phase modulators) to encode the bit and basis information of the emitted quantum signals.		
Equipment Specialised equipment	- Bidirectional QKD configuration (e.g., “plug-and-play”): Setup similar to that of Bob to replace the pulses from (legitimate) Bob with those having specific properties, e.g., adjustable arrival times at Alice’s modulator. In a Sagnac setup, Eve modifies the lengths of the two arms of the Sagnac interferometer. - Unidirectional QKD configuration: Phase modulator. - Intercept-and-resend attack apparatus.		
Description	The basic idea of a phase-remapping attack is to manipulate the phase encoding process of Alice, which can then be exploited through an effective intercept-and-resend attack (see Section 2.5.2). In a bidirectional QKD setup, Bob sends relatively strong laser pulses to Alice, who encodes her information on the received signals, attenuates them to single-photon level, and sends them back to Bob. To implement this attack, Eve replaces Bob’s pulses with those prepared by herself to manipulate Alice’s state preparation process. In particular, Eve can enforce Alice’s phase modulator to remap the BB84 phases $\{0, \pi/2, \pi, 3\pi/2\}$ to some phases $\{0, \delta_1, \delta_2, \delta_3\}$ in a controllable manner [**Fung2007**]. In a plug-and-play QKD configuration, this can be achieved by adjusting the properties, e.g., the polarisation and/or arrival time at Alice’s phase modulator, of the pulses that Eve sends to Alice. In a Sagnac-loop configuration, Eve could modify the lengths of the two arms of the Sagnac interferometer to change their fibre length difference. Note that the relative phase between each pair of pulses encoding a signal depends on such fibre length difference. The flawed signals prepared by Alice allow Eve to launch an improved intercept-and-resend attack.		

Description	In **Fung2007**, phase-remapping attacks have been considered against the BB84 and the SARG04 protocols, for both single-photon states and weak-coherent states (see Section 2.4.3.2), and assuming both plug-and-play and Sagnac QKD configurations. In general, it has also been experimentally shown in **Xu2010** that the QBER incurred in those attacks is lower than the threshold dictated by some security proofs [**Chau2002**, **Gottesman2004**, **Fung2006**]. A similar remapping effect can be achieved in unidirectional QKD setups that implement active phase compensation [**Dong2014**]. By modifying the phase of the calibration signals exchanged between Alice and Bob, Eve induces Alice to apply a wrong phase during state preparation.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**). - Monitoring state preparation (**C7**) and incorporating the encoding flaws in the security analysis (**C5**). Specific countermeasures include the monitoring of the detection statistics of all BB84 states to avoid that Eve tries to minimise the QBER (incurred due to the attack) by sending Bob only a subset of the BB84 states [**Fung2007**, **Xu2010**]; or, in unidirectional QKD setups, do not calibrate the phase modulator amplitudes for the different phases in the field but in a controlled environment.
Remarks	-
Feasibility $t_{Attack} < 1$ day	A proof-of-principle experiment against a commercial QKD setup using a plug-and-play configuration has been reported in **Xu2010**.
Reference(s)	**Chau2002**, **Gottesman2004**, **Fung2006**, **Fung2007**, **Xu2010**, **Dong2014**

Table 4.8: Phase-remapping attack

Name	Source attack of decoy-state QKD using phase information		
Category	Non-random phase attack		
Component	Transmitter	**Subcomponent**	Quantum signal (weak-coherent state)
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Beyond-High	**Attack Type**	Mixed
Protocol	Applicable to BB84 with decoy states.		
Target(s)	Partial knowledge of the key		
Short Description	A PNS-based attack applicable to decoy-state-based BB84 protocols if the relative phase of the emitted states is not randomised.		
Precondition Public information	- QKD transmitter generates weak-coherent states (see Section 2.4.3). - Non-randomised phase relation between pulses.		
Equipment Non-existent equipment	- Interception apparatus with the capabilities to perform unambiguous state discrimination (USD) measurements and quantum non-demolition photon-number-resolving measurements. - Lossless quantum channel.		
Description	If the global phase of a quantum state is not randomised, Eve can perform a USD measurement to distinguish between signal and decoy states without disturbing the quantum states sent by Alice [**Tang2013a**]. In practice, a USD measurement was shown by **Tang2013a** on a phase-encoded BB84 scheme with decoy states. Here, the information is encoded in the relative phase of a bright reference pulse and a dim secondary pulse. Since the global phase of the bright reference pulse is known, a USD measurement can be performed on only the bright reference pulse, for example using interferometry. This enables Eve to perfectly distinguish between decoy and signal states with a known probability $1 - p_f$, without destroying the quantum information still present in the secondary pulse. Here, the failure probability p_f is determined by the overlap of the two states, which are to be distinguished using the USD measurement (see **Tang2013a** for details). This information can be used to apply a PNS attack (see Table 4.2), which is thus contrarily not hindered by the decoy-state scheme. Therefore, the security of the key can be compromised using this attack.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Active randomisation of the phase (**C6**). - Incorporate the imperfection, i.e., imperfect phase randomisation, in security proof (**C5**). Other specific countermeasures include: - Passive phase randomisation [**Yuan2007**], e.g., by operating the laser in a gain-switched mode instead of pulse carving.		

Remarks	This attack only applies to QKD transmitters generating weak-coherent states (see Section 2.4.3.1). Single-photon sources emit Fock states which intrinsically have a randomised phase. PNS attacks, which are necessary for this attack, are beyond current technology.
Feasibility $t_{Attack} < 1$ day	This attack has not been demonstrated on a practical QKD system. However, the USD measurement on a decoy state BB84 scheme was shown in **Tang2013a**.
Reference(s)	**Yuan2007**, **Tang2013a**

Table 4.9: Source attack of decoy-state QKD using phase information

Name	Frequency-shift attack		
Category	Phase-remapping attack		
Component	Transmitter	**Subcomponent**	Phase modulator
Expertise	Proficient	**Opportunity**	Difficult
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to bidirectional QKD protocols that use phase coding. For illustration purposes, so far the scientific literature has considered the BB84 protocol implemented on a “plug-and-play” setup.		
Target(s)	Complete knowledge of the key		
Short Description	In a bidirectional QKD configuration, Eve replaces Bob’s optical pulses with time-shifted pulses which get modulated on the rising edge of Alice’s phase modulator. The resulting frequency of Alice’s modulated signals depends on the state encoded, allowing Eve to implement an effective intercept-and-resend attack.		
Precondition Public information	- Use of a QKD setup with a bidirectional configuration. - Use of phase modulators to encode the bit and basis information of the emitted quantum signals.		
Equipment Specialised equipment	- Receiver module similar to Bob’s. - Quantum transmitter. - Optical frequency/wavelength measurement module.		
Description	Frequency-shift attacks belong to the class of phase-remapping attacks (see Table 4.8) where the basic idea is to manipulate the phase encoding process in Alice, which can then be exploited through an effective intercept-and-resend attack (see Section 2.5.2). In a bidirectional QKD setup, Bob sends relatively strong laser pulses to Alice, who encodes her information on the received signals, attenuates them to single-photon level, and sends them back to Bob. In a frequency-shift attack, Eve replaces Bob’s strong laser pulses with other time-shifted pulses. The goal is to ensure that Alice modulates the received signals on the rising edge of her phase modulator (instead of in the plateau region) [**Jiang2014**]. This produces a frequency shift of the modulated signals, which is dependent on the BB84 state selected by Alice. In an intercept-and-resend attack, Eve can then identify Alice’s emitted states by simply measuring their frequency and sending the identified signals to Bob. Frequency-shift attacks were introduced in **Jiang2014** against a phase-coding BB84 protocol operating in a plug-and-play configuration. In contrast to remapping the phase, the goal to shift the frequency of Alice’s signals here is more powerful, as it can provide Eve full information about the key, while the QBER incurred by Bob is negligible, even if one considers a realistic scenario in which Eve’s laser has a finite linewidth.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include:		

Proposed Countermeasures	- Using watchdog detectors (**C2**). - Using a narrow spectral filter to ensure that only signals with the correct frequency exit Alice's device (**C4**). - Monitoring state preparation (**C7**) and incorporating the imperfection, i.e., distinguishability in signal frequency, in the security analysis (**C5**). Specific countermeasures include triggering Alice's phase modulator with the bright light pulses that she receives.
Remarks	Similar ideas could be applied to a Sagnac-QKD configuration. See Table 4.24 for a related attack.
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Jiang2014**

Table 4.10: Frequency-shift attack

Name	Partially-random-phase attack		
Category	Phase-remapping attack		
Component	Transmitter	**Subcomponent**	Phase modulator
Expertise	Expert	**Opportunity**	Difficult
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to bidirectional QKD protocols that use active phase randomisation. The scientific literature has considered the (decoy-state) BB84 protocol with phase coding in a plug-and-play configuration.		
Target(s)	Complete knowledge of the key		
Short Description	Tampering with the active phase randomisation process in Alice and exploiting it through an effective intercept-and-resend attack.		
Precondition Public information	- Use of a QKD setup with a bidirectional configuration. - Use of a phase modulator for active phase randomisation.		
Equipment Bespoke equipment	- Setup similar to that of Bob to replace the pulses from (legitimate) Bob with those having specific properties, e.g., adjustable arrival times at Alice's modulator. - Intercept-and-resend attack apparatus (using homodyne detection in **Sun2012**).		
Description	Partially-random-phase attacks belong to the class of phase-remapping attacks (see Table 4.8) where the basic idea is to manipulate the phase encoding process in Alice, which can then be exploited through an effective intercept-and-resend attack (see Section 2.5.2). In a bidirectional QKD setup, Bob sends relatively strong laser pulses to Alice, who encodes her information on the received signals, attenuates them to single-photon level, and sends them back to Bob. In a partially-random-phase attack, Eve replaces Bob's laser pulses with pulses prepared by herself to manipulate Alice's active phase randomisation process. The goal is to ensure that Alice modulates Eve's pulse on the rising edge of her phase modulator (instead of in the plateau region) [**Sun2012**]. In doing so, the global phase of Alice's emitted signals is no longer randomly distributed in [0,2π] but its range is reduced to [0,δ] with $\delta < 2\pi$ controlled by Eve. Next, Eve uses an intercept-and-resend attack against the flawed signals prepared by Alice. A partially-random-phase attack against a phase-coding BB84 protocol (with and without decoy states) in a plug-and-play configuration was introduced in **Sun2012**. There, the authors considered a specific intercept-and-resend attack for Eve which had a trade-off between the incurred QBER by Bob and Eve's probability to identify Alice's states correctly (using homodyne detection). It was also demonstrated how this attack may be able to compromise the security of one-decoy-state BB84.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include:		

Proposed Countermeasures	- Using watchdog detectors (**C2**). - Monitoring state preparation (**C7**) and incorporating the flaws found in the active phase randomisation process in the security analysis (**C5**). - Using the decoy-state method with three intensity settings, one of them being vacuum. It is argued in **Sun2012** that this countermeasure is robust against the specific intercept-and-resend attack based on homodyne detection considered in that paper. However, the intercept-and-resend attack introduced in **Sun2012** might not be optimal. Indeed, in **Sun2014** the authors presented an alternative approach to defeat a decoy-state method with three intensity settings, but the analysis turned out to be incorrect [**Sun2018**]. - Triggering Alice's phase modulator with the bright light pulses that she receives.
Remarks	In active phase randomisation, only a discrete number of phases is selected. However, the analysis in **Sun2012** assumes, for simplicity, that the phases are uniformly distributed in a certain interval. In addition, the time-shifted signals that Eve sends to Alice might also remap the BB84 states to slightly different states, like in the phase-remapping attack [**Fung2007**]. This effect has not been considered in **Sun2012**.
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Fung2007**, **Sun2012**, **Sun2014**, **Sun2018**

Table 4.11: Partially-random-phase attack

Name	Detector control of passively-quenched APDs via blinding and faked states		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Passively-quenched or negative-feedback APD
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Multiple protocols are potentially vulnerable. So far, it has been applied to BB84 (with or without decoy-states), SARG04, B92, Ekert91, six-state protocol [**Makarov2009**], BBM92 [**Gerhardt2011**].		
Target(s)	Complete knowledge of the key		
Short Description	By blinding passively-quenched APDs, an adversary can render them insensitive to single photons and then produce controlled detection events by using faked states.		
Precondition Public information	Passively-quenched APDs or negative-feedback active diode detectors in the QKD receiver.		
Equipment Bespoke equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - CW lasers to blind the APDs and pulsed lasers for preparing faked states (faked-states generator [**Liu2014**]). In general, the ability to change the DOF (e.g. polarisation) of the lasers so that APDs can be selectively blinded is required. This can be obtained via a modulator or a set of lasers.		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Amongst all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on passively-quenched APDs, which are described in Section 2.4.1.1. A constant illumination of all APDs is used to blind them, i.e., make them insensitive to single photons. When the attacker wants to trigger a detection event in a particular APD, one of the following methods can be chosen: - The CW illumination is changed so that exactly one APD becomes active. For example, in a polarisation-coding scheme, the polarisation DOF would be used so that only a desired APD is sensitive to single photons. Shortly after that, the illumination is reverted to full blinding mode, so that if a detection event was registered, it could only have been from the targeted APD [**Makarov2009**]. - An additional "faked-state" pulse is applied to control the detection outcomes, as explained in Section 2.5.2.1.		

Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**). - Monitoring the electrical parameters (**C10**). Specific to passively-quenched APDs, **Makarov2009** proposes to process detection signals only if all APDs have a minimum detection efficiency. - Using the technique of bit-mapped gating (**C12**) and monitoring the sensitivity of the single-photon detector (**C13**). - Using newer QKD protocols (**C9**) or novel QKD receiver configurations (**C18**). Other specific countermeasures include: - The use of authenticated timing in QKD is introduced and immediately rejected, since the author proposes a way to get around it [**Makarov2009**].
Remarks	A similar method is used in **Gerhardt2011a** to fake the violation of Bell's inequality. This is a crucial component of inter alia the Ekert91 and device-independent QKD protocols. Other types of detectors might also be affected by this attack.
Feasibility $t_{Attack} < 1$ day	**Makarov2009** demonstrates the possibility to blind three different models of passively-quenched APDs, while **Gras2020** focuses on so-called negative-feedback avalanche diodes. An attack targeting the BBM92 protocol has been fully implemented in **Gerhardt2011**.
Reference(s)	**Makarov2009**, **Gerhardt2011**, **Gerhardt2011a**, **Liu2014**, **Gras2020**

Table 4.12: Detector control of passively-quenched APDs via blinding and faked states

Name	Detector control of gated APDs via blinding and faked states		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Gated APD
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use APDs in gated mode for single-photon detection. Specifically, SARG04 and BB84 (both with and without decoy states), DPS and COW are discussed in **Lydersen2010a**, **Lydersen2010c**, **Lydersen2011a** and **Alhussein2019**, round-robin differential-phase-shift (DPS) in **Iwakoshi2015**; subcarrier-wave QKD is attacked in **Chistiakov2019**.		
Target(s)	Complete knowledge of the key		
Short Description	Controlling the detection outcomes in the QKD receiver through tailored illumination (CW and/or pulsed light).		
Precondition Public information	- Gated mode operation of the APDs. - APDs can be forced to be in linear mode by excessive illumination via blinding [**Lydersen2010a**] or heating [**Lydersen2010c**]. Specific assumptions in **Lydersen2010a**: - Resistor in series with APD, that leads to a restriction of the (re-)charge current.		
Equipment Bespoke equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - CW lasers to blind the APDs and pulsed lasers for preparing faked states, e.g., the faked-states generator [**Liu2014**].		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Among all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on APDs operating in gated mode, which is described in Section 2.4.1.1. The general idea of this attack is very similar to the one described in Table 4.12. The gated APDs considered here are forced to be in linear mode (instead of Geiger mode) by two possible mechanisms that involve illumination with bright light. In **Lydersen2010a** and **Chistiakov2019**, the APDs are almost instantly blinded by intense CW light, while in **Lydersen2010c**, light is used to heat the APDs but the result of this “thermal blinding” is the same, even if delayed. In **Wu2020**, pulsed light is used to blind the detectors. Simultaneously, Eve performs the faked-state attack (see Section 2.5.2.1) to conditionally produce detection events in Bob. Depending on the protocol, the exact implementation can vary. For instance, in the (round-robin) DPS case [**Iwakoshi2015**], Eve would have to send a pulse train (at least always two pulses in		

Description	series) with a carefully defined relative phase depending on which of the detectors she wants to trigger. This can lead to full knowledge of the (sifted) key. The strategies can be optimised according to Bob's basis choice (active or passive).
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors **(C2)**. - Monitoring the electrical parameters **(C10)** and the photocurrents **(C11)** of the APDs. - Using the technique of bit-mapped gating **(C12)** and monitoring the sensitivity of the single-photon detector **(C13)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**. Other specific countermeasures include: - Gain modulation (gating) is expected to work as a countermeasure against thermal blinding in **Yuan2010**. - Using an additional DOF for checking whether the photon has been intercepted and resent [**Hegazy2022**]. - The APDs under scrutiny (in Clavis2 [**Lydersen2010a**, **Lydersen2010c**] and QPN 5505 [**Lydersen2010a**]) have a bias resistor with rather high impedance in the charging path of the APD, which was claimed to be the culprit leading to optical blinding in **Yuan2010** and **Yuan2011**, who then suggested setting an appropriate discriminator threshold in connection with removing the bias resistor as a countermeasure. This was disputed in **Lydersen2010b**, who claimed that even with an optimal discriminator threshold and without the bias resistor, the detectors are vulnerable to so-called sinkhole blinding, i.e., heating by strong illumination between the gate windows [**Lydersen2010c**] and after-gate attacks, discussed in Table 4.15. For DPS protocols: - Adding 6 dB of attenuation randomly before the receiver's interferometer and analysing the photon statistics [**Alhussein2019a**]. - Checking for coincidence detections in mismatched bases: When the detectors are blinded, those will be suppressed [**Alhussein2019**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	Some of the publications [**Lydersen2010a**, **Lydersen2010c**, **Lydersen2011a**, **Alhussein2019**, **Alhussein2019a**, **Iwakoshi2015**] are of theoretical nature. Detector control has been shown to work in laboratories and on commercially available devices, namely Clavis2 QKD system [**Lydersen2010a**, **Lydersen2010c**] and ID210 single-photon detector [**Chistiakov2019**] from ID Quantique, and QPN 5505 from MagiQ Technologies [**Lydersen2010a**]. This approach may also work on similar implementations.
Reference(s)	**Lydersen2010a**, **Lydersen2010b**, **Lydersen2010c**, **Yuan2010**, **Lydersen2011a**, **Yuan2011**, **Liu2014**, **Chistiakov2019**, **Wu2020**, **Hegazy2022**, **Iwakoshi2015**, **Alhussein2019**, **Alhussein2019a**

Table 4.13: Detector control of gated APDs via blinding and faked states

Name	Detector control of actively-quenched APD via blinding and faked states		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Actively-quenched APD
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use actively-quenched APDs for single-photon detection. Specifically, BB84 and similar four-state protocols are mentioned in **Sauge2011**. DPS and coherent-one-way (COW) have been discussed in **Lydersen2011a**, round-robin DPS in **Iwakoshi2015**.		
Target(s)	Complete knowledge of the key		
Short Description	Controlling the detection outcomes in the QKD receiver by blinding them with bright pulsed illumination and causing deterministic detection events by faked states.		
Precondition Public information	- Actively-quenched APDs. - APDs can be forced into linear mode by excessive pulsed illumination via blinding or heating.		
Equipment Bespoke equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - Pulsed laser(s) for blinding/heating. - Faked-states generator [**Liu2014**].		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Among all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on actively-quenched APDs which are described in Section 2.4.1.1. Similar to the attacks described in Table 4.12 and Table 4.13, the actively-quenched APDs are forced to operate in the linear mode using bright pulsed illumination [**Sauge2011**]. In the time interval between two bright pulses, the APD is insensitive to single photons, but detection outcomes can nevertheless be obtained in a controlled manner by Eve, using interleaved "faked-state" pulses. Several blinding mechanism variants are discussed based on the repetition rate of the laser pulses. Note these mechanisms might be specific to the APD used in **Sauge2011** (Excelitas SPCM-AQR). For instance, at low repetition rates, an amplifier overload causes the bias voltage to drop, while at high repetition rates the cooling mechanism of the APD cannot cope with the heat produced due to the strong illumination and high current. Depending on the protocol, the exact implementation can vary. For instance, in the (round-robin) DPS case [**Iwakoshi2015**], Eve would have to send a pulse train (at least always two pulses in series) with a carefully		

Description	defined relative phase depending on which of the detectors she wants to trigger.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**). - Monitoring the electrical parameters (**C10**) and photocurrents (**C11**) of the APDs. - Using the technique of bit-mapped gating (**C12**) and monitoring the sensitivity of the single-photon detector (**C13**). - Using newer QKD protocols (**C9**) or novel QKD receiver configurations (**C18**). For DPS protocols: - Adding 6 dB of attenuation randomly before the receiver's interferometer and analysing the photon statistics [**Alhussein2019a**]. - Checking for coincidence detections in mismatched bases: When the detectors are blinded, those will be suppressed [**Alhussein2019**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	The detector control has been shown to work in laboratories and on commercially available detectors (PerkinElmer SPCM-AQR) [**Sauge2011**]). This approach is expected to work on similar implementations.
Reference(s)	**Sauge2011**, **Liu2014**, **Lydersen2011a**, **Iwakoshi2015**, **Alhussein2019**, **Alhussein2019a**

Table 4.14: Detector control of actively-quenched APD via blinding and faked states

Name	Detector control via after-gate pulses		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Gated APD
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Enhanced-Basic	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use gated APDs for detection. For illustration purposes, so far the scientific literature has mainly considered BB84 (with or without decoy states) and SARG04.		
Target(s)	Complete knowledge of the key		
Short Description	Controlling the detection outcomes in the QKD receiver by timing "faked-state" pulses to impinge on the APDs outside (and after) the gating windows.		
Precondition Public information	- APDs operated in gated mode. - Detection events near the outer boundaries of the gating windows are still accepted.		
Equipment Specialised equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - Faked-states generator, such as the one shown in **Liu2014**.		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Among all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on gated APDs, which are described in Section 2.4.1.1. Gated APDs operate in Geiger mode only during the time a gate voltage pulse is activated, increasing the bias across the APD to be above breakdown voltage. Just after these gates (also called gating windows), the APDs are, however, in linear mode [**Wiechers2011**]. If the QKD receiver accepts detection outcomes that occur at such time instants outside the windows, the APDs can be controlled by a faked-state attack in which Eve sends relatively bright faked-state pulses so that they impinge on the APDs just after the gating window. In **Wiechers2011**, it was additionally found that the QKD receiver accepts detection outcomes even during the dead time (see Section 2.4.1.3) of the detectors. A side effect of this attack is that the afterpulsing (see Section 2.4.1.1) may be significantly increased which can expose the attack as it leads to a higher QBER.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent the after-gate attack. These include: - Randomly changing the detection efficiencies of the APDs **(C15)** and statistical analysis of the detection rates **(C14)**. - Using the technique of bit-mapped gating **(C12)** and monitoring the sensitivity of the single-photon detector **(C13)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**.		

Proposed Countermeasures	Also, as mentioned above, the side effect of increased afterpulsing prevents a simple after-gate attack but Eve can exploit the fact that the QKD system accepts detection outcomes even during the dead time of the detectors. The countermeasures include: - Rejection of detection events that occur during an imposed dead time, recording time gaps between consecutive detection events (which should not be below the dead time), and discrimination of detection events inside and outside of gating windows [**Wiechers2011**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	The attack has been shown to work on a commercially available system (ID Quantique Clavis2) [**Wiechers2011**]. This approach is expected to work on similar implementations.
Reference(s)	**Wiechers2011**, **Liu2014**

Table 4.15: Detector control via after-gate pulses

Name	Detector control by exploiting superlinearity		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	Gated APD, SNSPD
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use gated APDs or SNSPDs. BB84 with active basis choice has been investigated.		
Target(s)	Partial knowledge of the key		
Short Description	Achieving partial knowledge of the key by exploiting the superlinear response of the detectors in the QKD receiver.		
Precondition Public information	Usage of gated APDs or SNSPDs.		
Equipment Specialised equipment	- Receiver module, similar to that of the legitimate receiver. - Faked-states generator, such as the one shown in **Liu2014**.		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Among all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on gated APDs and SNSPDs, which are described in Section 2.4.1.1 and 2.4.1.2, respectively. This attack is similar to those discussed in Table 4.13 and Table 4.15. To perform this attack, the detectors need to exhibit a behaviour called superlinearity [**Lydersen2011b**], meaning that the detection efficiency (e.g., at the edges of a gate window) is higher than theoretically expected (compared to a linear detector) if multiple photons impinge on the detector nearly simultaneously. This can lead up to detector control through faked-states attacks (see Section 2.5.2.1). The higher the superlinearity, the better the detector control. However, compared to some of the attacks in Table 4.13, the QBER incurred by Bob is non-zero. In addition to the QBER, this attack also introduces additional loss. However, the main strength of this attack is that Eve needs to use faint light pulses. Attacks exploiting this superlinearity feature on the flanks of the gating window have been proposed and experimentally demonstrated [**Lydersen2011b**, **Qian2018**, **Ye2020a**].		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Monitoring the electrical parameters **(C10)** and photocurrents **(C11)** of the APDs. - Using the technique of bit-mapped gating **(C12)** or monitoring the sensitivity of the single-photon detector **(C13)** with some tweaks [**Lydersen2011b**].		

Proposed Countermeasures	- Using newer QKD protocols (**C9**) or novel QKD receiver configurations (**C18**) or incorporating the imperfection in security proof (**C5**). Other specific countermeasures include: - Mitigation mechanism mentioned in **KoehlerSidki2019**.
Remarks	Other types of detectors might also be affected by this attack.
Feasibility $t_{Attack} < 1$ day	Detector control has been shown to work on SNSPDs, and also gated APDs in ID Quantique's Clavis2 system [**Lydersen2011b**]. A comparatively high QBER (around 13%) was recorded in **Lydersen2011b**, while a similar research system demonstrated low QBER (around 0.5%) [**Qian2018**].
Reference(s)	**Lydersen2011b**, **Liu2014**, **Qian2018**, **KoehlerSidki2019**, **Ye2020a**

Table 4.16: Detector control by exploiting superlinearity

Name	Detector control via blinding using dead time without interception		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	APD
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use free-running (passively- or actively-quenched) APDs in Geiger mode for single-photon detection, specifically, BB84 was demonstrated in **Weier2011**.		
Target(s)	Complete knowledge of the key		
Short Description	Achieving knowledge of the key by exploiting the dead time of APDs without having to detect the photons from the legitimate transmitter.		
Precondition Public information	- At least 2 free-running APDs (or other photodection devices with single-photon sensitivity). - The dead time of these detectors has to be at least on the order of the time window accepting detection events.		
Equipment Specialised equipment	- Light source that produces similar pulses as the legitimate transmitter, but with higher intensity.		
Description	This attack is based on the dead time (see Section 2.4.1.1 or Section 2.4.1.2) of APDs. The main idea is that the attacker can selectively blind all but one detector for a certain time (the dead time), i.e., only one of the detectors remains active. If a detection event occurs in the legitimate detector during that time window, the attacker knows which detector that must have been since all the others were blind. This precludes the need for a faked-states attack (see Section 2.5.2.1). In this respect, the general idea is similar to **Qi2007** and **Zhao2008**, see Table 4.5). While here Eve exploits the polarisation degree of freedom that is used to encode the quantum state in the QKD protocol implementation [**Weier2011**], the general idea is applicable to other protocols and DOFs too. It was shown experimentally that the attacker could gain almost full knowledge about the (sifted) key by employing very dim light pulses (mean value less than 20 photons per pulse), that would be hard to detect with a watchdog detector.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Monitoring the electrical parameters **(C10)** and photocurrents **(C11)** of the APDs. - Using the technique of bit-mapped gating **(C12)** and monitoring the sensitivity of the single-photon detector **(C13)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**.		

Proposed Countermeasures	Other specific countermeasures include: - Modified sifting algorithm: Whenever there are detection events closer in time than the dead time, only the first detection event is considered [**Rogers2007**]. - All detectors shall be held off, while one is inactive [**Xu2006**]. - Self-disabling detector by time-multiplexing the different bit values in each basis on one physical detector [**Rogers2007**].[10] - A specific countermeasure for the dead time prolongation attack is the subject of **Honjo2013**. The authors propose and test experimentally a method that evaluates the ratio of coincidence detection events, since this specific attack produces a lot of those.
Remarks	-
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work in laboratories on a research QKD system built by the same group [**Weier2011**]. It is expected to work on similar implementations.
Reference(s)	**Xu2006**, **Qi2007**, **Rogers2007**, **Zhao2008**, **Weier2011**, **Honjo2013**

Table 4.17: Detector control via blinding using dead time without interception

[10] Time-multiplexed detectors exhibit other vulnerabilities though, see 4.5.

Name	Detector control by blinding of self-differencing APDs		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	APD
Expertise	Expert	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any DV-QKD protocol that uses self-differencing APDs for high-speed single-photon detection.		
Target(s)	Complete knowledge of the key		
Short Description	Achieving complete knowledge of the key by blinding self-differencing (SD) APDs.		
Precondition Public information	The receiver uses one or more SD APDs.		
Equipment Specialised equipment	- Receiver module, similar to that of the legitimate receiver. - Faked-states generator, such as the one shown in **Liu2014**.		
Description	To counter the accompanying side effect of afterpulsing, the SD technique can be employed for APDs. **Jiang2013** describes the working principle as follows: First, the APD is reverse loaded by a combination of a periodic signal and a DC bias voltage. Then, the output of an APD which also amounts for the weak avalanche signal is split into two equal parts. One part is shifted by one gate cycle respective to the other. Afterwards, both parts of the signal are recombined and sent to a differencer. For normal QKD operation, the mean photon numbers reaching the SD APDs are very low, which therefore entails a negligible probability of two photons in two adjacent pulses. Since the arising avalanche signal appears in the form of a positive peak followed by a negative peak separated by one gate cycle, weak avalanche signals caused by afterpulsing can be discriminated from the actual photon count while maintaining the advantageous high gating frequency. However, if the incident photon flux increases, multiphoton signals are capable of triggering avalanches in every other gate. As a consequence, discrimination of weaker avalanche signals can no longer be achieved, resulting in APD blinding. As **Jiang2013** proposes and experimentally demonstrates, intercept-and-resend attacks (as described in Section 2.5.2) can be made possible due to blinding of SD APDs. Further, increasing the incident photon flux after blinding, a recovery of the detector's count rate can be measured [**Jiang2013**, **KoehlerSidki2018**, **KoehlerSidki2018a**]. By examining this observation (theoretically and experimentally), **KoehlerSidki2018** found that the discrimination level, which is the voltage level chosen that rejects the residual capacitive background from avalanches triggered by actual photons, has an influence on the width of the observed blinding gap.		

Description	**KoehlerSidki2018** explains this behaviour in the following way: Increasing the photon flux, the detector is more likely to produce an avalanche with a saturated amplitude, leading to a decrease of the SD APD's output. Contrary to that, the residual capacitive background also increases with increasing incident photon flux, providing means to counter the decrease of photon-induced signals. While **Jiang2013** and **KoehlerSidki2018** used CW lasers for blinding SD APDs, **Gao2022** investigated their behaviour employing pulsed laser illumination: Using a strong pulsed laser with the same frequency as the gated signal, blinding of the SD APDs could be achieved. However, the observed drop of bias voltage is not as significant as compared to the attack performed with CW illumination.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Monitoring the photocurrents **(C11)** of the APDs. - Using the technique of bit-mapped gating **(C12)** or monitoring the sensitivity of the single-photon detector **(C13)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**. - Incorporating the imperfection in security proof **(C5)**. Other specific countermeasures include: - Setting an appropriate discrimination level. - Usage of different resistance values in a QKD system comprised of two or more detectors. - Prior verification if the residual capacitive response is able to surpass the detector discrimination voltage when the APD's reverse bias is lowered below its breakdown. - Prior modelling of the detectors behaviour.
Remarks	-
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work in laboratories and on commercially available systems [**Lee2016**]. It is expected to work on similar implementations.
Reference(s)	**Jiang2013**, **Liu2014**, **Lee2016**, **KoehlerSidki2018**, **KoehlerSidki2018a**, **Gao2022**

Table 4.18: Detector control by blinding of self-differencing APDs

Name	Detector control of SNSPD-based receivers		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	SNSPD
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use SNSPDs, specifically BB84 and DPS are mentioned in **Lydersen2011**, round-robin DPS in **Iwakoshi2015**.		
Target(s)	Complete knowledge of the key		
Short Description	Controlling the detection outcomes in a QKD receiver based on SNSPDs through mechanisms such as permanent latching and deadtime prolongation.		
Precondition Public information	SNSPDs that can be put in a latched state and/or have the deadtime extended by tailored illumination.		
Equipment Specialised equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - Faked-states generator, such as the one shown in **Liu2014**.		
Description	The principle of detector-control attacks using faked states is described in Section 2.5.2.1. Amongst all known attacks on DV-QKD systems, detector-control attacks comprise the largest set and have been investigated on a wide variety of single-photon detectors. In this table, the focus is on gated SNSPDs, which are described in Section 2.4.1.2. Control of SNSPDs using faked states has been demonstrated in **Lydersen2011** in two different ways: The first method is to bring the SNSPD into the so-called latched state (see Section 2.4.1.2) by applying intense illumination. When it is latched, it will stay in this state and become insensitive to single photons. An additional bright light pulse will trigger the comparator behind the SNSPD and thus can be used for a faked-states attack. The second method an eavesdropper can use is extending the dead time of the SNSPDs by illuminating the detectors with a comparatively long bright pulse. Afterwards, a sequence of short pulses is emitted, extending the dead time of all but one of the detectors. The active detector is then triggered by yet another specific light pulse (i.e., a detection event is enforced) and the whole procedure starts again. This method has been successfully tested experimentally on several SNSPD types in **Fujiwara2013** and **Tanner2014**. Depending on the protocol, the exact implementation can vary. For instance, in the (round-robin) DPS case [**Iwakoshi2015**], Eve would have to send a pulse train (at least always two pulses in series) with a carefully defined relative phase, depending on which of the detectors she wants to trigger.		

Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors **(C2)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**. Other specific countermeasures include: - Permanent latching could be avoided by an automated reset or by including a resistor in parallel with the nanowire [**Lydersen2011**, **Elezov2015**]. This has been experimentally tested in **Tanner2014** who also suggested the possibility of an active reset mechanism. - An active latching-reset circuit has been studied in **Elezov2019**, but this could only reduce the controllability of the SNSPD under test to some extent. - Monitoring the parameters of the SNSPDs (e.g., DC bias voltage or output pulse) is suggested in **Tanner2014**. However, the authors note that the effects of an attack could be hard to discern. - A specific countermeasure for the dead time extension is subject of **Honjo2013**. The authors propose and test experimentally a method that evaluates the ratio of coincidence detection events, since this specific attack produces a lot of those. For DPS protocols: - Adding 6 dB of attenuation randomly before the receiver's interferometer and analysing the photon statistics [**Alhussein2019a**]. - Checking for coincidence detections in mismatched bases: When the detectors are blinded, those will be suppressed [**Alhussein2019**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	Detector control has been shown to work on a commercially available SNSPD from Scontel [**Lydersen2011**] and different type of research-lab detectors [**Tanner2014**]. This approach is expected to work on similar implementations.
Reference(s)	**Lydersen2011**, **Fujiwara2013**, **Honjo2013**, **Liu2014**, **Tanner2014**, **Elezov2015**, **Iwakoshi2015**, **Elezov2019**, **Alhussein2019**, **Alhussein2019a**

Table 4.19: Detector control of SNSPD-based receivers

Name	Detector control of TES-based receivers		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	TES
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use transition-edge sensors (TESs) for single-photon detection, with or without using photon number resolution. Specifically, BB84 and COW are named.		
Target(s)	Partial knowledge of the key		
Short Description	Controlling the detection outcomes in the TES receiver through tailored illumination (CW and pulsed light).		
Precondition Public information	QKD receiver based on TES.		
Equipment Bespoke equipment	- A receiver device similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter). - CW lasers to blind the TESs and pulsed lasers for preparing faked states (Faked-states generator) [**Liu2014**].		
Description	Detector control of a TES as a threshold detector (not in photon number resolving mode) is shown in two steps: First, the device is rendered insensitive to single photons by illumination with CW light due to heating of the sensor. Then, a bright laser pulse can produce a reaction that mimics that of a single-photon detection under normal conditions. If the TES was used in photon number resolving mode, for example as part of a counter measure for other similar attacks, the eavesdropper could use the fact that the energy of the photon(s) determine the reaction of the TES: One photon with a certain wavelength will produce the same effect as multiple photons of lower wavelength, if the total energies are the same.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors **(C2)**. - Using optical filters **(C4)**. - Using newer QKD protocols **(C9)** or novel QKD receiver configurations **(C18)**. Specific countermeasures: Possibly looking at the pulse shape of the output pulse [**Chaiwongkhot2022**].		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	Detector control has been demonstrated on a TES [**Chaiwongkhot2022**].		
Reference(s)	**Liu2014**, **Chaiwongkhot2022**		

Table 4.20: Detector control of TES-based receivers

Name	Wavelength-dependent beamsplitter attack		
Category	Wavelength-dependent manipulation attack		
Component	Receiver	**Subcomponent**	Beamsplitter
Expertise	Expert	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that satisfy the preconditions. Specifically, BB84 was demonstrated in **Li2011**.		
Target(s)	Partial knowledge of the key		
Short Description	Controlling measurement results of Bob by exploiting the wavelength dependence of the beamsplitter used in the QKD receiver.		
Precondition Public information	Bob implements a passive basis choice using a beamsplitter that exhibits wavelength-dependent transmittance and reflectance.		
Equipment Specialised equipment	Intercept-and-resend equipment for multiple wavelengths: - Detection module to measure the quantum signals from Alice. - Multi-wavelength sources and modulators to prepare and send optical signals to Bob.		
Description	The behaviour of optical components may strongly depend on properties such as the wavelength of the input light. For instance, the coupling ratio of an optical beamsplitter (see Section 2.4.4.1) changes from 50:50 at 1550 nm to nearly 99:1 at 1470 nm [**Li2011**]. If such a beamsplitter is used for implementing the passive basis choice at the receiver, Eve can exploit the wavelength dependence via an intercept-and-resend attack (see Section 2.5.2). The states that Eve re-sends to Bob are prepared at one of two different wavelengths, so that states at the first wavelength are mainly reflected while those at the second wavelength are primarily transmitted through the beamsplitter at Bob. In this manner, Eve can control Bob's measurement outcomes to get information about the key. In **Fei2018b**, the wavelength dependence of the passive basis-choice beamsplitter is exploited to induce a basis-dependent detector efficiency mismatch (BEM) during the calibration procedure. During the line length measurement, Eve blocks all pulses from Alice and sends fake calibration signals containing two equal-intensity random-polarisation pulses with different wavelengths in one cycle to induce large BEM. In **Li2022**, the authors study the physical properties of beamsplitters in the context of these attacks and provide a security analysis.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using spectral monitoring of the input optical signals (**C2**) and wavelength filters (**C4**).		

Proposed Countermeasures	Other specific measures include: - Using actively modulated phase encoding QKD systems [**Li2011**]. - Characterise beamsplitters for a wide range of wavelengths, and use only those that exhibit a low dependence [**Li2022**]. - Detect the QBER and abort the protocol in case it exceeds the pre-set threshold, determined by the wavelength-dependent behaviour of the beamsplitter [**Li2022**]. - Using newer QKD protocols (**C9**).
Remarks	Table 4.39 covers attacks due to this imperfection on CV-QKD systems.
Feasibility $t_{Attack} < 1$ day	The attack in **Li2011** has been shown to work in laboratories experimentally. The attack proposed in **Fei2018b** is of theoretical nature and has not yet been demonstrated on a working device.
Reference(s)	**Li2011**, **Fei2018b**, **Li2022**

Table 4.21: Wavelength-dependent beamsplitter attack

Name	Passive Faraday mirror attack		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Faraday mirror
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Passive
Protocol	Applicable to BB84.		
Target(s)	Partial knowledge of the key		
Short Description	Achieving partial knowledge of the key by measuring BB84 states using exploitation of the polarisation DOF affected by imperfections of a Faraday mirror (FM) in a phase-encoded QKD system.		
Precondition Public information	Use of Faraday mirror with imperfections in Alice's setup in a one-way or two-way QKD setup.		
Equipment Specialised equipment	- A state analysis module capable of performing suitable positive operator-valued measure (POVM) operators to distinguish BB84 states. - A photon source and state preparation module for an intercept-and-resend attack.		
Description	A passive FM attack, first proposed by **Sun2011**, exploits imperfections of FMs in a QKD system leading to information leakage to an eavesdropper. In **Sun2011**, a two-way QKD system using a FM to compensate for birefringence in fibre is analysed. An imperfect FM gives access to the polarisation DOF of the phase-encoded signal states, as there is no perfect polarisation rotation. Exploiting these imperfections using suitable POVM operators to distinguish the BB84 states encoded by Alice, combined with an intercept-and-resend attack, Eve is able to gain information about the key while introducing far less attack-induced QBER than in the general intercept-and-resend attack. The attack can also be combined with a phase-remapping attack (see Table 4.8) to reduce the induced QBER even more. This attack strategy has been modified in **Wang2013** for a two-way QKD system, where four FMs are used. There, only the imperfect FM on the path where the encoded signal pulse is transmitted results in more information about the secure key. Additionally, a passive FM attack in a one-way Faraday-Michelson system is shown and analysed.		
Proposed Countermeasures	- Perfect alignment of FM to reduce induced errors [**Sun2011**]. - Quantifying FM imperfections and taking them into account in the security analysis [**Wang2013**].		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.		
Reference(s)	**Sun2011**, **Wang2013**		

Table 4.22: Passive Faraday mirror attack

Name	Timing mismatch of pump current modulation generated signal and decoy states		
Category	Timing attack		
Component	Transmitter	**Subcomponent**	Laser
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Passive
Protocol	Applicable to BB84 with decoy states.		
Target(s)	Partial knowledge of the key		
Short Description	Exploiting timing mismatch between signal and decoy states due to the generation through modulation of pump current of a gain-switched laser diode mounting a PNS attack.		
Precondition Public information	Alice has to use pump-current modulation of a gain-switched laser diode to generate different intensities for the decoy-state protocol.		
Equipment Specialised equipment	- Apparatus to perform PNS attack (see Table 4.2). - Clock to choose photons according to time windows.		
Description	In **Huang2018**, a side channel concerning the generation of decoy states with different intensities by laser diode gain-switching using modulation of its pump current is presented. Due to different pump currents used for the generation of the different intensities, with high probability, the signal state is emitted earlier than the decoy state. The main peaks of the emission probability distributions are mismatched. This leads to a distinguishability between the generated states and compromises the decoy-state protocol, thus, making it possible to perform a modified PNS attack proposed in **Huang2018**. Eve chooses time windows for the signal and the decoy states. All states observed in the signal time window are treated as signal states, likewise for decoy window and decoy states. She blocks or forwards the single-photon states in the observation windows and blocks all states outside of it. For multi-photon states in the observation window, Eve keeps one photon and either blocks or forwards the rest of the photons to Bob. She forwards all photons when the states are outside the window. When she obtains photons in both time windows, she randomly keeps photons in only one window and forwards the rest, introducing an error half the time. Eve can get partial knowledge of the final key by optimising the time windows, while not introducing any error if signal and decoy states are distinguished correctly.		
Proposed Countermeasures	Countermeasures tackling the side channel are: - Adjusting the timing and shape of pump current to reduce mismatch, although this is unlikely to fully eliminate the vulnerability. - Incorporating imperfections in security proof [**Huang2018**].		

Proposed Countermeasures	- Using an external intensity modulator to generate signal- and decoy-state intensities. In the analysis done by **Huang2018**, this showed no measurable timing mismatch. Note, however, that intensity modulators are vulnerable to Trojan-horse attacks (see Table 4.48).
Remarks	-
Feasibility $t_{Attack} < 1$ day	The timing mismatch of signal and decoy states has been experimentally verified. The proposed PNS attack has been simulated numerically but has not been demonstrated experimentally.
Reference(s)	**Huang2018**

Table 4.23: Timing mismatch of pump current modulation generated signal and decoy states

Name	Wavelength-selected photon-number splitting attack		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Intensity modulator
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to BB84 with decoy states.		
Target(s)	Partial knowledge of the key		
Short Description	Achieving some knowledge of the key by using frequency shifts introduced by intensity modulators (IMs).		
Precondition Public information	- Use of a two-way system. - Use of an IM for the generation of states with different intensities. - Alice must not monitor the arrival times of signal and reference pulses.		
Equipment Specialised equipment	- System to introduce time shifts between signal and reference pulse. - Wavelength-division multiplexer (WDM). - PNS attack module.		
Description	In decoy-state protocols, intensity modulators are used to imprint different intensities on light pulses resulting in vacuum, signal, and decoy pulses. The IMs work by applying voltage onto an electro-optical material inducing a phase shift in the transmitted pulse. Basically, the voltage is assumed to be constant when the light pulse comes, and the IM responds to have a pure intensity modulation. In plug-and-play systems, Eve time shifts the pulses such that the electro-optical effect happens at the rising edge of intensity modulation voltage to introduce a frequency shift, as shown in **Jiang2012**. As the intensity modulation is only applied to the decoy and vacuum state, its frequency will change while the frequency of the signal state will retain. Using a wavelength-division multiplexer (WDM), Eve can now distinguish between signal and decoy state. Subsequently, Eve performs a PNS attack on signal and decoy states.		
Proposed Countermeasures	In **Jiang2012** several countermeasures are described: - Monitoring the arrival times of the signal and reference pulses at Alice - Monitoring the intensity of the decoy pulses at Alice (Eve's time shift introduces a change) - Using a one-way QKD protocol, as Eve cannot time-shift the light pulse there.		
Remarks	See Table 4.10 for a related attack.		
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.		
Reference(s)	**Jiang2012**		

Table 4.24: Wavelength-selected photon-number splitting attack

Name	Attack on spatial information leakage from misaligned sources		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Laser diode
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Mixed
Protocol	Should be applicable to QKD protocols that use multiple lasers for encoding. The scientific literature has considered only BB84 protocol so far.		
Target(s)	Partial knowledge of the key		
Short Description	Exploiting spatial distinguishability between signal states due to misaligned laser diodes to get knowledge of the key.		
Precondition Public information	The proposed attack can be performed on all free-space QKD system using multiple laser diodes for state generation.		
Equipment Specialised equipment	- Optical system for focusing different beams onto single-photon detector array. - Single-photon detector array. - Transmitter module to resend states to Bob.		
Description	Spatial distinguishability between signal states can severely compromise the security of free-space QKD systems. The use of four laser diodes for state generation can lead to this spatial information leakage if there is angular misalignment between them. In **Huang2019a**, this information leakage is analysed and an attack is proposed considering point sources, spherical waves, and a transmitter that truncates the beams. The idea of the attack is to focus beams with different angles of arrival onto different areas of a single-photon detector array to get encoding information and resend the states according to the outcome to Bob. **ArteagaDiaz2022** further improved these ideas by considering Gaussian beams and no introduction of truncation effects at the exit aperture, as these are more realistic assumptions. If the beams of the different lasers do not overlap at Eve's detector array, the states can be fully distinguished and Eve can get knowledge of the full key. Furthermore, an attacker could increase the transmission distance to increase the spatial distinguishability between the states. Current space telescopes' sizes make QKD systems that rely on sources with an angular misalignment of more than 1 μrad completely insecure.		
Proposed Countermeasures	Several countermeasures have been proposed in the scientific literature: - Using aperture in the QKD sender to reduce spatial information. Parameters to be optimised are the diameter of the aperture and the distance between the aperture and the source plane. The effect should be quantified and remaining leakage information taken into account in the privacy amplification [**Huang2019a**]. - Coupling all states into the same single-mode optical fibre before sending them into the free-space channel.		

Proposed Countermeasures	In this way, by confining them in the fibre, a single spatial mode of propagation is achieved that makes them almost spatially indistinguishable, obtaining low information leakage [**ArteagaDiaz2022**, **Nauerth2009**]. - Using a single laser diode to eliminate all information leakage of the lasers (spatial, spectral, temporal) [**ArteagaDiaz2022**]. - Incorporate the effect of device imperfections in the security proof (**C5**).
Remarks	-
Feasibility $t_{Attack} < 1$ day	The proposed attack has been shown in a proof-of-principle experiment using a simplified setup in **ArteagaDiaz2022**.
Reference(s)	**Nauerth2009**, **Huang2019a**, **ArteagaDiaz2022**

Table 4.25: Attack on spatial information leakage from misaligned sources

Name	Free-space QKD system hacking by wavelength control using an external laser		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Laser diode
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use multiple lasers for encoding. For illustration purposes, so far the scientific literature has mainly considered the BB84 protocol.		
Target(s)	Partial knowledge of the key		
Short Description	Using an external laser to change and thus distinguish the wavelength of signal states and get knowledge of the key.		
Precondition Public information	- Using different laser diodes for preparing different polarisation signal states. - Using polarising elements for state preparation.		
Equipment Specialised equipment	- Laser diode as external laser source. - WDM to split the signals of different wavelengths. - Polarisation optics such as PBS, HWP (see Section 2.4.4.3). - Single-photon detectors. - Laser diodes of the same model as Alice's.		
Description	In **Lee2017**, an attack strategy targeting the wavelength of the laser diodes in the state preparation at Alice is proposed. In contrast to side channels arising from differences between the laser diodes (see Table 4.61) in case of this attack, the laser diodes can have the same characteristics. An external laser is used by Eve to increase the internal temperature of Alice's laser diodes. By sending a strong laser with a certain polarisation coinciding with one of the four signal states through Alice's state preparation setup, Alice's laser diodes are exposed to different laser powers. This leads to different increases in temperatures of the laser diodes and therefore different changes in the wavelengths. Now, by using a WDM, Eve can directly distinguish horizontal, vertical, and diagonal photons by their wavelength, and using a HWP and a PBS she can distinguish both diagonal photon orientations. By sending the measured state to Bob, she can stay completely undetected and get full knowledge of the key. In a proof-of-principle experiment, they confirmed that the wavelength of the laser diodes can be changed by 5 to 8 nm with external laser radiation of up to 600 mW if a thermoelectric cooler is used to change the laser diodes' temperature and make the wavelength equal. Without temperature control at the laser diodes, wavelength changes up to 40 pm with a power of 25 mW have been shown.		

Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using optical isolation **(C1)**, watchdog detectors **(C2)**, and appropriate wavelength filtering **(C4)**. Other specific countermeasures include: - Random variations in the laser diode wavelength under Alice's control [**Lee2017**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work in laboratories in **Lee2017**. It is expected to work on similar implementations.
Reference(s)	**Lee2017**

Table 4.26: Free-space QKD system hacking by wavelength control using an external laser

Name	Exploiting passive side channels from imperfections in the transmitter		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Light source
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Mixed
Protocol	The scientific literature has considered only BB84 protocol so far (with and without decoy states). The attack could possibly be applicable to further protocols using imperfect light sources.		
Target(s)	Partial knowledge of the key		
Short Description	Attacking passive light-source side channels to gain information about the key.		
Precondition Public information	The TOE has to have information leakage from side channels in the transmitter.		
Equipment Specialised equipment	- Intercept-and-resend module [**Babukhin2020**][11]. - Quantum memory (optional).		
Description	Imperfect light sources (see Table 4.25 and Table 4.61, for example) can lead to information leakage about the operational degree of freedom to other degrees of freedom that can be exploited by an eavesdropper increasing its success rate when attacking the QKD system. In **Babukhin2020**, an explicit intercept-and-resend attack (see Section 2.5.2) exploiting the distinguishability of signal states due to passive side channels of the light source is proposed. An eavesdropper tries to find POVMs for optimal state discrimination before performing the intercept-and-resend attack. The higher the distinguishability, the lower the induced error and the better the states can be discriminated by the eavesdropper. A more promising method is the use of phase-covariant cloning attacks. The principle of this attack relies on Eve performing quantum cloning on the signal state, correlating it with her ancillary state, which is stored in a quantum memory. After basis exchange, she measures the states in the quantum memory collectively to get the most information about the key out of her ancillary states. In **Babukhin2021**, a USD measurement on the side-channel DOF is performed. If the measurement is successful, Eve obtains the secret bit. If not, she performs a phase-covariant cloning attack (PCCA) of the signal state. Eve then has two possible states in her quantum memory which she optimally discriminates with a minimum error measurement. **Babukhin2022a** further analysed the different possibilities of using PCCA combined with minimal-error and USD measurements.		

[11] As the attacks described here are all of a purely theoretical nature, there is no further equipment for the proposed attacks mentioned

Description	Three different attack strategies have been shown: 1.) minimal-error measurement of the side-channel state and phase-covariant cloning of the signal-photon state; 2.) minimal-error measurement of the side-channel state, soft filtering, and two-state cloning; 3.) USD measurement of the side-channel state and phase-covariant cloning. An even more sophisticated attack using a joint collective measurement of the side channel and the operational DOF after a phase-covariant cloning attack of the signal-photon state is proposed by **Babukhin2022**. The joint collective measurement of operational and non-operational DOFs is a stronger eavesdropping strategy than the one of **Babukhin2022a**. The effects of attacks using joint collective measurements in combination with a Trojan-horse attack (THA) are analysed in **Molotkov2020**, **Molotkov2020a**, and **Molotkov2020d**.
Proposed Countermeasures	Several countermeasures are proposed in the scientific literature: - Calculating lower bounds on the secure key rate by using Hong-Ou-Mandel (HOM) interference visibility between different emitted signals to quantify the amount of distinguishability between signal states and integrate them into security proofs. Can be used for single-photon states and phase-randomised weak-coherent states. The HOM interference allows for the study of the general distinguishability of pulses, as opposed to measuring individual DOFs. This is because non-interfering states are considered distinguishable [**Duplinskiy2019**, **Sych2021**, **Babukhin2020**, **Babukhin2022**, **Babukhin2022a**]. Limitations on the measurement of the interference contrast may overestimate the information leakage [**Sych2021**]. - Calculating upper bounds on the secure key rate by taking into account the effects of attacks including passive light-source side channels [**Babukhin2020**, **Babukhin2021**, **Babukhin2022**, **Babukhin2022a**, **Molotkov2020**][12]. - An automatised testing module can be integrated into Alice's device to monitor laser diodes' side channels [**Duplinskiy2019**]. - Using protocols with more quantum states in the communication alphabet to make state discrimination more difficult [**Sych2021**, **Babukhin2021**]. - Take into account information leakage from side channels into secret key rate in terms of parameters, that can be observed on the receiving side [**Molotkov2020d**]. - Use of a generalised decoy-state method, which takes into account joint collective measurements of information quantum states and quantum states in side channels [**Molotkov2020**, **Molotkov2020a**]. - Incorporate the effect of device imperfections in the security proof (**C5**).
Remarks	The attack rating takes into account the equipment used in **Babukhin2020** which does not need a quantum memory.

[12] Note that the best attack strategy against passive-source side channels has not yet been found.

Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Duplinskiy2019**, **Babukhin2020**, **Molotkov2020**, **Molotkov2020a**, **Molotkov2020d**, **Sych2021**, **Babukhin2021**, **Babukhin2022**, **Babukhin2022a**

Table 4.27: Exploiting passive side channels from imperfections in the transmitter

Name	Exploiting frequency side channels in sending or not-sending twin-field QKD with passive frequency-shift attack		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	Intensity modulator
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Passive
Protocol	Applicable to TF-QKD.		
Target(s)	Partial knowledge of the key		
Short Description	Exploiting a frequency side channel due to imperfect intensity modulation to get knowledge of the key in TF-QKD.		
Precondition Public information	Sending or not-sending (SNS) TF-QKD, where only one IM is used to modulate signal and reference pulses.		
Equipment Specialised equipment	- WDM. - Single-photon detectors (SPDs). - Light-path selectors.		
Description	The use of IMs in decoy state protocols can create a passive side channel in the frequency domain, causing distinguishability between signal and decoy states. **Lu2021** experimentally demonstrated this effect using a Mach-Zehnder electro-optical IM that induces frequency shifts in light pulses. The spectra of the states will be changed differently by the IM depending on the intensity. They proposed a passive frequency-shift attack on an imperfect SNS TF-QKD protocol with actively odd-parity pairing (AOPP). The attack involves only one IM to modulate signal pulses. Eve intercepts portions of the signal pulses at Alice and Bob's outputs and distinguishes signal and decoy states using a WDM and three SPDs. Eve configures the WDM to cut out small wavelength intervals of the spectrum where the differences between the different intensity pulses are greatest (see Figure 1 and 3 in **Lu2021**). Light-path selectors ensure that only one SPD will click at most during the measurement process. As only small intervals of the total wavelength spectrum are cut out by the WDM, Eve's actions can be viewed as loss without phase noise. Using this distinguishability between the pulses, it is more likely that one detector clicks than another. Through this process, Eve can obtain partial raw-key bits after the legitimate parties announce the signal and decoy windows. Although Eve cannot distinguish the decoy and signal states without errors, the decoy-state method may inaccurately estimate the lower bound of the secret key rate when the transmittances of the signal and decoy states differ, compromising the secrecy of the final key. Simulation results quantitatively demonstrate the effectiveness of the attack on imperfect devices over long distances.		

Proposed Countermeasures	Several countermeasures against the presented attack have been proposed in **Lu2021**: - Using three IMs to modulate the signal pulses and reference pulses, where the last IM is used to eliminate the side channels. This can mitigate the attack at present in actual QKD systems. - Include side channels in theory with models like the loss-tolerant method with characterization of real apparatuses.
Remarks	-
Feasibility $t_{Attack} < 1$ day	A proof-of-principle experiment showing the side channel has been done. The proposed attack is theoretical and has only been simulated numerically.
Reference(s)	**Lu2021**

Table 4.28: Exploiting frequency side channels in sending or not-sending twin-field QKD with passive frequency-shift attack

Name	Trojan-horse attack against the SARG04 protocol		
Category	Trojan-horse attack		
Component	Receiver	**Subcomponent**	Phase modulator
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to SARG04.		
Target(s)	Partial knowledge of the key		
Short Description	Achieving partial knowledge of the key by injecting Trojan-horse pulses into the receiver and obtaining information about the basis choice.		
Precondition Public information	- Use of a two-way setup. - Low noise response (e.g., afterpulsing) from the detectors at the wavelength of the Trojan-horse pulses. - Use of a phase modulator for basis choice.		
Equipment Bespoke equipment	- Pulsed laser tuneable in time, power, and polarisation. - Phase decoding module, e.g., homodyne detector.		
Description	Trojan-horse attacks, introduced in more detail in Table 4.48, normally target QKD transmitters. In DV-QKD protocols such as BB84 (see Section 2.3.1.1), a successful attack yields Eve both the bit and the basis choice of Alice. Since the basis choice of Bob is publicly disclosed in the sifting/reconciliation stage, a Trojan-horse attack on Bob cannot yield Eve any helpful information. However, in a variant of BB84 called SARG04 [**Scarani2004**], the final secret bit is given by Bob's basis choice. Therefore, an attack could be used for compromising the security of the QKD system. SARG04 is more immune to PNS attacks than BB84 and does not require any hardware change in the QKD implementation. In **Jain2014**, the authors proposed and experimentally demonstrated a Trojan-horse attack against the SARG04 protocol being operated on a two-way QKD system from ID Quantique (Clavis2). The aim was to discern Bob's phase modulator setting, as that information yields Eve the basis choice and eventual access to the raw key bits. This was accomplished by sending a carefully designed bright pulse into Bob during the active phase modulation period and analysing the back-reflections via homodyne measurements. An unavoidable consequence of this attack was a significant increase in noise (due to afterpulsing; see Section 2.4.1.3) in the QKD receiver due to the bright Trojan-horse pulses impinging on the single-photon detectors. As this would lead to a high QBER, it is critical for Eve to lower the noise significantly. It was suggested that this could be possible by selecting an appropriate injection time, intensity, and wavelength of the Trojan-horse pulse.		

Description	An experimental investigation in **Sajeed2017** (on the same type of QKD system as in **Jain2014**) reported that changing the Trojan-horse pulse wavelength from 1550 nm to 1924 nm did greatly reduce the amount of afterpulsing.
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this class of attacks. These include: - Using wavelength filters (**C4**). - Using a watchdog detector (**C2**) with a tweak, namely, a low-loss optical switch to randomly route and check a small fraction of the incoming signals [**Jain2014**]. - Using novel QKD receiver configurations (**C18**). - Monitoring the parameters of the detector (**C10**) and analysing detection rates statistically (**C14**). Specific countermeasures include: - Reducing the width of phase modulation voltage pulse to limit the time of access to Eve (though this would make the attack just more difficult but not impossible) [**Jain2014**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	The proposed attack has been tried on the commercially available system Clavis2 from ID Quantique unsuccessfully in **Jain2014**. In **Sajeed2017**, they provide experimental evidence that the proposed attack could succeed under certain conditions.
Reference(s)	**Scarani2004**, **Jain2014**, **Sajeed2017**

Table 4.29: Trojan-horse attack against the SARG04 protocol

Name	Trojan-horse attack on counterfactual QKD		
Category	Trojan-horse attack		
Component	Receiver	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to Counterfactual quantum key distribution (CfQKD) [**Liu2014a**].		
Target(s)	Partial knowledge of the key		
Short Description	Achieving partial knowledge of the key by insertion of fake signal pulses in CfQKD.		
Precondition Public information	No preconditions needed.		
Equipment Standard equipment	- Counterfactual communication module similar to that of Alice. - Router module consisting of a BS, a phase modulator (PM), and a FM.		
Description	In CfQKD a Michelson-type interferometer split between Alice and Bob is used for secret key generation. Alice generates signals in the form of either horizontally (H) or vertically (V) polarised photons. These are split at a BS (see Section 2.4.4.1), with one mode sent to Bob and the other sent on an optical delay line and reflected back by a FM. At Bob, the H component of the incoming signal passes through a PBS, while the V component gets reflected, and sent through an optical loop back to the PBS, to then take the same path as the H signal. This introduces a time delay between H and V pulses. Bob uses an optical switch at different times to send the pulse to a detector and either measure H or V. If the two parties choose different bit values (encoding is done in polarisation, e.g. H=0 and V=1), the pulse will be reflected by a FM and be sent back to Alice. At Alice the pulses will be recombined and, according to their phase difference, they will interfere and different detectors will click. If Alice and Bob choose the same bit value, Bob's detector will block the pulse. The two parties will only use events for their secret key rate where the photon never leaves Alice's setup, which only occurs if the photon is reflected and then transmitted at Alice's BS. Eve's attack strategy involves the use of a counterfactual communication module similar to that of Alice, i.e., which emits and detects single-photon pulses, as well as a router module, which routes the signals [**Liu2014a**]. Eve's communication module and router module are coupled into the quantum channel between Alice and Bob with a BS. In each transmission round, when Alice sends a pulse to Bob, Eve also generates a single-photon pulse with a randomly chosen polarisation and sends it to Bob over the introduced BS together with the signal sent by Alice.		

Description	Eve then records which detector in her detection module clicks upon receiving back her injected photon, depending on the different bit choices of Alice, Bob, and Eve. Which detector clicks depends on how the different pulses interfere with each other at the several BSs. After Alice and Bob have published their detection results, Eve uses her recorded data to determine the secret bits by identifying the events where there is a simultaneous detection click in her detection module and in that of Bob.
Proposed Countermeasures	Adding a switchable polarisation rotator into Bob's station which transforms the polarisation state of the input light into its orthogonal polarisation state. In each transmission round, Bob randomly chooses to switch it on or off.
Remarks	-
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Liu2014a**

Table 4.30: Trojan-horse attack on counterfactual QKD

Name	Laser-damage attack on detectors in QKD systems		
Category	Laser-damage attack		
Component	Transmitter, receiver	**Subcomponent**	Photodiode
Expertise	Expert	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any protocol that is susceptible to different types of faked-states attacks against a QKD receiver (see, e.g., Tables 4.5 and 4.12) or Trojan-horse attacks (Table 4.48) against a QKD transmitter.		
Target(s)	Enabling other attacks		
Short Description	Characteristics of a photodetector are altered or damaged in a way that the system becomes vulnerable to attacks.		
Precondition Public information	Usage of a photodiode for monitoring the incoming pulse energy (typically in a QKD transmitter) or an APD for single-photon detection (QKD receiver).		
Equipment Bespoke equipment	High-power laser.		
Description	In **Bugge2014**, the investigated detector is a free-space passively-quenched APD (see subsection 2.4.1.1). High-power laser light focussed onto the APD alters the characteristics in significantly different ways, depending on the amount of power. For instance, in a certain power range, the detectors become permanently prone to the detection efficiency mismatch vulnerability (see Table 4.5) in the polarisation degree of freedom. At a higher power range, they are permanently blinded (see for instance Table 4.12). In particular, 10 different samples of the same APD were investigated in 6 different power regimes. In **Makarov2016**, it is shown that in case an adversary uses high-power laser light to inflict damage to the photodiode, which maybe used in a watchdog detector, the reduced sensitivity enables an attacker to perform Trojan-horse attacks (see Table 4.48). The same type of attack on free-space APDs opens up the detection efficiency mismatch vulnerability (see Table 4.5) in the spatial degree of freedom.		
Proposed Countermeasures	The countermeasures against this attack rely on the assumption that the input light injected by Eve is upper bounded by physical means (e.g., laser damage threshold). Under that assumption, some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using optical isolation (**C1**) and watchdog detectors (**C2**). - Monitoring the health of implemented countermeasures (**C3**). - Using newer QKD protocols (**C9**).		

Remarks	The targeted components can be either in the receiver [**Bugge2014**] or the transmitter [**Makarov2016**].
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work on commercial APDs (PerkinElmer C30902SH) in **Bugge2014** and on commercially available systems (Clavis2 from ID Quantique in **Makarov2016**). It is expected to work on similar implementations (both fiber-optic and free-space systems).
Reference(s)	**Bugge2014**, **Makarov2016**

Table 4.31: Laser-damage attack on detectors in QKD systems

Name	Laser-damage attack against optical attenuators in QKD systems		
Category	Laser-damage attack		
Component	Transmitter	**Subcomponent**	Attenuator
Expertise	Expert	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use an attenuated laser to prepare weak-coherent states. BB84 (with and without decoy states) and MDI-QKD protocols are mentioned in **Huang2020**.		
Target(s)	Complete knowledge of the key		
Short Description	Injecting high-power laser light into optical attenuators to decrease their attenuation capabilities, such that the attacker can split off a part of the signal unnoticed.		
Precondition Public information	Employ a laser as a source and an optical attenuator to tweak the photon number statistics down to the single-photon level.		
Equipment Bespoke equipment	High-power laser.		
Description	Weak-coherent states (see Section 2.4.3.1) are the most frequently employed quantum states in DV-QKD systems. The most common method to produce such states is by using an optical attenuator (see Section 2.4.4.2) after a laser. However, by injecting a high-power laser from the channel into the transmitter, the eavesdropper can induce damage on the attenuator in a way that decreases the actual attenuation. As a result, the assumption about the mean photon number of the quantum states is no longer valid.		
Proposed Countermeasures	The countermeasures against this attack rely on the assumption that the input light injected by Eve is upper bounded by physical means (e.g., laser damage threshold). Under that assumption, some of the general countermeasures mentioned in Section 4.5 are applicable for preventing this attack. These include: - Using optical isolation **(C1)** and watchdog detectors **(C2)**. - Monitoring the health of implemented countermeasures **(C3)**.		
Remarks	The decrease in attenuation renders the signal pulses with a much higher mean photon number, which opens up the loophole related to PNS attacks (see Section 2.5.1).		
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work on commercially available attenuators. While for fixed attenuators there was a temporary decrease (2 dB), for VOAs based on MEMS elements (9.2 dB) and variable-density metal-coating (9.6 dB), the decrease was permanent. It is expected to work on similar implementations.		
Reference(s)	**Huang2020**		

Table 4.32: Laser-damage attack against optical attenuators in QKD systems

Name	Pulse-intensity-increase in bidirectional QKD configurations		
Category	Laser-seeding attack		
Component	Transmitter	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Enhanced-Basic	**Attack Type**	Active
Protocol	Applicable to any QKD protocol with a bidirectional configuration. For illustration purposes, so far the scientific literature has mainly considered the BB84 and the SARG04 protocols with phase coding.		
Target(s)	Enabling other attacks		
Short Description	Eve increases the intensity of Alice's emitted optical pulses by replacing the pulses that Bob sends to Alice with others of higher intensity.		
Precondition Public information	- QKD setup operating in a bidirectional configuration. - Absent or flawed pulse-intensity-monitoring detector.		
Equipment Specialised equipment	- Receiver module similar to Bob's. To exploit the intensity-increase of Alice's pulses, two alternative sets of equipment are proposed [**Sajeed2015**]: - Lossless quantum channel, quantum memory and quantum-nondemolition photon-number measurements. - BSs, optical switches and single-photon detectors.		
Description	In a bidirectional QKD setup, Bob sends strong laser pulses to Alice, who encodes her information on the received signals, attenuates them to the single-photon level, and sends them back to Bob. In this attack, Eve replaces Bob's strong laser pulses with pulses of higher intensity prepared by herself, to force Alice's emitted pulses to have higher intensity too. Indeed, in **Sajeed2015**, two specific attacks based on photon-number-splitting and unambiguous state discrimination, respectively, are proposed which exploit such intensity increase of Alice's signals to provide Eve full information about the generated key. Also, the finite precision of Alice's calibration process might as well underestimate the intensity of her emitted pulses. This violates a crucial assumption in QKD security proofs, and can be exploited by Eve to learn complete (or partial) information about the generated key.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack, and can be combined with tailored security proofs [**Zhao2008a**, **Zhao2010**]. This includes: - Using watchdog detectors **(C2)** and spectral filtering **(C4)**.		
Remarks	The results in **Sajeed2015** highlight the difficulty of properly designing a hack-proof monitoring detector, which is a common countermeasure against many quantum hacking attacks.		

Feasibility $t_{Attack} < 1$ day	The possibility to increase the intensity of Alice's input pulses without the monitoring detector (that is included in the ID Quantique's commercial QKD system Clavis2) raising an alarm has been experimentally proven in **Sajeed2015**.
Reference(s)	**Zhao2008a**, **Zhao2010**, **Sajeed2015**

Table 4.33: Pulse-intensity-increase in bidirectional QKD configurations

Name	Variation of laser's characteristics via temperature increase		
Category	Laser-seeding attack		
Component	Transmitter	**Subcomponent**	Laser diode
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use gain-switched lasers to generate the quantum signals. For illustration purposes, so far it has been applied to the BB84 protocol (with and without decoy states).		
Target(s)	Complete knowledge of the key Enabling other attacks		
Short Description	Eve uses strong light illumination to increase the temperature of Alice's laser diode in order to vary its working characteristics, and create side channels that leak information about Alice's choice of settings and, thus, about the key.		
Precondition Public information	- Use of gain-switched lasers to generate Alice's quantum signals. - Use of polarisation coding with multiple lasers, each of them generating a different state (e.g., BB84 states). This is required in **Lee2019** and in one attack in **Fei2018**.		
Equipment Bespoke equipment	- Laser or microwave source [**Fei2018**, **Lee2019**]. - A QND measurement together with an optical switch [**Fei2018**].		
Description	The temperature of laser diodes can be increased by illuminating them with strong light, even if they are installed with thermoelectric coolers, as experimentally demonstrated in **Lee2017**. This effect can also be achieved with microwave radiation. As a consequence of this temperature increase, various characteristics of the laser change. This includes, e.g., the wavelength of the emitted signals [**Lee2017**, **Lee2019**], the recovery time of the carrier density, the intensity of the output pulses, and the time interval between signal state and decoy state pulses [**Fei2018**]. Note that a variation of the recovery time of the carrier density can produce large intensity fluctuations between adjacent pulses, as well as a variation of their emission time, when the laser works at a frequency near the maximum repetition rate. All these effects break standard assumptions in most QKD security proofs. **Lee2019** exploits the change of the wavelength of the emitted signals to experimentally demonstrate a simple attack against a polarisation-based BB84 protocol implemented with four lasers where Eve can learn the key without introducing any error. Eve sends Alice strong light in a certain BB84 polarisation state to increase the temperature of all of Alice's lasers except the one preparing pulses with polarisation orthogonal to the one injected by Eve. As a result, the frequency of all pulses (except those with orthogonal polarisation) is shifted and can be blocked with a		

Description	wavelength filter. Once Alice and Bob announce their basis, Eve learns all shifted keys. Alternatively, Eve can also try to distinguish Alice's emitted pulses based on the emission time of the pulses, as this also changes for all lasers except the one preparing states orthogonal to that injected by Eve [**Fei2018**]. In this later theoretical work, it is also proposed a modified photon-number-splitting (PNS) attack against a decoy-state BB84 protocol, where Eve exploits the pulses' emission time to partly distinguish signal and decoy pulses. This allows her to treat Alice's pulses differently depending on their identity. For the experimental parameters considered, **Fei2018** theoretically demonstrates that such PNS attack could provide Eve complete information of the key, while preserving the expected detection statistics at Bob's side of both signal and decoy pulses, for transmission distances above about 50 km.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using optical isolation (**C1**) and watchdog detectors (**C2**). - Monitoring the health of implemented countermeasures (**C3**). - Incorporate the imperfections, i.e., Eve's ability to force information leakage and emission of multimode signals, in the security proof (**C5**). - Monitoring the temperature of the laser and of the chassis to detect undesired variations.
Remarks	-
Feasibility $t_{Attack} < 1$ day	The attack in **Lee2019** has been experimentally demonstrated against a free-space QKD setup. The attack in **Fei2018** has not yet been experimentally demonstrated.
Reference(s)	**Lee2017**, **Fei2018**, **Lee2019**

Table 4.34: Variation of laser's characteristics via temperature increase

Name	Injection-locking attack		
Category	Laser-seeding attack		
Component	Transmitter	**Subcomponent**	Laser diode
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to QKD protocols that use laser sources to generate the quantum states. For illustration purposes, so far it has been investigated against the BB84 protocol (with and without decoy states), measurement-device-independent QKD (MDI-QKD), and a variant of twin-field QKD (TF-QKD).		
Target(s)	Complete knowledge of the key		
Short Description	Injection of optical pulses into Alice's laser diode that lead to a conditional frequency shift of Alice's emitted pulses depending on their quantum state. This allows Eve to distinguish Alice's states with a frequency filter.		
Precondition Public information	- Use of polarisation coding by Alice to encode the quantum states [**Pang2020**]. - Absence of internal isolation in Alice's laser diode [**Zhang2022a**]. - The period of Alice's emitted pulses matches the time interval between her laser and the intensity modulator that encodes the decoy states [**Zhang2022a**]. This ensures that Eve's injected light is attenuated by the intensity modulator before affecting the frequency of Alice's following pulse, thus correlating the intensity settings chosen by Alice with the frequency of her emitted signals.		
Equipment Bespoke equipment	- A laser source to send off-resonance photons to Alice. - A frequency filter to block the unwanted pulses from Alice, and a frequency-shifting device, e.g., an acoustic optical modulator, to restore the frequency of Alice's unblocked pulses [**Pang2020**]. - A wavelength division multiplexer, to discriminate Alice's optical pulses based on their wavelength, and equipment to perform a PNS attack [**Zhang2022a**].		
Description	This attack exploits a phenomenon called injection locking. Essentially, Eve injects near off-resonance optical pulses into Alice's laser to shift the frequency of the emitted signals depending on the intensity of the injected light. Importantly, this intensity can be made dependent on the states prepared by Alice. For instance, in **Pang2020**, Eve injects light in a polarisation state chosen at random to try to match that of Alice. When she succeeds, and the intensity of the injected pulse is sufficiently strong, injection locking happens at a shifted frequency equal to that of Eve's laser. Otherwise, the frequency of Alice's pulses is only partially shifted, or not shifted at all (when Eve's polarisation state is orthogonal to that of Alice). In doing so, the frequency of the matched pulses becomes distinct from the unmatched cases, and Eve can separate and resend Bob the matched ones (after		

Description	converting their frequency to the original value). If Eve would have perfect devices, this attack would provide her complete information of the key. A proof-of-principle experimental demonstration (with imperfect devices) against a MDI-QKD transmitter has been reported in **Pang2020** where Eve learns about 60% of the raw key, while introducing a QBER of about 6.1%. The implications of the attack against the BB84 protocol (with and without decoy states and with single-photon sources) as well as against a variant of TF-QKD, have been theoretically investigated in **Pang2020** and **Zhang2022a**. In the case of decoy-state QKD, Eve's injected light is attenuated differently depending on Alice's intensity choice, and Eve can distinguish decoy and signal states by analysing the frequency of successive pulses. In all cases, it is shown that Eve can learn information about the generated key without being detected.
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Employing optical isolation (**C1**). - Using watchdog detectors (**C2**). - Monitoring the health of implemented countermeasures (**C3**). - Incorporating the imperfection in a security proof (**C5**). Other specific countermeasures include: - Controlling the pulse repetition period of Alice's laser so that it does not match the time interval between the laser and the intensity modulator [**Zhang2022a**].
Remarks	Given that Eve can force Alice to produce polarisation states in a different spectral region, this vulnerability can be exploited by hacking attacks other than the one described in **Pang2020**.
Feasibility $t_{Attack} < 1$ day	The attack was experimentally demonstrated against a lab-based MDI-QKD setup in **Pang2020**.
Reference(s)	**Pang2020**, **Zhang2022a**

Table 4.35: Injection-locking attack

Name	Information leakage through electromagnetic radiation		
Category	Classical side-channel attack		
Component	Multiple entry points	**Subcomponent**	Any component emitting electromagnetic radiation
Expertise	Proficient	**Opportunity**	Difficult
Attack Rating	Beyond High	**Attack Type**	Passive
Protocol	Applicable to any QKD protocol, both based on discrete or continuous variables. So far, the scientific literature has mainly considered the BB84 protocol (with and without decoy states), and with a plug-and-play configuration.		
Target(s)	Complete knowledge of the key		
Short Description	Eve measures the electromagnetic radiation emitted by Alice's transmitter and/or Bob's receiver to learn information about the generated key.		
Precondition Public information	Use of optical modulators (e.g., intensity, polarisation and/or phase modulators) to encode the state of Alice's emitted quantum signals [**Kim2018**].		
Equipment Specialised equipment	- Oscilloscope. - Electromagnetic probe. - Quantum memory (optional). Sophisticated attacks may involve joint measurements on the electromagnetic radiation and the quantum signals emitted by Alice, supported by quantum memories.		
Description	In this attack, Eve takes advantage of the information leaked through electromagnetic radiation by Alice and/or Bob's QKD devices to learn information about the generated key. For instance, in **Kim2018**, the authors experimentally measured the electromagnetic trace emitted by Alice's phase modulator in a BB84 protocol with a plug-and-play configuration. In doing so, this work was able to identify the BB84 state encoded by Alice each given time. **Molotkov2013** and **Molotkov2020c** consider the problem of how to incorporate the effect of passive information leakage into the asymptotic security of QKD. For this, it is assumed a particular side-channel model, that the side-channel states are known, and Eve measures them independently from Alice's emitted quantum signals. The asymptotic security of decoy-state BB84 against various specific collective attacks (not necessarily optimal) in the presence of both passive and active information leakage from the phase modulator is studied in **Molotkov2019**.		

Proposed Countermeasures	Main countermeasures include the following: - Use of similar techniques like those employed to protect classical encryption of key handling equipment, including electromagnetic shielding, such as a Faraday cage, to significantly reduce the intensity of the electromagnetic radiation. - Incorporate the effect of information leakage in the QKD security proof by using, e.g., the tools in **Navarrete2022** and **CurrasLorenzo2023**, which do not need to know the side-channel states and can protect against general adversary models.
Remarks	Machine learning algorithms might be used to extract information from the leaked electromagnetic radiation. Similar conclusions apply to other types of passive information leakage.
Feasibility $t_{Attack} < 1$ week	An example of attack has been experimentally demonstrated against a BB84 protocol with a plug-and-play configuration in **Kim2018**. Similar attacks have been successfully launched against classical cryptosystems.
Reference(s)	**Kim2018**, **Molotkov2013**, **Molotkov2019**, **Molotkov2020c**, **Navarrete2022**, **CurrasLorenzo2023**

Table 4.36: Information leakage through electromagnetic radiation

4.2 CV-QKD Attack Tables

In this section, attack tables for implementation attacks which are mostly relevant to CV-QKD systems and protocols are listed.

Number	Attack Table Name
Table 4.38	Manipulation of vacuum-noise estimation
Table 4.39	Wavelength-dependent beamsplitter attack (CV)
Table 4.40	Saturation attack
Table 4.41	CV detector-control attack
Table 4.42	Leakage in state preparation
Table 4.43	Exploitation of an imperfect quantum channel model
Table 4.44	CV laser-seeding
Table 4.45	Attack exploiting the trusted phase noise model
Table 4.46	Power analysis of integrated systems

Table 4.37: List of CV-QKD attack tables

Name	Manipulation of vacuum-noise estimation		
Category	Calibration attack		
Component	Receiver	**Subcomponent**	LO monitor
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Enhanced-Basic	**Attack Type**	Active
Protocol	Applicable to any CV-QKD protocol implementation where the LO is also transmitted on the quantum channel. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Enabling other attacks		
Short Description	Exploiting the relationship between vacuum-noise variance and LO parameters (by manipulating the LO) to mask the excess noise arising from other type of attacks.		
Precondition Public information	- LO transmitted on the open quantum channel from Alice to Bob. - Bob relies on a LO-assisted calibration of vacuum-noise level. - Missing/imperfect LO power monitoring in Bob.		
Equipment Specialised equipment	- Optical delay line, power meter, attenuator for manifesting the vulnerability. - Intercept-and-resend attack apparatus (see Section 2.5.2).		
Description	The fundamental role of the LO and the significance of vacuum noise to the operation and security of CV-QKD systems has been elaborated in Section 2.3.2. It is well known that the variance of the vacuum noise has a linear relationship with the LO power, and this is how CV-QKD systems calibrate the vacuum noise level. To elaborate, during the QKD protocol run, the CV-QKD receiver measures the (incoming) LO power to evaluate the vacuum noise variance and uses it in the estimation of the channel parameters. This calibration is, however, subject to manipulation for CV-QKD implementations in which the LO is transmitted (together with the quantum signal) on the open quantum channel. The manipulation allows Eve to influence what Alice and Bob believe is their knowledge of Eve's interference, thus resulting in the generation of an insecure key at the end of the QKD protocol. It was first reported in **Ferenczi2007** and **Haeseler2008**, how Eve could manipulate the LO power in the channel to modify the vacuum-noise variance estimated by Bob, resulting in the estimate of "excess noise" to be lower than the actual value. This difference facilitates an intercept-and-resend attack through which Eve could enhance her knowledge of the key without Alice and Bob noticing it. **Ma2013a** focused on the idea of exploiting the "fluctuations" in the LO power, and simulated a successful general Gaussian collective attack, assuming Eve's tampering with the LO power in the channel goes unnoticed. In **Jouguet2013**, a proof-of-concept experiment on how to exploit the vacuum-noise calibration was reported: Eve attenuated the LO pulse front to delay the triggering of the differential photocurrent integration at Bob.		

Description	This decreased the actual vacuum-noise variance, but, unaware of this manipulation, Bob used the larger pre-calibrated value, thereby underestimating the excess noise. In **Huang2014**, the wavelength-dependent behaviour of components, particularly BSs, was exploited to manipulate the vacuum-noise measurements. Eve performed an intercept-and-resend attack, and biased the vacuum-noise estimation to her advantage by (re)sending light at three different wavelengths. Notably, the attack was shown to be successful even if Bob estimated the vacuum-noise in real time (instead of relying on a pre-calibrated relationship with LO power). In **Zhao2018**, the authors sketched an attack where Eve modulates the polarisation of a pre-identified set of LO pulses in the channel to control the LO power.
Proposed Countermeasures	Several countermeasures to the aforementioned attacks have been proposed, with a majority of them focusing—with various levels of intricacy—on some form of monitoring in the CV-QKD receiver. Note that some countermeasures have already been shown to be ineffective due to other imperfections in the CV-QKD system. - Monitor the power of the "transmitted" LO after it arrives at Bob if using the pre-calibrated relationship of the vacuum-noise variance with the LO power [**Ferenczi2007**, **Haeseler2008**, **Wittmann2010**], and not just the average but also the instantaneous LO power [**Ma2013a**]. In **Wittmann2010**, it was additionally suggested to compare the LO excess noise with the coherent detector's common mode rejection ratio[13]. - Measure the vacuum-noise in real time (instead of relying on any pre-calibrated relationship) through hardware modifications, e.g., an optical switch / intensity modulator or an additional homodyne detector, inside the CV-QKD receiver [**Jouguet2013**]. As explained before, the implementation of this countermeasure was found to be ineffective in **Huang2014** due to the wavelength-dependent behaviour of some components, and it was then evident that filtering the optical radiation entering the CV-QKD receiver was required in addition to prevent Eve's exploitation of this behaviour. - Acquire and process in real-time the quadrature measurements at randomly chosen optical attenuations of the quantum signal arriving in Bob [**KunzJacques2015**]. It was shown (via simulations) that Eve's manipulation modifies an otherwise linear relation between the variance of the signal and the variance of noise, thus revealing the attack. The countermeasure, while being robust against the wavelength-dependent behaviour of **Huang2014**, requires extra hardware[14]. - Combine the three aforementioned approaches and calculate (during parameter estimation) inter alia a constraint quantifying the manipulation of the LO power by Eve who is assumed to be additionally launching arbitrary individual or collective attacks on the quantum signal [**Liu2017**, **Zheng2020**].

[13] This measure could probably be defeated if Eve exploits the wavelength-dependent behaviour shown in **Huang2014**.

[14] And it also introduces an undesired loss of the quantum signal.

Proposed Countermeasures	- Synchronise the instantaneous analogue outputs of the LO monitor and the coherent detector, and locate a peak or valley in the quadrature measurement outcomes [**Huang2017**], as this also provides an attack signature[15]. - Use machine-learning-based approaches to recognise attacks through monitoring the variation of the quadrature values. In **Mao2020**, measurement results under a no-attack scenario are used to train the parameters of a hidden Markov model, while in **Mao2020a**, a set of feature vectors labeled by the calibration vulnerability and LO manipulation is constructed to train an artificial neural network. In both cases, the authors claim via simulations that deviations between normal data and abnormal data lead to attack recognition with a high precision. - Self-manipulation by Bob of the LO power to stabilise it to a required optimal constant value, suggested in **Ma2014**, can improve the resistance to Eve's manipulation. - Eve cannot have any influence on the vacuum-noise measurements if Bob generates as well as uses the LO locally inside the CV-QKD receiver. Such "local" LO-based CV-QKD implementations, proposed first in **Qi2015** and **Soh2015**, are naturally protected from the attacks discussed in this table.
Remarks	-
Feasibility $t_{Attack} < 1$ day	Proof-of-concept experimental measurements showcase the vulnerability, which is expected to manifest on similar implementations. Some countermeasures can be implemented in hardware and (data processing) software.
Reference(s)	**Ferenczi2007**, **Haeseler2008**, **Wittmann2010**, **Jouguet2013**, **Ma2013a**, **Ma2014**, **Huang2014**, **KunzJacques2015**, **Qi2015**, **Soh2015**, **Liu2017**, **Huang2017**, **Zhao2018**, **Mao2020**, **Mao2020a**, **Zheng2020**

Table 4.38: Manipulation of vacuum-noise estimation

[15] While the optical setup before the detector does not change, the countermeasure is effectively implemented only with large oversampling and fast data processing, which may require using a high-speed analogue to digital converter (ADC) and field programmable gate array (FPGA)/graphics processing unit (GPU).

Name	Wavelength-dependent beamsplitter attack (CV)		
Category	Wavelength-dependent manipulation attack		
Component	Receiver	**Subcomponent**	Beamsplitter
Expertise	Expert	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any coherent-state CV-QKD protocol that satisfies the preconditions. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Partial knowledge of the key Enabling other attacks		
Short Description	Controlling measurement results of Bob by exploiting the wavelength dependence of the beamsplitter used in the QKD receiver.		
Precondition Public information	- Bob uses beamsplitter(s) in his coherent receiver that exhibit(s) wavelength-dependent transmittance and reflectance. - Alice transmits the LO to Bob on the quantum channel.		
Equipment Specialised equipment	Intercept-and-resend equipment for multiple wavelengths: - Detection module to measure the quantum signals from Alice - Multi-wavelength sources and modulators to prepare and send optical signals to Bob.		
Description	The behaviour of optical components may strongly depend on properties such as the wavelength of the input light. For instance, the coupling ratio of an optical beamsplitter (see Section 2.4.4.1) changes from 50:50 at 1550 nm to nearly 99:1 at 1470 nm [**Li2011**]. Attacks on DV-QKD systems that exploit such a behaviour are provided in Table 4.21. **Huang2013** extended this idea to control the measurement outcomes in CV-QKD systems that perform dual-quadrature measurements using a heterodyne detector[16]. The basic idea of this attack (and in fact, all attacks discussed in this table) is to exploit the wavelength-dependent properties of beamsplitters and other components to mask the noise added by an intercept-and-resend attack (see Section 2.5.2). In **Ma2013**, the authors provide a more rigorous analysis of the same attack (1) by considering the vacuum noise of the (classical) states at different wavelengths that Eve sends to Bob, and (2) by solving the equations—describing Eve's constraints—in a practical parameter regime for validating the attack (both of these were neglected in **Huang2013**). The work of **Tan2021** explores on how to exploit this wavelength-dependent imperfection when atmospheric links are used as quantum channels, i.e., in cases where the assumption of the channel transmittance being a constant may not hold (see also Table 4.43). The manipulation of the vacuum-noise estimation by exploiting the wavelength-dependent behaviour of beamsplitters [**Huang2014**] has already been explained in Table 4.38.		

[16] A phase-diverse receiver is the correct term for what is often called "heterodyne detector" in CV-QKD papers.

Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using spectral monitoring of the input optical signals **(C2)** and optical isolation through wavelength filters **(C4)**. This, however, is with the caveat that since Eve could always increase the intensity of her signals, Bob should actually choose between monitoring with/without a wavelength filter randomly [**Huang2013**], while also checking the health of the implemented countermeasures (C3). Other specific countermeasures include: - Acquire and process in real-time the quadrature measurements at randomly chosen optical attenuations of the quantum signal arriving at Bob [**KunzJacques2015**]. It was shown (via simulations) that Eve's manipulation modifies an otherwise linear relation between the variance of the signal and the variance of noise, thus revealing the attack. The countermeasure, while being robust against the wavelength-dependent behaviour of **Huang2014**, requires extra hardware[17].
Remarks	Eve can neither have any influence on the vacuum-noise measurements [**Huang2014**] nor has sufficient constraints to satisfy for an intercept-and-resend attack [**Huang2013**, **Ma2013**, **Tan2021**] if Bob generates as well as uses the LO locally inside the CV-QKD receiver. Such "local" LO-based CV-QKD implementations, proposed first in **Qi2015** and **Soh2015**, might be naturally protected from the attacks discussed in this table.
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Li2011**, **Huang2013**, **Ma2013**, **Huang2014**, **KunzJacques2015**, **Soh2015**, **Qi2015**, **Tan2021**

Table 4.39: Wavelength-dependent beamsplitter attack (CV)

[17] And it also introduces an undesired loss of the quantum signal.

Name	Saturation attack		
Category	Saturation attack		
Component	Receiver	**Subcomponent**	Coherent detector
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to both coherent-state (modulation-based) and squeezed-state CV-QKD protocols. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Complete knowledge of the key		
Short Description	Saturating the detector by injecting light into the CV-QKD receiver to mask the increase of excess noise from an accompanying intercept-and-resend attack.		
Precondition Public information	- Detectors get saturated above a certain power of impinging light. - Attenuation of quantum channel is above approximately 6 dB. - First-order moments (mean values) are not monitored by the CV-QKD receiver.		
Equipment Bespoke equipment	- Intercept-and-resend attack apparatus (see Section 2.5.2), i.e., a receiver similar to the legitimate QKD receiver (for interception of photons from the QKD transmitter) and a transmitter having its laser locked to Alice's laser. -Unbalanced beamsplitter for mixing the quantum signal with an intense beam.		
Description	The attack here exploits imperfections in coherent detectors, which are described in some detail in Section 2.4.2.1. In this attack the detection outcomes are saturated; In the context of homodyne detection, instead of measuring a quantity proportional to the quadrature x, the outcome is instead $\mathrm{Min}(\mathrm{Max}(x, -\alpha), \alpha)$ for some $\alpha > 0$ [**KunzJacques2015**]. The attack described in **Qin2013** is an intercept-and-resend attack which is performed while the saturation of the receiver's detector is induced. The detector can be saturated due to the limited linearity of the photodiodes and/or the limited range of analog-to-digital conversion. In this way, the attacker can bias the excess noise estimation by displacing in phase space the mean value of the coherent states that impinge on the detector. By reducing the measured excess noise, the added noise of the intercept-and-resend attack is masked. The estimated channel transmission has to be left unchanged for the attack to remain unnoticed. Therefore, the attacker rescales her sent states by a gain factor. The interplay between displacement and gain requires the original channel attenuation to be above approximately 6 dB for this attack to remain unnoticed.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**).		

Proposed Countermeasures	- Using CV MDI-QKD protocols (**C9**). Specific countermeasures include: - Discard all data blocks exhibiting measurement outcomes outside the linearity region, while taking care of the Gaussianity of the remaining data [**Qin2016**]. - Attenuation on the receiver's signal port can be randomly varied in order to verify the linearity of the detector. This countermeasure requires additional hardware and also reduces the key rate due to additional attenuation [**KunzJacques2015**]. - **Xu2022** proposes using an adjustable optical filter. - Simulations with an artificial neural network (inputs: mean and variance of signal, intensity of local oscillator, shot noise variance) can identify the saturation attack [**Mao2020a**].
Remarks	**Kumar2021** evaluated this attack using an approach based on the CEM resulting in a similar attack rating.
Feasibility $t_{Attack} < 1$ day	The working principles of the attack have been demonstrated in several experiments and simulations, but a full attack has not been published yet.
Reference(s)	**Qin2013**, **KunzJacques2015**, **Qin2016**, **Mao2020a**, **Kumar2021**, **Xu2022**

Table 4.40: Saturation attack

Name	CV detector-control attack		
Category	Detector-control attack		
Component	Receiver	**Subcomponent**	DC balancing
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to the GMCS protocol.		
Target(s)	Complete knowledge of the key		
Short Description	Injecting bright light into the signal port of the CV-QKD receiver to saturate the detector electronics and mask other attacks.		
Precondition Public information	- Balancing of homodyne detector is not optimal for signal. - Homodyne detector has finite linear detection range due to saturation in ADC, amplifier or P(I)N photodiodes.		
Equipment Specialised equipment	- Sender and receiver as used by legitimate parties. - Laser (can be incoherent to signal).		
Description	This attack expands on saturation attacks presented in Table 4.40, which exploit imperfections in coherent detectors that are described in Section 2.4.2.1. Since coherently displacing the signal without adding detectable excess noise is challenging, a CV detector-control attack without the need for coherence between signal and attack laser has been developed [**Qin2018**]: Bright pulses are sent onto the signal port of the homodyne detector in order to induce electronics saturation. Usually, balancing is optimised for the LO and therefore not ideal for signal, such that strong light on the signal port can lead to electronics saturation. The excess noise measurement is biased due to saturation, allowing the additional noise of an intercept-resend attack to be concealed.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**). - Using CV MDI-QKD protocols (**C9**). Specific countermeasures include: - Monitoring photocurrents from the photodiodes. - Randomly varying the attenuation on the signal port to verify the linearity of the detector. This countermeasure requires additional hardware and reduces the key rate [**KunzJacques2015**]. - Using security thresholds in data postprocessing.		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	The working principle of this attack has been demonstrated by characterisation measurements and simulations in **Qin2018**.		
Reference(s)	**KunzJacques2015**, **Qin2018**		

Table 4.41: CV detector-control attack

Name	Leakage in state preparation		
Category	Excessive modulation attack		
Component	Transmitter	**Subcomponent**	Quadrature modulator
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to both coherent-state (modulation-based) and squeezed-state CV-QKD protocols. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Partial knowledge of the key		
Short Description	Information about single-mode quantum states can be leaked when multiple modes are generated (instead of only a single mode). For squeezed-state based protocols, leakage from before the modulation can lead to this side channel.		
Precondition Public information	- Coherent states are (weakly) encoded using "single-sideband modulation" into single frequency sidebands of the carrier at the transmitter and measured with RF heterodyne detection at the receiver. - Alternatively, too strong modulation in displacing the vacuum states or squeezed-vacuum states could also lead to generation of multiple modes. - For squeezed states some optical reflection before the modulation needs to leave the transmitter and be captured by Eve.		
Equipment Specialised equipment	- For coherent state protocols with single-sideband modulation, an optical filter for splitting off the excessive modes from the desired ones. - For coherent and squeezed state protocols, a QKD receiver module, similar to that of the TOE, capable of detecting and analysing the excessive modes.		
Description	Typical QKD protocols consider the quantum states to be in single optical modes. If the state preparation in the transmitter however prepares the quantum states in multiple modes instead, while the receiver only measures one mode, the additional or excessive modes (also containing information about the quantum state) can be captured by Eve. If Eve is able to do this while evading detection by the legitimate parties, she obtains a non-negligible knowledge of the key without degrading the quantum correlations between Alice and Bob, thus compromising the security of the protocol [**Derkach2016**, **Derkach2017**]. Optical single-sideband modulation (OSSB) is an encoding technique for coherent states, prone to modulation of multiple modes due to imperfect devices [**Jain2021**]. OSSB is obtained by driving a phase modulator and an amplitude modulator, or the two arms of an in-phase-and-quadrature (IQ) modulator, with phase conjugate waveforms. This is done such that the lower (upper)		

Description	modulation sidebands of the optical carrier are suppressed while the upper (lower) ones are enhanced and used as the quantum information carrying signal. Ideally, the suppression is perfect, however inreal devices, typical suppression factors of 20 to 40 dB are achieved. Typically, RF heterodyne detection is used in conjunction with OSSB to simultaneously measure the amplitude and phase quadratures of light; see Section 2.4.2.1. If the QKD receiver measures only the desired quantum-information carrying signal without taking cognisance of the suppressed frequency sidebands, then such excessive modulation is a side channel that can be exploited by Eve. A side channel can also arise due to leakage during state preparation before the modulation stage. In **Derkach2016**, it has been shown that coherent-state protocols are not affected by this side channel because the leaked mode is uncorrelated to the modulated mode. Squeezed-state protocols are however vulnerable as the modes are quantum correlated.
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this class of attacks. These include: - Combining optical isolation **(C1)** and monitoring state preparation **(C7)** for squeezed-state protocols. - Incorporating the imperfection in security proofs **(C5)**. Other specific countermeasures include: - Using baseband modulation instead of OSSB [**Hajomer2022**].
Remarks	-
Feasibility $t_{Attack} < 1$ day	Proof-of-concept experimental measurements in **Jain2021** showcase the vulnerability in OSSB coherent state protocols, which is expected to manifest on similar implementations.
Reference(s)	**Derkach2016**, **Derkach2017**, **Jain2021**, **Hajomer2022**

Table 4.42: Leakage in state preparation

Name	Exploitation of an imperfect quantum channel model		
Category	Calibration attack		
Component	Receiver	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Easy
Attack rating	High	**Attack Type**	Active
Protocol	Applicable to both coherent-state (modulation-based) and squeezed-state CV-QKD protocols. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Enabling other attacks		
Short description	Exploit an imperfect channel transmittance model that leads to an overestimation of the secret key length.		
Precondition Public information	Alice and Bob use an imperfect channel model/uncalibrated channel transmittance.		
Equipment Bespoke equipment	- Intercept-and-resend apparatus. - Variable BS.		
Description	The propagation of quantum states in atmospheric channels is affected by several elements such as turbulence, pointing errors, diffraction effects, and background noise. This implies that the transmittance of the quantum channel is not constant in time, and in the case of CV-QKD systems, can lead to a non-Gaussian mixed state at the receiver. This resulting degradation of the (virtual) entanglement needs to be properly taken into consideration by the QKD users, otherwise, as shown in **Guo2017**, Eve can apply an intercept-and-resend attack to bias the estimation of parameters that are evaluated in the later stages of the QKD protocol. The attack involves Eve performing entanglement distillation to obtain information about the key while staying undisclosed to the QKD users, thus violating the security assurance the QKD system is supposed to provide. Furthermore, using a convolutional neural network, as described in **Huang2019b**, Eve can improve her predictions about the instances of non-Gaussian mixture, thus enhancing her eavesdropping capability.		
Proposed Countermeasures	See “Remarks” below.		
Remarks	A proper calibration of the quantum channel performed at random instances is expected to prevent this attack.		
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.		
Reference(s)	**Guo2017**, **Huang2019b**		

Table 4.43: Exploitation of an imperfect quantum channel model

Name	CV laser-seeding		
Category	Laser-seeding attack		
Component	Transmitter	**Subcomponent**	Laser
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Basic	**Attack Type**	Active
Protocol	Applicable to any protocol employing coherent states.		
Target(s)	Partial knowledge of the key		
Short Description	Light injection into the laser modules of the QKD transmitter leads to increased intensity of the quantum signal which an attacker can split off and measure to acquire extra knowledge.		
Precondition Public information	A seedable laser is used for the creation of quantum states.		
Equipment Standard equipment	- Tuneable seed laser. - Polarisation control can optimise the attack.		
Description	The attacker injects light at Alice's pump transition wavelength into the laser modules of the QKD transmitter, which results in an increased intensity of the generated optical signal. This so-called laser seeding is possible in the widely used laser diodes, but also in further laser types [**Huang2019**, **Zheng2019**]. The increased intensity due to seeding allows the attacker to split off the surplus part of the signal beam while the receiver detects the expected signal.		
Proposed Countermeasures	Some of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include: - Using watchdog detectors (**C2**). - Monitoring the state preparation process in real time (**C7**). Contrary to intuition, optical isolators may not be able to prevent this attack since small amounts of transmitted light have been shown to be sufficient for this attack [**Huang2019**]. Furthermore, optical isolators can be manipulated or destroyed through a preceding laser-damage attack (see e.g., Table 4.31).		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	This attack is a theoretical proposal for CV-QKD systems. However, it has been shown to work in a DV context [**Sun2015a**] and can be transferred to CV systems.		
Reference(s)	**Sun2015a**, **Huang2019**, **Zheng2019**		

Table 4.44: CV laser-seeding

Name	Attack exploiting the trusted phase noise model		
Category	Phase-reference-alignment attack		
Component	Receiver	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Easy
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any CV-QKD protocol implementation that assumes a portion of the excess noise stemming from phase noise can be trusted. So far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Enabling other attacks		
Short Description	Manipulating the classical signal used for phase-reference alignment between the CV-QKD transmitter and receiver, and taking advantage of the fact that Alice and Bob do not attribute some of the errors (in this phase-reference alignment process) to Eve.		
Precondition Restricted information	Alice and Bob trust a part of the excess noise that stems from the imperfect phase-reference alignment, required in the local LO type of CV-QKD implementations.		
Equipment Specialised equipment	- Fast optical switch. - Low-loss quantum channel. - Phase-insensitive amplifier.		
Description	Generation of the LO locally inside the CV-QKD receiver prevents the vulnerability reported in Table 4.38. In such local LO CV-QKD implementations, the phase reference is then provided by (classical) reference signals—pulses/pilot tones multiplexed in time/frequency—to the quantum signal in the CV-QKD transmitter (see Section 2.3.2). However, an accurate phase-reference alignment is hard to achieve in such implementations due to the laser phase noise and the inevitable phase estimation error in the coherent detection of the reference signals. Attributing all the errors from the phase-reference alignment procedure to Eve adversely affects the performance: For instance, it can easily lead to a zero secret key length. In the so-called trusted-phase-noise model, error contributions (arising in the alignment process) that cannot be realistically influenced by Eve are identified, and the CV-QKD system is calibrated to trust the corresponding portion of excess noise. In **Ren2019** and **Ren2019a**, the authors propose an attack where the reference signals are routed (via a fast switch) through a low-loss channel segment inserted in the quantum channel connecting Alice and Bob. This results in Bob obtaining reference signals with a higher amplitude, which should potentially lower his phase estimation error. The corresponding reduction, however, is exploited by Eve, e.g., through a more intense collective attack on the quantum signals that considerably increases her correlations with the secret key (while also increasing the corresponding excess		

Description	noise contribution, however, while preserving the total excess noise to "without attack" conditions). Since Alice and Bob cannot distinguish between the two sources of excess noise, they underestimate Eve's knowledge of the key. **Shao2022** proposes two practical attack schemes essentially to the same effect. In the first, they suggest using a phase-insensitive amplifier instead of the low-loss channel. In the second, they suggest attenuating the intensity of the phase-reference signals during the calibration stage, but increasing it later, i.e., during the actual quantum key exchange.
Proposed Countermeasures	- Using an upgraded trusted-phase-noise model where the noise contribution to be tolerated assumes a lossless channel for the reference signal transmission [**Ren2019**, **Ren2019a**]. - Monitoring the instantaneous amplitude of the reference signals and calibrating phase noise in real time, so that Eve's information can be accordingly upgraded [**Ren2019**, **Ren2019a**, **Shao2022**].
Remarks	**Ren2019** and **Ren2019a** essentially describe the same attack.
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.
Reference(s)	**Ren2019**, **Ren2019a**, **Shao2022**

Table 4.45: Attack exploiting the trusted phase noise model

Name	Power analysis of integrated systems		
Category	Degree-of-freedom coupling attack		
Component	Transmitter	**Subcomponent**	-
Expertise	Proficient	**Opportunity**	Difficult
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any QKD protocol implementation. For illustration purposes, so far the scientific literature has mainly considered the GMCS protocol.		
Target(s)	Partial knowledge of the key		
Short Description	Analysing the power consumption originating from the integrated electrical control circuit used for state preparation.		
Precondition Public information	Alice prepares quantum states by using an integrated electrical control circuit whose power consumption is accessible to the eavesdropper.		
Equipment Standard equipment	- Identical transmitter chip to analyse the relationship between sent quantum states and power consumption. - Power meter that can resolve transients from switching of transmitter states. - Machine learning algorithm such as support vector regression (SVR) to handle nonlinear correlations between power and modulated signal states.		
Description	This attack can be implemented by analysing the power consumption originating from the integrated electrical control circuit that is used for state preparation [**Zheng2021**]. Machine learning can help to correlate the analysed power with generated quantum states. The attacker does not have to physically access the transmitter chip. A similar attack could be performed on DV-QKD systems.		
Proposed Countermeasures	- Randomising the power of the electrical control circuit can be an effective countermeasure for classical chips. Adaptation of this approach for QKD transmitters, however, would have to be investigated in more detail. - Dynamic voltage and frequency scaling (DVFS) can be applied to reduce the dynamic power.		
Remarks	While known to work against conventional cryptographic systems, a transfer to QKD in practice may not be straightforward due to the fundamentally different processes of key generation.		
Feasibility $t_{Attack} < 1$ week	This side channel is a theoretical proposal against QKD systems.		
Reference(s)	**Zheng2021**		

Table 4.46: Power analysis of integrated systems

4.3 Common Attack Tables

In this section, tables for attacks which are general enough that they can be mounted on both a CV-QKD and a DV-QKD implementations are listed. It should be noted that the attacks presented in Tables 4.32 and 4.36 (currently in Section 4.1) and Table 4.46 (currently in Section 4.2) are in principle or potentially with some simple tweaks applicable to both DV-QKD and CV-QKD implementations. However, they are not presented in this section due to lack of published articles.

Number	Attack Table Name
Table 4.48	Trojan-horse attack against QKD transmitters
Table 4.49	Enabling light-injection attacks by application of external magnetic fields
Table 4.50	Hardware-software Trojans and covert channels
Table 4.51	Cache side channels in the post-processing of QKD systems
Table 4.52	Single-trace side-channel attack on information reconciliation in QKD

Table 4.47: List of attack tables which fit in both categories of CV-QKD and DV-QKD

Name	Trojan-horse attack against QKD transmitters		
Category	Trojan-horse attack		
Component	Transmitter	**Subcomponent**	Optical modulator
Expertise	Expert	**Opportunity**	Easy
Attack Rating	High	**Attack Type**	Active
Protocol	Applicable to any QKD protocol that uses optical modulators to encode the quantum signals. So far, the scientific literature has considered BB84 and some variants (e.g., with and without decoy states) and measurement-device-independent (MDI) protocols for DV-QKD systems and both discrete modulation and GMCS protocol for CV-QKD systems.		
Target(s)	Complete knowledge of the key		
Short Description	Injection of external light into the QKD transmitter and analysis of the back-reflections to obtain information about the modulators' encoding choices used for quantum state preparation.		
Precondition Public information	General assumptions: - Use of optical modulators, such as intensity, polarisation, and phase modulators to encode the state of the emitted quantum signals. - The QKD transmitter exhibits refractive index variations leading to back-reflections. Specific assumption in **GarciaEscartin2020**: - Availability of a line of sight to optical components from outside the transmitter module, e.g., through ventilation holes.		
Equipment Bespoke equipment	Suitably tweaked reflectometry equipment, i.e., - Laser source (pulsed or continuous) to inject light into the QKD transmitter. - Measurement module to analyse properties such as intensity, phase, or wavelength of the back-reflected light.		
Description	In a Trojan-horse attack (THA), Eve obtains information about the quantum states prepared by Alice by injecting her own light into the QKD transmitter and then analysing the back-reflected light, which carries information that can be correlated to the encoding of Alice's quantum states. For instance, on its return path to the channel, Eve's back-reflected light could pass through the transmitter's modulator(s) and be encoded with the same information as Alice's signals. Since modulators are used in both DV-QKD and CV-QKD transmitters, this attack is applicable to both type of implementations. For instance, in DV-QKD protocols such as BB84, a successful attack yields Eve both the bit and the basis choice of Alice (see Section 2.3.1). A CV-QKD system operating a Gaussian modulated coherent state protocol could be attacked to obtain the information about the amplitude and/or phase quadrature used in the state preparation (see Section 2.3.2).		

Description

THAs were first considered in a plug-and-play configuration of the BB84 protocol in **Zbinden2000** and **Bethune2000**. The term "Trojan-horse attack" was coined in **Gisin2006** where the authors experimentally measured an optical frequency domain reflectometry (OFDR) trace of Alice's plug-and-play DV-QKD transmitter, and demonstrated that the back-reflected light provides Eve information about Alice's signals. A similar result was already obtained in **Vakhitov2001** for a one-way BB84 configuration by using optical time domain reflectometry (OTDR). Both **Vakhitov2001** and **Gisin2006** provided rough theoretical estimates about the amount of information leaked to Eve for the case of phase modulation (phase-coded quantum signals) in Alice. OTDR has also been used in **Lucamarini2015** to experimentally characterise the reflectivity and transmission of most relevant components in a decoy-state QKD transmitter. **Jain2015** studied the feasibility of THAs through similar reflectometry measurements but at wavelengths other than those used by Alice and Bob, and with a focus on the spectral characteristics of optical elements such as isolators, circulators and monitoring detectors (typically used by QKD transmitters for protection against THAs). OFDR measurements on a silicon transmitter chip integrated with a polarisation modulator and an intensity modulator have been performed in **Tan2021a**. Proof-of-concept THAs have been performed on CV-QKD transmitters in **Stiller2015** and **Ma2016**.

Proposed Countermeasures

The countermeasures to THA rely on the assumption that the input light injected by Eve is upper bounded by physical means (e.g., laser damage threshold). Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this attack. These include:
- Using optical isolation (**C1**), watchdog detectors (**C2**), and appropriate wavelength filtering (**C4**).
- Monitoring the health of implemented countermeasures (**C3**).
- Active randomisation of the phase (**C6**).

Other specific countermeasures include:
- Usage of anti-reflection coatings and angle polished connectors [**Vakhitov2001**] as well as eliminating open ports and splicing fibre components (instead of mating sleeves) [**Jain2015**] can also reduce the level of back-reflections.
- Sensitive components should be covered with an opaque material if they are optically accessible from outside, e.g., through the ventilation holes [**GarciaEscartin2020**].
- Ensure that modulators are activated only when required, i.e., when Alice's signals pass through them [**Vakhitov2001**, **Gisin2006**].
- For CV-QKD transmitters: Monitoring for increased excess noise by Raman scattering [**Pan2020**] or crosstalk [**Ma2016**, **Pan2020**], depending on the wavelength of the attack.
- For two-way CV-QKD systems: tag frames inserted by the receiver and waveform detector at the sender to record time intervals between tag frames [**Ma2016**].
- Upper bounding the intensity of the back-reflected light and

Proposed Countermeasures	incorporating this information in the security proof. This was first done in **Lucamarini2015** against a THA targeting the phase modulator that encodes the BB84 signals. **Tamaki2016** extended this proof to a THA that targets both the phase modulator (encoding the BB84 signals) and the intensity modulator (encoding the decoy states) in a decoy-state BB84 protocol. Both works assume the asymptotic scenario, while the finite-key regime has been considered in **Wang2018b**, **Wang2020a** and **Navarrete2022**. None of these results assume anything about Eve's measurement, but require knowing the quantum state of the back-reflected light. This state is typically assumed to be a coherent state, proven to be optimal in certain scenarios [**Vinay2018**]. - An alternative providing intrinsic immunity against THAs is to employ passive transmitters that use a linear optics network combined with post-selection techniques (instead of optical modulators) to encode the quantum signals [**Curty2010**, **Curty2010b**]. Fully passive transmitter schemes for decoy-state BB84 protocol have been presented recently [**Zapatero2023**, **Wang2022**].
Remarks	Attacks on QKD transmitters with phase modulators may also be applicable (with suitable modifications) to QKD transmitters which use, for instance, polarisation modulators.
Feasibility $t_{Attack} < 1$ day	In case of DV-QKD, the working principles of the attack have been demonstrated in several experiments and simulations [**Vakhitov2001**, **Gisin2006**] and on commercially available systems [**GarciaEscartin2020**], and most recently, a photonic integrated chip based QKD transmitter [**Tan2021a**]. In case of CV-QKD, attacks have been performed on both commercially available and research-lab systems [**Stiller2015**, **Ma2016**]. Some versions of the attack have been theoretically proposed but not experimentally demonstrated.
Reference(s)	**Zbinden2000**, **Bethune2000**, **Vakhitov2001**, **Gisin2006**, **Curty2010**,**Curty2010b**, **Lucamarini2015**, **Jain2015**, **Stiller2015**, **Ma2016**, **Tamaki2016**, **Vinay2018**, **Wang2018b**, **GarciaEscartin2020**, **Pan2020**, **Wang2020a**, **Tan2021a**, **Navarrete2022**, **Wang2022**, **Zapatero2023**

Table 4.48: Trojan-horse attack against QKD transmitters

Name	Enabling light-injection attacks by application of external magnetic fields		
Category	Trojan-horse attack		
Component	Transmitter, receiver	**Subcomponent**	Optical isolator, circulator
Expertise	Laymen	**Opportunity**	Difficult
Attack Rating	Enhanced-Basic	**Attack Type**	Active
Protocol	Applicable to any QKD protocol that uses optical isolators and/or circulators for protection against injection of light.		
Target(s)	Enabling other attacks		
Short Description	Application of external magnetic fields on optical isolators or circulators used for protection against light-injection attacks can have a significant impact on the capabilities of these devices.		
Precondition Public information	The QKD device uses optical isolators and/or circulators that function based on the Faraday effect.		
Equipment Standard equipment	Device capable of applying a tuneable magnetic field. In **Tan2022**, a solenoid in combination with a DC power supply was used.		
Description	Optical components such as isolators and circulators that utilise the Faraday effect to achieve a desired functionality based on the rotation of optical polarisation are commonly used in QKD systems. For instance, a calibrated static magnetic field applied on a Faraday rotator followed by a PBS (see Section 2.4.4.3) can be used for greatly reducing the transmittance of light in one direction. This is the basic principle behind an optical isolator. Application of external magnetic fields can, however, disrupt the desired functionality, and lead the QKD system to behave abnormally. In experimental tests conducted by **Tan2022**, the isolation from an optical isolator was shown to be reduced by almost 60 dB while the directivity of a circulator was modified by almost 53 dB. The security analysis done by **Tan2022** also showed that the reduced isolation capabilities of the isolator lead to an increased risk of Trojan-horse attacks (see Table 4.48) and laser-seeding attacks, such as those described in Table 4.35 and Table 4.33.		
Proposed Countermeasures	- Employing magnetic shielding such as μ-metal and Supra-50. - If the shielding capabilities are limited, incorporating Hall elements to monitor the external magnetic field that sets off an alarm if a certain threshold is exceeded.		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	This attack has been shown to work in laboratories. It is expected to work on similar implementations.		
Reference(s)	**Tan2022**		

Table 4.49: Enabling light-injection attacks by application of external magnetic fields

Name	Hardware-software Trojans and covert channels		
Category	Classical side-channel attack		
Component	Transmitter, receiver	**Subcomponent**	Optical components, classical processing
Expertise	Laymen	**Opportunity**	Unlimited
Attack Rating	Moderate	**Attack Type**	Active
Protocol	Applicable to any QKD protocol, both based on discrete or continuous variables. For illustration purposes, the scientific literature has so far mainly considered DI-QKD, or decoy-state MDI-QKD as specific targets.		
Target(s)	Complete knowledge of the key		
Short Description	Insertion of malicious hardware and/or software within the QKD equipment to store and transmit information covertly that helps Eve gain knowledge of the key.		
Precondition Sensitive information	- Procured QKD equipment (hardware, firmware, software) can access, store, and covertly transmit information to Eve.		
Equipment Standard equipment	Sensors, memory modules, transmitters (hardware), malicious code (firmware/software).		
Description	In this attack, Eve places malicious hardware and/or software in the QKD equipment to store and covertly leak the key material produced during QKD sessions. Note that once a key has been generated, it is a classical object which is no longer protected by quantum mechanics. For instance, it can be copied without any penalty for Eve. These type of attacks are a known threat against virtually all cryptographic systems today. In the context of QKD, this type of attack was first considered in **Barrett2013** against device-independent QKD (DI-QKD). The authors outlined various strategies for a malicious memory and transmitter to compromise the security. For instance, the classical bits of the copied key could be hidden in the classical communication exchanged between Alice and Bob during the post-processing phase of future QKD sessions, or by making the protocol to abort at a certain time instant that depends on the key generated in a previous QKD session, thus revealing information about the latter. A more conservative scenario against both DI-QKD and device-dependent QKD was considered in **Curty2019**. This work assumes that the behaviour of malicious hardware/software can arbitrarily deviate from the prescriptions of the QKD protocol and it can communicate any received input information directly to Eve, even during the execution of a QKD session.		
Proposed Countermeasures	Main countermeasures include the following: - Use of redundant devices (for instance, purchased from different vendors) in combination with verifiable secret sharing and privacy amplification techniques [**Barrett2013**, **Curty2019**]. If Alice and		

Proposed Countermeasures	Bob share various pairs of QKD modules together with n classical post-processing units at their disposal, it has been shown in **Curty2019** that it is possible to generate a secure key given that at least one pair of the QKD modules and more than two thirds of each of the n classical post-processing units are honest. Indeed, it has been proven that the protocols introduced in **Curty2019** are essentially optimal with respect to the resulting secret key, whenever malicious devices can freely collaborate and communicate between them and with Eve. A proof-of-principle experiment implementing the ideas in **Curty2019** has been reported in **Li2021**. More recently, **Zapatero2021** considered various alternatives (and more restricted) adversary models, in which, e.g., malicious equipment cannot collaborate between them, or it cannot deviate from the prescriptions of the protocol but only leak information to Eve. - Encrypt the data interchanged between Alice and Bob during the post-processing phase of a QKD protocol to prevent Eve from hiding information [**Barrett2013**]. Possible drawbacks of this approach are, however, the significant consumption of secret keys for such an encryption, or that malicious devices might be able to covertly communicate information to Eve by different means anyway[18]. Other countermeasures introduced in **Barrett2013** suffer from similar drawbacks and are ineffective against general adversaries, as reported in that work. - Use of classical countermeasures against malicious software, like e.g. patch and update the software, and use firewalls and security software, such as antimalware and antivirus inter alia.
Remarks	Hiding malicious devices within optical components of a QKD setup might be possible as well, though no results have been reported in the scientific literature.
Feasibility $t_{Attack} < 1$ day	This attack has not been demonstrated experimentally against a QKD setup, but similar attacks have been successfully launched against classical cryptosystems.
Reference(s)	**Barrett2013**, **Curty2019**, **Li2021**, **Zapatero2021**

Table 4.50: Hardware-software Trojans and covert channels

[18] In addition, this countermeasure is also not effective in cryptographic environments involving communication with multiple users who may not all be trustworthy.

Name	Cache side channels in the post-processing of QKD systems		
Category	Classical side-channel attack		
Component	Postprocessing	**Subcomponent**	Privacy amplification, error correction
Expertise	Laymen	**Opportunity**	Unlimited
Attack Rating	Moderate	**Attack Type**	Passive
Protocol	The scientific literature has studied this attack on the BB84 protocol.		
Target(s)	Complete knowledge of the key		
Short Description	Exploiting software cache accesses to get knowledge about the key by observing cache hits and misses.		
Precondition Public information	The QKD system has to use the optimised low-density parity check (LDPC) technique where multiplications with zero are skipped.		
Equipment Standard equipment	Equipment to observe cache traces.		
Description	Secret information is stored in memory entries in the cache during post-processing. An eavesdropper can exploit the cache hits and misses accessed by the software to gain knowledge of the key. A cache hit occurs if the CPU accesses an entry that is stored in the cache, and a cache miss occurs if an entry is accessed, which is not stored in the cache. In **Nikiforov2018**, four attack strategies on the software implementation of privacy amplification are analysed using the tool CacheAudit 0.2c, which gives bounds on the vulnerability of the software. In the attack models, the attacker can observe: 1) the time taken for cache hits and misses during a run of privacy amplification, 2) the trace for cache hits and misses during a run of privacy amplification, 3) the amount of memory entries in the cache after a run of privacy amplification, 4) the contents of the cache after a run of privacy amplification. The analysis suggests that no secret information about the secret key is leaked to attackers. **Weber2021** extended the analysis to x86 binaries with floating point instructions on a system using the LDPC technique. A vulnerability in the error-correction step concerning an optimisation of the LDPC (skip of multiplications with zero) is discovered. The eavesdropper is able to recover the entire secret key from one cache trace, e.g., based on CPU performance counters.		
Proposed Countermeasures	In **Weber2021**, a mitigation strategy of the described vulnerability is presented. It consists of program rewriting such that memory accesses are independent of the sifted key.		
Remarks	-		
Feasibility $t_{Attack} < 1$ day	This attack has not yet been demonstrated on a practical QKD system.		

Reference(s)	**Nikiforov2018**, **Weber2021**

Table 4.51: Cache side channels in the post-processing of QKD systems

Name	Single-trace side-channel attack on information reconciliation in QKD		
Category	Classical side-channel attack		
Component	Postprocessing	**Subcomponent**	Information reconciliation
Expertise	Proficient	**Opportunity**	Difficult
Attack Rating	High	**Attack Type**	Passive
Protocol	Possibly applicable to any QKD protocol.		
Target(s)	Complete knowledge of the key		
Short Description	Measuring and exploiting the power consumption during information reconciliation to learn information about the sifted key.		
Precondition Public information	- Use of a LDPC matrix for the information reconciliation process [**Park2020**, **Park2021**]. - Use of parity sums for information reconciliation [**Kim2021**].		
Equipment Specialised equipment	Oscilloscope that measures the power consumption of the targeted post-processing board.		
Description	A single-trace attack against the information reconciliation process of a QKD system that exploits the power consumption difference associated with storing different bit values by the information reconciliation algorithm. In **Park2020** and **Park2021**, the QKD studied system uses an information reconciliation step based on a binary LDPC matrix. Eve attacks the system when Alice computes the syndrome of the LDPC code for Bob's error correction. Two specific attack targets, namely the XOR operation and the modulo-2 operation employed during the syndrome computation, are exploited depending on the error-correction algorithm used. **Kim2021** generalises this approach to all information reconciliation processes based on the parity sum algorithm, which includes Cascade, Winnow, and LDPC. Experimental results show that this type of attack can provide Eve with complete information about the key. **Kim2021** also evaluates the effect of the signal-to-noise ratio of the measured traces on the attack success.		
Proposed Countermeasures	Proposed countermeasures can be very specific to certain steps in the information reconciliation algorithm. They include: - Randomising the order of the syndrome bit computation and keeping this randomisation secret. While this compromises Eve's attack strategy, the order does not affect the final output between Alice and Bob [**Park2021**, **Kim2021**]. - Randomly inserting dummy operations before, during, and after the algorithm's execution [**Kim2021**]. - Using a secret permutation rule [**Kim2021**].		
Remarks	Power analysis is also a threat against classical cryptosystems and countermeasures there can be applied here as well.		

Feasibility $t_{Attack} < 1$ day	The presented attacks on the information reconciliation process have been experimentally demonstrated in **Park2020**, **Park2021**, and **Kim2021**.
Reference(s)	**Park2020**, **Park2021**, **Kim2021**

Table 4.52: Single-trace side-channel attack on information reconciliation in QKD

4.4 Additional Vulnerabilities

In this section, tables for vulnerabilities, i.e., side channels for which no clear attack paths can be identified with the current state of research and equipment, are described. It should be noted that attack ratings shall not be provided here; for further details, see Chapter 3.

Number	Vulnerability Table Name
Table 4.54	Imperfect Gaussian modulation
Table 4.55	Imbalance in dual quadrature detection
Table 4.56	Imperfect phase randomisation of laser diodes in QKD
Table 4.57	Phase-derandomisation and intensity-manipulation
Table 4.58	Information leakage due to use of Faraday mirror
Table 4.59	Information leakage via laser source side channels in QKD
Table 4.60	Pulse correlations due to imperfect modulation
Table 4.61	Side channels in random bit generation with multiple lasers
Table 4.62	Violation of Bell's inequality by blinding passively-quenched APDs

Table 4.53: List of vulnerability tables

Vulnerability	Imperfect Gaussian modulation		
Component	Transmitter, postprocessing	**Subcomponent**	Modulation system
Protocol	Applicable to the GMCS protocol.		
Short Description	Exploiting finite resolution and range of devices involved in the modulation to obtain unwanted a priori knowledge of the prepared quantum states.		
Precondition	Finite resolution and range of devices involved in generation of modulated signals.		
Description	Section 2.3.2.1 describes Gaussian modulation together with its limitations. To elaborate upon the latter, it is impossible in practice to implement continuous Gaussian modulation due to finite resolution and range of quantum random number generators (QRNGs), digital-to-analog-converters (DACs) and processing software. Furthermore, the optical modulators themselves have a limited range. All these deviations from the ideal protocol might give an attacker a priori knowledge of the sent quantum states [**Jouguet2012**].		
Proposed Countermeasures	- Quantify deviations in the approximate Gaussian modulation and incorporate them in security proofs. - Using true discrete modulation (see Section 2.3.2.1).		
Remarks	An attacker needs to be able to distinguish the imperfect sent state from a thermal state, which is feasible.		
Reference(s)	**Jouguet2012**		

Table 4.54: Imperfect Gaussian modulation

Vulnerability	Imbalance in dual quadrature detection		
Component	Receiver	**Subcomponent**	Balanced homodyne detector, beamsplitter
Protocol	Applicable to any CV-QKD protocol implementation using two homodyne detectors for dual quadrature measurements.		
Short Description	Assumption of identical quantum efficiencies (which may not be the case in practice) leading to an underestimation of excess noise.		
Precondition	Bob implements a dual quadrature measurement using two balanced homodyne detectors (with four photodiodes that do not exhibit identical quantum efficiencies).		
Description	No two optical components are perfectly identical. In case of photodiodes used in the construction of a heterodyne detector[19], a mismatch in the quantum efficiencies of the photodiodes can therefore be expected. If accounted for properly, Bob should observe an increased excess noise, for instance, due to the poor relative intensity noise (RIN) cancellation. However, if Bob assumes no imbalance in his coherent receiver configuration, this vulnerability is manifested, and Eve could use the corresponding margin (of the excess noise) to launch some attack during the execution of the QKD protocol and gain more knowledge of the key than what Alice and Bob eventually estimate [**Kong2022**]. Apart from the non-identical quantum efficiencies of the (four) photodiodes of the two balanced homodyne detectors (see Section 2.4.2.1), imbalance can also occur due to non-symmetric beamsplitters (see Section 2.4.4.1). In **Kong2022**, the authors absorb the deviation from the 50:50 splitting ratio of the beamsplitter into the mismatch of the quantum efficiencies.		
Proposed Countermeasures	Using VOAs for detector balancing [**Kong2022**].		
Remarks	From an experimental perspective, detector balancing is a basic prerequisite to getting a functional CV-QKD receiver. It is thus unlikely that a CV-QKD protocol would be executed before balancing the detectors. However, a mismatch could be forced, for instance, using the wavelength-dependent properties of the components, as shown in Table 4.39.		
Reference(s)	**Kong2022**		

Table 4.55: Imbalance in dual quadrature detection

[19] A phase-diverse receiver is the correct term for what is often called "heterodyne detector" in CV-QKD papers.

Vulnerability	Imperfect phase randomisation of laser diodes in QKD
Component	Transmitter **Subcomponent** Laser diode
Protocol	The scientific literature presented here has shown the proposed vulnerability in BB84 and BB84 with decoy states protocols.
Short Description	Exploiting phase correlations due to imperfect phase randomisation in gain-switched laser diodes.
Precondition	Use of gain-switched laser diodes under conditions inducing phase correlations between consecutive pulses.
Description	Consecutive pulses of a gain-switched laser diode can exhibit phase correlations. If there is some residual excitation left in the resonator in the pulse interval until the next excitation, the lasing can be seeded by the remaining photons, thus relating the phases of the two consecutive pulses as the stimulated emission conserves the phase as shown by **Kobayashi2014**. The assumption of phase randomisation between pulses is not fulfilled in this case. An asymmetric Mach-Zehnder interferometer is used to observe the interference visibility of a 10 GHz clocked laser diode and quantify the information leakage. In **Gruenenfelder2020** this has been done for a 5 GHz clocked source. The phase correlation will increase the information leakage and thus reduce the secure key rate. They show that phase correlations increase the probability of Eve discriminating the signal state from the decoy state for partially coherent states.
Proposed Countermeasures	Several countermeasures are proposed in the scientific literature: - The laser diode should be reversely biased at the bottom of the pulses [**Kobayashi2014**]. - The effective photon lifetime should be less than the turn-off duration [**Kobayashi2014**]. - Incorporate the effect of non-perfect phase randomisation in the security proof of QKD. Indeed, in the security proof presented in **CurrasLorenzo2022** for a decoy-state BB84 protocol with laser sources it is shown that correlations between the global phases of adjacent pulses present in state-of-the-art setups **Gruenenfelder2020** seem to have a quite limited impact on the achievable performance, and the resulting secret key rates are close to those of the ideals scenario without phase correlations. The results of **Kobayashi2014** indicate that for 10 GHz pulse repetition rate and small minimum drive currents, the phases of pulses are still random. Furthermore, **Gruenenfelder2020** concluded that for their 5 GHz QKD system the effects due to phase correlations are negligible.
Remarks	The vulnerability should also impact other protocols if they use laser sources in the described conditions.
Reference(s)	**Kobayashi2014**, **Gruenenfelder2020**, **CurrasLorenzo2022**

Table 4.56: Imperfect phase randomisation of laser diodes in QKD

Vulnerability	Phase-derandomisation and intensity-manipulation		
Component	Transmitter	**Subcomponent**	Laser diode
Protocol	Applicable to any QKD protocol that uses laser sources.		
Short Description	Eve injects light into Alice's laser source to modify the intensity and/or global phase of Alice's generated laser pulses.		
Precondition	Use of a pulsed laser source by Alice to generate the quantum states.		
Description	Eve injects external light into Alice's laser diode to change the intensity and global phase of the light pulses emitted by the latter, thus violating some assumptions of QKD security proofs. Indeed, if external photons are injected into a laser cavity, these photons will also be amplified to generate laser pulses. If such injected photons greatly outnumber the initial photons that arise from spontaneous emission, the phase of the generated laser pulse is largely determined by the phase of the injected photons, and its intensity also increases. It was first introduced in **Sun2015a** where the authors confirmed experimentally that Eve can control the phase of Alice's emitted pulses by injecting light from a CW laser. Once the global phase of Alice's pulses has been derandomised, Eve could launch various attacks to exploit this vulnerability, see, e.g., the partially-random-phase attack in **Sun2012** and the source attack of decoy-state QKD using phase information in **Tang2013a**. The fact that the injection of external light from Eve also increases the intensity of Alice's pulses, has been experimentally demonstrated in **Huang2019**. There, the authors explicitly showed, for the decoy-state BB84 and MDI-QKD protocols, that a direct application of a security proof (which does not consider the intensity changes produced by Eve) would overestimate the secret key rate even beyond well-known upper bounds, thus delivering a key that is actually insecure. In any case, once the intensity of Alice's signals has been increased, Eve must launch a tailored attack able to exploit this vulnerability to learn information about the key.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this vulnerability. These include: - Using optical isolation (**C1**), watchdog detectors (**C2**), and spectral filtering (**C4**). - Monitoring the health of implemented countermeasures (**C3**). - Active randomisation of the phase of the emitted pulses(**C6**), which requires care with the timing of such randomisation. - Incorporate the imperfection in security proof (**C5**), namely, the fact that Eve can partially control the phase and intensity of the emitted pulses. A security proof, valid when the value of the global phase is known, has been provided in **Lo2007**; the case where the global phase follows an arbitrary continuous distribution has been recently addressed in **CurrasLorenzo2022**.		

Proposed Countermeasures	Also, Alice and Bob can treat the fact that Eve can modify the intensity of Alice's pulses by using the techniques in **Wang2008**, **Zhao2008a**, **Zhao2010** or **Hu2010**.
Remarks	This vulnerability might be effective against CV-QKD systems as well. Wavelength filters may be ineffective countermeasures from a practical point of view because the wavelength of Eve's control laser is typically very close to that of Alice's laser.
Reference(s)	**Lo2007**, **Wang2008**, **Zhao2008a**, **Hu2010**, **Zhao2010**, **Sun2012**, **Tang2013a**, **Sun2015a**, **Huang2019**, **CurrasLorenzo2022**

Table 4.57: Phase-derandomisation and intensity-manipulation

Vulnerability	Information leakage due to use of Faraday mirror		
Component	Transmitter	**Subcomponent**	Phase modulator
Protocol	Applicable to the MDI-QKD, three-state, and BB84 protocol.		
Short Description	Exploiting correlations between leakage light and signal state encoding due to the use of a FM.		
Precondition	Use of a FM for stabilising state preparation and leakage light due to imperfect pulse generation.		
Description	Weak optical radiation leaked in between pulses (due to e.g., finite extinction of the intensity modulator) can get unintentionally modulated in a time-dependent manner. This opens up a passive security loophole which can be exploited by an eavesdropper. In **Bourassa2021**, a polarisation-based MDI-QKD setup using a FM for stable electro-optic bit modulation is used as a representative case example of such a side channel. Optical pulses first travel through the PM, experiencing voltage and unintentional temperature-induced phase modulation, encoding bit and basis information in polarisation. Upon reflection at the FM, the optical pulses return through the PM, where they encounter only temperature-induced phase modulation, and no voltage pulse is applied. As optical pulses are derived from continuous wave light using intensity modulation, this unavoidably leads to weak light leakage due to the finite extinction ratio in-between the signal pulses. No voltage is applied to the phase modulator as the leakage light travels through it the first time, but it inevitably could collide with a voltage pulse counter-propagating in the PM going through it the second time. This interaction modulates the polarisation of the leakage light and correlates it with the polarisation encoding of the signal states. It has been observed that the modulation of the leakage light is time-dependent since it travels counter to the voltage pulse direction. Additionally, it relies on the shape of the voltage pulse utilised for phase modulation and the length of the PM's electrode.		
Proposed Countermeasures	In **Bourassa2021**, a numerical security proof technique based on semi-definite programming is used to quantify the effect of the presented side channel on the secret key rate. They showed that accounting for the side channel using this technique instead of overestimating the information leakage due to rudimentary models provides a benefit to the key rate. For this, a careful characterisation of the side channel has to be done. Analysis showed that the three-state protocol gives less secret key as BB84 in the presence of source side channels. Further countermeasures are: - Use all detection statistics, and all initial state information for key calculation, rather than discarding cases when their basis choices do not match. - Modify the polarisation angle of the sent states to boost key rate. - Minimise the intensity of the leakage light by hardware solutions.		

Remarks	-
Reference(s)	**Bourassa2021**

Table 4.58: Information leakage due to use of Faraday mirror

Vulnerability	Information leakage via laser source side channels in QKD		
Component	Transmitter	**Subcomponent**	Laser diode
Protocol	Applicable to QKD protocols that use a laser source. BB84 with decoy states is mentioned in **Nauerth2009**.		
Short Description	Exploiting laser source side channels in various DOFs to compromise QKD system security.		
Precondition	Distinguishability of the quantum states in non-encoding DOFs.		
Description	In free-space BB84 QKD systems, several DOF side channels can compromise the system's security. Spatial, spectral, and temporal DOFs are non-operational in polarisation-encoded systems and can therefore lead to information leakage to an eavesdropper. These side channels result from the use of several laser diodes, which are not perfectly indistinguishable. In **Nauerth2009**, these side channels are analysed in a decoy-state BB84 QKD setup and quantified in terms of mutual information. The setup uses eight distinct laser diodes to prepare the four different signal states and four different decoy states. An eavesdropper can exploit correlations of these DOFs with the encoding of the quantum states for the different laser diodes without introducing additional errors. The higher the correlations, the more distinguishable are the quantum states. **Biswas2021** used the cross-correlation function to characterise and quantify the distinguishability in the spectrum, pulse width, time of arrival, and spatial mode. In **Sagar2022**, these spatial, spectral, and temporal DOF side channels including intensity correlations have been quantified and successfully mitigated in the case of a transmitter module in a nanosatellite.		
Proposed Countermeasures	Both general and specific (to the DOF) countermeasures are proposed: - Using single-mode fibres to cancel out spatial information [**Nauerth2009**]. - Using diffraction-limited pinhole to decrease spatial mode mismatch [**Sagar2022**]. - Using spectral filtering and temperature-stabilised diodes [**Nauerth2009**, **Biswas2021**, **Sagar2022**]. - Using shorter gate windows, faster timing circuits, or digitally programmable delay lines to adjust the temporal delays of the different laser diodes [**Nauerth2009**, **Sagar2022**, **Biswas2021**]. - Reducing repetition rate to mitigate pulse correlations [**Sagar2022**]. - Using a common laser driver circuit for all laser diodes to equalise pulse widths and intensities [**Biswas2021**, **Sagar2022**].		
Remarks	-		
Reference(s)	**Nauerth2009**, **Biswas2021**, **Sagar2022**		

Table 4.59: Information leakage via laser source side channels in QKD

Vulnerability	Pulse correlations due to imperfect modulation		
Component	Transmitter	**Subcomponent**	Optical modulator
Protocol	Applicable to any QKD protocol. So far, the scientific literature has mainly considered the BB84 protocol (with and without decoy states), and the three-state protocol.		
Short Description	Existence of pulse correlations between subsequent pulses due to memory effects in practical optical modulators and/or in the electronics that control them.		
Precondition	Use of optical modulators (e.g., intensity, polarisation and/or phase modulators) to encode the state of Alice's emitted quantum signals.		
Description	Most security proofs of QKD assume that Alice's generated signals are independent and identically distributed. However, practical imperfections in QKD implementations can create classical correlations between these signals, thus invalidating a crucial assumption of the security proofs. Setting-independent pulse correlations refer to those correlations that do not depend on Alice's previous setting choices to encode her signals, but are produced by setting-choice-independent factors such as temperature drifts or power fluctuations [**Nagamatsu2016**, **Mizutani2018**, **Pereira2022**]. Setting-dependent pulse correlations, on the other hand, refer to the scenario in which the state of each emitted pulse by Alice depends not only on the actual modulation setting selected by her but also on her previous modulation setting choices, meaning that the secret key information, i.e. the bit, basis and intensity choices, is encoded not only into a single pulse but also between subsequent pulses. This later type of correlations is typically produced by memory effects in the optical modulators and/or electronics that control them, mainly because practical devices are band-limited. Setting-dependent pulse correlations arising from the intensity modulator have been studied in **Yoshino2018**, **Gruenenfelder2020** and **Zapatero2021**, while those arising from phase and/or polarisation modulators have been considered in **Pereira2020**, **Pereira2022**, **Gruenenfelder2020** and **CurrasLorenzo2023**.		
Proposed Countermeasures	Main countermeasures include the following: - Incorporate the effect of pulse correlations in the security proof of QKD. Security proofs for setting-independent pulse correlations have been proposed in **Nagamatsu2016**, **Mizutani2018** and **Pereira2022**. Likewise, security proofs for setting-dependent pulse correlations arising from phase and/or polarisation modulators encoding the bit and basis information have been put forwarded in **Pereira2020**, **Pereira2022** and **CurrasLorenzo2023**, while those arising from the intensity modulator that encodes the decoy intensity settings have been considered in **Yoshino2018** and **Zapatero2021**. The work in **Yoshino2018** is restricted to nearest neighbour pulse correlations, while those in **Pereira2020**, **Zapatero2021**, **Pereira2022** and **CurrasLorenzo2023** can handle arbitrary correlation lengths.		

Proposed Countermeasures	- Initialise the modulation device each time after Alice emits a pulse. This could be done by always sending one or multiple pulses with fixed encoding settings in between the actual signal pulses [**Yoshino2018**, **Mizutani2018**]. - Reduce the clock rate of the QKD system to eliminate possible memory effects in the optical modulators, or use multiple optical modulators (each of them encoding different subsets of signals). For instance, in the case of nearest neighbour pulse correlations one could use one modulator to encode the even pulses and another one to encode the odd pulses [**Pereira2020**]. - In **Roberts2018**, a Sagnac interferometer-based intensity modulator is presented, mitigating the intensity correlation and fluctuation side channels. It was shown that a Sagnac intensity modulator has no temporal drift, meaning feedback mechanisms are not required, thus dramatically simplifying the implementation. - Replace the intensity modulator with an IQ modulator allows to mitigate the pattern effect due to intensity correlations in decoy-state QKD setups [**Gao2023**].
Remarks	In those QKD setups that use an external phase modulator to achieve global phase-randomisation of the emitted pulses, correlations between such global phases that may be introduced by the modulator are not covered by current security proofs. For the alternative scenario in which global phase-randomisation is achieved by driving the laser source under gain switching conditions see table 4.56.
Reference(s)	**Nagamatsu2016**, **Roberts2018**, **Mizutani2018**, **Yoshino2018**, **Pereira2020**, **Gruenenfelder2020**, **Zapatero2021**, **Pereira2022**, **CurrasLorenzo2023**, **Gao2023**

Table 4.60: Pulse correlations due to imperfect modulation

Vulnerability	Side channels in random bit generation with multiple lasers		
Component	Transmitter	**Subcomponent**	Laser diode
Protocol	Applicable to BB84.		
Short Description	Exploiting intensity correlations arising from aperiodic pulse generation due to random bit generation with multiple lasers.		
Precondition	Use of multiple laser diodes for random bit generation.		
Description	In **Ko2017**, laser side channels in a BB84 QKD system, where four polarisation states are produced by four different laser diodes, are analysed. Every laser diode is randomly switched on and off to generate random bit information. As in semiconductor laser diodes, the level of driving current and initial carrier density determine the intensity and the emission time of the pulse, aperiodic pulse generation leads to distinguishability of the pulses. This is a result of the remaining carrier density in case the intervals between pulses are short and lead to temporal disparity and intensity fluctuation among output pulses. Eve can exploit these correlations to get knowledge about the encoding of consecutive pulses with higher probability.		
Proposed Countermeasures	The proposed countermeasures against the analysed side channels mainly relate to finding suitable values for the DC bias conditions under certain clock speeds. One general but mostly undesirable countermeasure is to reduce the system clock frequency so that the minimum time interval between two pulses is much longer than the carrier lifetime [**Ko2017**]. Results from **Ko2017** show that increasing DC bias levels leads to diminishing temporal disparity and intensity fluctuations. However, this leads to background photons caused by spontaneous emission, increasing the QBER. The effects of the increase in QBER on the secure key rate due to mitigating strategies have been investigated in **Ko2017a**. In **Ko2017a**, some countermeasures tackling the increased QBER are proposed, these are: - Temporal filtering technique to remove unwanted photon detections. - Ultra-sharp spectral bandpass filters to filter out spontaneously emitted photons, as they have a broader spectrum than signal pulses. - Reducing system jitter to reduce QBER.		
Remarks	-		
Reference(s)	**Ko2017**, **Ko2017a**		

Table 4.61: Side channels in random bit generation with multiple lasers

Vulnerability	Violation of Bell's inequality by blinding passively-quenched APDs		
Component	Receiver	**Subcomponent**	APD
Protocol	Applicable to protocols that are based on polarisation or energy-time entanglement, like Ekert91, as well as device-independent protocols.		
Short Description	The violation of Bell's inequality is demonstrated using faked states to control the detectors.		
Precondition	- Passively-quenched APDs. - More than one APD.		
Description	The authors use the faked-state method (see Section 2.5.2.1) to control the APD-based single-photon detectors of the two receiver units to fake the violation of a Bell inequality that is supposed to witness the presence of polarisation [**Gerhardt2011a**] or energy-time (also called Franson-type) [**Jogenfors2015**] entanglement. While these were no attacks on a QKD protocol, the violation of a Bell inequality can be a vital part of a QKD protocol. Blinding mechanisms similar to **Gerhardt2011** (see Table 4.12) and **Lydersen2010a** (see Table 4.13), respectively, were employed to artificially generate the correlations leading to the violation of a Clauser-Horne-Shimony-Holt (CHSH) inequality.		
Proposed Countermeasures	Several of the general countermeasures mentioned in Section 4.5 can possibly prevent this vulnerability. These include: - Monitoring the electrical parameters (**C10)** and photocurrents (**C11)** of the APDs. - Using the technique of bit-mapped gating (**C12)** and monitoring the sensitivity of the single-photon detector (**C13)**. In addition, some specific countermeasures have been considered for the energy-time entanglement [**Jogenfors2015**]: - Fast-switching interferometers. - "Hugging" interferometers to avoid the post-selection loophole. - Stronger Bell inequalities like modified Pearle-Braunstein-Caves inequalities.		
Remarks	-		
Reference(s)	**Lydersen2010a**, **Gerhardt2011**, **Gerhardt2011a**, **Jogenfors2015**		

Table 4.62: Violation of Bell's inequality by blinding passively-quenched APDs

4.5 General Countermeasures

In the scientific literature, some of the measures proposed to protect specific QKD systems and/or QKD protocols from having their security broken by an attack on the implementation sometimes tend to work as a countermeasure to several other attacks, or even a class of attacks. In Section 2.6, two of the most well known of these measures have been explained in detail.

In this section, a list of general countermeasures (briefly referenced in one or more of the attack tables presented in the previous sections of this chapter) is compiled and presented. In some cases, it would be observed that there have been claims and even counterclaims stating that the proposed measures (do not) actually work. Efforts have been made to communicate the whole thread: As a reminder, the reader is referred to the disclaimer presented at the beginning of Chapter 4 that is applicable to all the countermeasures discussed in this document, including those below.

(C1) Employ optical isolation to guarantee that the intensity of the input (and/or, back-reflected light, if relevant) is sufficiently weak. Ideally, such an optical isolation mechanism should be able to either withstand high-power incoming light while attenuating it to a sufficiently weak level or attain a permanent high-attenuation state, i.e., effectivly breaking up the line and blocking the opical path. For this, one may combine devices like isolators (except in two-way configurations like plug-and-play), attenuators, circulators, and wavelength filters [**Bethune2000**, **Vakhitov2001**, **Gisin2006**, **Jain2015**, **Lucamarini2015**, **Ko2016**, **Vinay2018**, **Molotkov2020**, **Ponosova2022**, **Tan2022**, **Nasedkin2022**], passive optical power limiter [**Bugge2014**, **Makarov2016**], or deploy an optical fuse [**Gisin2006**, **Makarov2016**, **Vinay2018**, **Zhang2021**, **Peng2023**].

(C2) Use watchdog detectors (see Section 2.4.2.2) to monitor the input optical intensity [**Zbinden2000**, **Bethune2000**, **Vakhitov2001**, **Gisin2006**, **Jain2015**, **Ko2016**, **Qin2016**, **Dixon2017**, **Molotkov2020**]. However, deployment flaws in such watchdog detectors, as shown in **Sajeed2015**, could leave the QKD device unprotected. Investigating these flaws may in fact require several iterations and involve modifications to various parts, e.g., the front-end amplifier, the integrator, etc. of the electronic circuits.

(C3) Continuously monitor the functionality of the implemented measures as Eve could perform a laser damage attack to modify the functionality of the components, e.g., reduce the actual optical isolation [**Huang2020**] or defeat the monitors/watchdog detectors [**Bugge2014**].

(C4) Using optical filters to ensure that only the desired signal wavelength(s) enter/exit the QKD device [**Gisin2006**, **Jain2015**, **Lucamarini2015**, **Ponosova2022**]

(C5) Incorporate the effect of device imperfections in the security proof, ideally after minimising the imperfections, e.g. by employing some countermeasures. Below is a(n incomplete) list pairing the imperfection and corresponding security proofs that tackle it:

- State preparation flaws [**Gottesman2004**, **Tamaki2014**, **Pereira2020**, **Sun2021**, **Pereira2022**, **Metger2022**, **CurrasLorenzo2023**].
- Imperfect phase randomisation [**Lo2007**, **Zhao2007**, **Cao2015**, **CurrasLorenzo2022**, **Sixto2023**].
- Presence of correlations across multiple signals [**Pereira2020**, **Zapatero2021a**, **CurrasLorenzo2022**, **CurrasLorenzo2023**].
- Information leakage due to, e.g., Trojan-horse attacks or other passive mechanisms [**Gottesman2004**, **Lucamarini2015**, **Tamaki2016**, **Wang2020a**, **Sun2021**, **Navarrete2022**, **CurrasLorenzo2023**].
- Emission of multimode signals that encode information in undesired modes [**Gottesman2004**, **Pereira2020**, **Sun2021**, **Metger2022**, **CurrasLorenzo2023**].
- Detection efficiency mismatch [**Fung2009**, **Maroey2017**, **Bochkov2019**, **Sun2021**, **Zhang2021a**, **Trushechkin2022**].
- Presence of malicious devices [**Curty2019**, **Zapatero2021**].

(C6) Actively randomise the phase of each emitted signal [**Gisin2006**, **Lucamarini2015**, **Tamaki2016**].

(C7) Monitor the state preparation process in Alice to ensure that the various degrees of freedom, e.g., time, wavelength, polarisation (using, e.g., wavelength filters, polarisers inter alia) are as expected or obey a certain tolerance.

(C8) QKD schemes using so-called intra-particle entanglement have been theoretically shown to be immune to some side-channel attacks on state preparation [**Adhikari2015**]. However, practical implementations of such schemes are beyond the technical resources available today.

(C9) Detector-control attacks are of no use against QKD implementations that use protocols from the MDI [**Lo2012**, **Pirandola2015**], twin-field (TF) [**Lucamarini2018**] and its variants [**Curty2019a**, **Wang2018c**, **Xu2020a**], or the RDI [**AlDarwbi2022**, **Ioannou2022**] family of QKD protocols, as they are fundamentally immune against all attacks that exploit imperfections in the QKD receiver. Some other protocols, such as the virtual protocol [**Braunstein2012**], or the prepare and measure Bell test protocol [**Tan2016**] do not strictly fall into one of the aforementioned categories, but might also be applicable. Two-way deterministic QKD [**Lu2013**] has also been shown to be immune to receiver attacks on Bob's but not yet Alice's side. We note that with the exception of MDI-QKD and TF-QKD protocols, practical implementations of all other schemes mentioned here are beyond the technical resources available today.

(C10) Monitoring the electrical parameters (bias voltage, current) of the APD [**Xu2006**, **Makarov2009**, **Lydersen2010c**, **Yuan2010**, **Gerhardt2011**, **Weier2011**, **Silva2012**]. In **Gerhardt2011**, the authors also suggest to monitor the thermal parameters of the APDs. However, in **Lydersen2010c** it is shown that thermal blinding might not change the outer temperature of the APD cooling mechanism, so this countermeasure may not be impenetrable.

(C11) Monitoring the APD photocurrent is proposed in **Yuan2011** to detect "anomalously high values", which is however disputed by **Lydersen2011c**, for instance, in connection with **Lydersen2011b**. This has again been countered by **Yuan2011a**, strengthening their claim that monitoring the photocurrent is an effective countermeasure. But **Wu2020** counterclaims that their "pulse illumination attack" might not be picked up by monitoring the photocurrent.

(C12) Bit-mapped gating [**Lydersen2011d**]: The bit-mapping of detection events[20] is changed in a random fashion optically and in software, so that they only coincide within a narrowed gate window. Various detector-control attacks get revealed under bit-mapped gating as all detection events outside the central part of the detector gate result in high QBER.

(C13) Active checking of the single-photon detector sensitivity [**Lydersen2011d**, **Maroey2017**, **Shen2022**] with a suitable light source inside the QKD receiver module.

(C14) Statistical analysis of the detection rates [**Silva2012**, **Lee2016**, **Molotkov2019a**, **Gaidash2022**] can be used to prevent blinding attacks and in the case of **Silva2012** even timing-related attacks. The viability and security, though, depends on the concrete detector characteristics and must be verified individually. The authors in **Balygin2018** even propose that phase coding QKD systems can be inherently secure against detector blinding attacks by incorporating additional postprocessing. However, the effectiveness of this countermeasures is questioned [**Fedorov2019**] and its use is therefore not recommended without further investigation.

(C15) Randomly changing the detection efficiency of the APDs to take two or more values and comparing the expected efficiencies with the measured ones [**Legre2012**, **Lim2014a**] has been proposed, but found to be not sufficient [**Huang2016**]. A similar countermeasure,

[20] Implies if a detector clicks, does that provide the bit "0" or the bit "1"?

additionally comparing the respective QBER is described in **Qian2019** and **Qian2020**, but also found to be based on assumptions that might not hold in reality [**Wu2020b**]. That in turn is disputed by the authors of the original paper [**He2020**].

(**C16**) **Wang2020** explores the possibility of applying temporal ghost imaging for detecting any temporal changes on the quantum signal, which could be used to thwart time-shift and detector-blinding attacks.

(**C17**) An interleaved sequence of decoy states along with an active bases choice on the receiver produces a characteristic detection distribution on the receiver side, which can be used to detect timing and blinding attacks [**Lizama2012**].

(**C18**) Using an upconversion[21] protected QKD receiver [**Jain2016**] that is able to restrict Eve's injection from the channel in DOFs such as wavelength, time, power, etc. The design and implementation of such a QKD receiver imparts it certain features that prevent detector-control attacks, wavelength-dependent manipulation attacks, Trojan-horse attacks, and laser-damage attacks.

[21] Upconversion, or more generally, quantum frequency conversion, is a nonlinear technique in which the wavelength of the signal is changed (while however preserving all other signal properties).

5 Summary and Conclusion

In the previous chapter, a comprehensive overview of implementation attacks on QKD has been provided through a series of tables, which were prepared by perusing well over 300 scientific articles. The data collected and organised in these tables facilitate both a qualitative and quantitative analysis of different attacks and vulnerabilities. In this chapter, some statistical results and findings based on this data are summarised and discussed, and wherever relevant, suitable conclusions and outlook are also added.

As depicted in the pie chart on the left in Figure 5.1, a total of 49 attack paths presented in Sections 4.1 (35 on DV), 4.2 (9 on CV) and 4.3 (5 on both DV and CV) and 9 vulnerabilities from Section 4.4 have been identified. A total of 18 countermeasures, which have been presented in Section 4.5, are found to be sufficiently general in nature to cater to multiple attacks. It needs to be emphasized that each of the attack tables also list specific countermeasures that can range from few to several in addition to these general countermeasures.

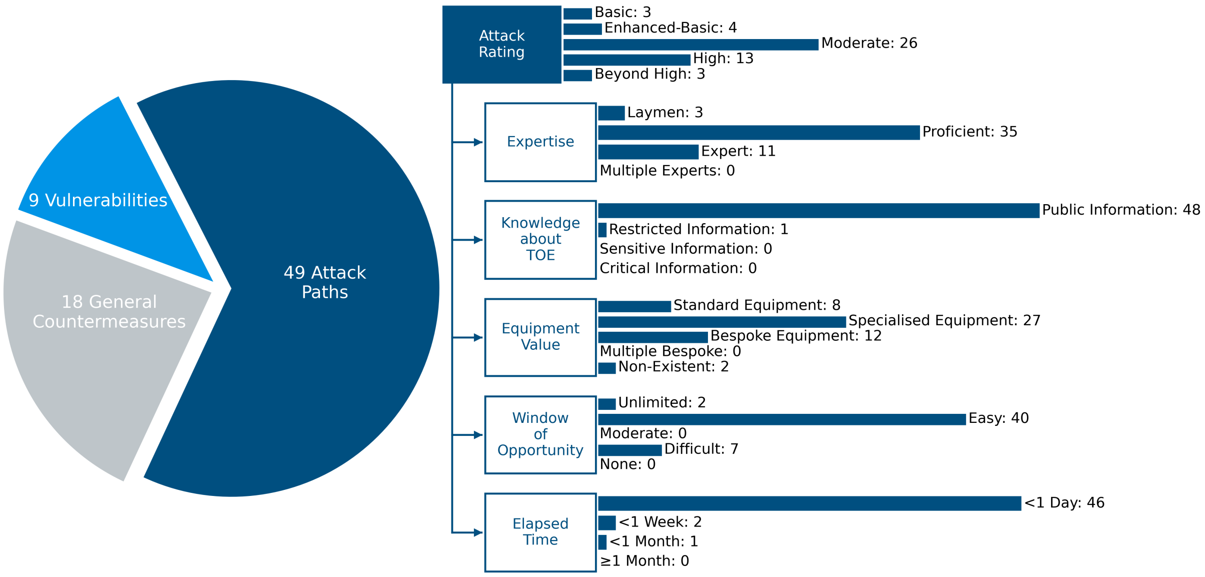

Figure 5.1: Statistical overview of implementation attacks on QKD systems. (Left): Pie chart shows the distribution of identified attacks, vulnerabilities and general countermeasures that were presented in Chapter 4. (Right): Statistical information about the applied attack ratings as well as its underlying components. Details related to attack rating can be obtained in Section 3.2 (Elapsed Time: Table 3.4, Window of Opportunity: Table 3.9, Equipment Value: Table 3.11, Knowledge about TOE: Table 3.7, Expertise: Table 3.5, and Attack Rating: Table 3.13). TOE stands for Target of Evaluation.

The number of attack paths that cater to DV-QKD systems (35+5=40) are almost thrice as many as those that cater to CV-QKD systems (9+5=14). It would therefore seem that CV-QKD systems have received less attention than their DV counterparts when it comes to the topic of implementation attacks. This is however not unreasonable as apart from being older (inception in 1984, first implementations in the early 1990s), the field of DV-QKD has been the focus of a significantly larger number of research groups than CV-QKD (inception in 1999, first implementations from 2004 onward).

Diving deeper into the tables presented in Sections 4.1-4.4, one can make some conclusions related to which attack categories have been thoroughly researched and how well are the countermeasures (to mitigate those type of attacks) known now. A good percentage of attacks in Section 4.1 have "detector-control attacks" as their assigned category. Together with "Trojan-horse attacks" (which are applicable to both DV-QKD and CV-QKD systems, and primarily on transmitters), the entire attack paths as well as mitigation strategies in these two categories are likely to be the best understood.

Conversely, there are several candidates for the attack categories that are still not very well understood and need more research. With the recent major developments in the fields of MDI-QKD and TF-QKD (which are immune to any attacks on QKD receivers), a greater focus on attacks against QKD transmitters can be expected.

Attack ratings (Section 3.2) based on the available literature and the combined knowledge of the authors of this document have been provided in each of the tables in Sections 4.1-4.3. By gleaning data from these tables, it becomes possible to obtain statistical distributions on the different components that go into the calculation of ratings. These distributions are illustrated using various bar charts on the right in Figure 5.1. Information about the labels on each of these bar charts can be obtained through the tables that are mentioned in the caption of the figure.

As mentioned right at the beginning of this document (in Section 1.2) and then explained in detail in Section 3.2 and beginning of Chapter 4, there is a fair bit of uncertainty in the determination of these ratings. While qualitative mappings from numerical values have been provided through the various fields in the attack tables, these represent a snapshot of evaluation at the point of writing.

Nonetheless, it is possible to visualise trends and make somewhat simple projections. Starting with the top bar chart on attack ratings, it can be observed that a substantial number of implementation attacks have a rating of 'Moderate' or higher. The main contributors to these ratings are the facts that in most cases, an expertise ranging from 'Proficient' to 'Expert' and equipment ranging from 'Specialised' to 'Bespoke' is required to mount the attacks.

It is notable that these attack ratings are calculated assuming the worst-case scenario. That is evidenced by the fact that the knowledge about the TOE is almost in all cases 'Public information' in Figure 5.1, which is quite a relaxed assumption as detailed datasheets about QKD systems are usually not easy to access. The most probable elapsed time of < 1 day is only considering the exploitation phase (but can actually be assumed to be a few weeks in the identification phase for most of the attacks).

In conclusion, a fairly exhaustive overview of implementation attacks against QKD systems has been provided in this document. Information about various aspects of an attack (or a class of attacks) together with countermeasures proposed to prevent them have been disseminated through a series of tables. Assignment of attack ratings, while not authoritative, has also paved the path for presenting some simple interpretations at least on an ensemble level.

Using best practices, namely applying the proposed countermeasures through hardware modifications or software patches to an existing QKD system can help in preserving security assurances such as the fundamental inability to retroactively break the security of a QKD-facilitated key agreement. Alternative solutions include embracing different schemes such as MDI-QKD and TF-QKD that completely relax the security requirements on QKD receivers, thus reducing the overall need and effort of system characterization (though at the cost of a major overhaul of the physical realization).

As an outlook, it can be expected that the overall state of knowledge on the topic of practical security of QKD systems and implementation attacks shall rise to higher technological readiness levels in the near future. This would require increasing collaborations between academia, industry, and metrology institutes for development on a commercial scale as well as for product evaluation and standardisation. The most relevant implication from this further research and adoption of QKD is the discovery of more vulnerabilities and attacks, together with the corresponding countermeasures. Conversely, some of the here-described paths and measures may become obsolete. With more research in this field, it is expected that the ratings can be made more granular and certain.

Bibliography

Adhikari2015 S. Adhikari, D. Home, A. Majumdar, A. Pan, A. Shenoy, and R. Srikanth. "Toward secure communication using intra-particle entanglement". In: Quantum Inf. Process. 14.4 (2015), pp. 1451–1468. DOI: 10.1007/s11128-015-0941-0.

Alhussein2019a M. Alhussein and K. Inoue. "Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks". In: Japanese Journal of Applied Physics 58.10 (2019), p. 102001. DOI: 10.7567/1347-4065/ab42c7.

Alhussein2019 M. Alhussein, K. Inoue, and T. Honjo. "Monitoring coincident clicks in differential-quadrature-phase shift QKD to reveal detector blinding and control attacks". In: Japanese Journal of Applied Physics 58.1 (2019), p. 012006. DOI: 10.7567/1347-4065/aaec1c.

Arnon2019 S. Arnon. "Quantum technology for optical wireless communication in data-center security and hacking". In: Broadband Access Communication Technologies XIII. Vol. 10945. 2019. DOI: 10.1117/12.2505733.

ArteagaDiaz2022 P. Arteaga-Díaz, D. Cano, and V. Fernandez. "Practical Side-Channel Attack on Free-Space QKD Systems With Misaligned Sources and Countermeasures". In: IEEE Access 10 (2022), pp. 82697–82705. DOI: 10.1109/ACCESS.2022.3196677.

Babukhin2022a D. Babukhin, D. Kronberg, and D. Sych. "Explicit attacks on the Bennett-Brassard 1984 protocol with partially distinguishable photons". In: Phys. Rev. A 106 (2022), p. 042403. DOI: 10.1103/PhysRevA.106.042403.

Babukhin2020 D. Babukhin and D. Sych. "Intercept-resend attack on passive side channel of the light source in BB84 decoy-state protocol". In: Journal of Physics Conference Series. Vol. 1695. 2020, p. 012119. DOI: 10.1088/1742-6596/1695/1/012119.

Babukhin2021 D. Babukhin and D. Sych. "Explicit attacks on passive side channels of the light source in the BB84 decoy state protocol". In: Journal of Physics: Conference Series 1984 (2021), p. 012008. DOI: 10.1088/1742-6596/1984/1/012008.

Babukhin2022 D. Babukhin and D. Sych. "Joint eavesdropping on the BB84 decoy state protocol with an arbitrary passive light-source side channel". In: Preprint arXiv:2211.13669 (2022).

Balygin2018 K. Balygin, A. Klimov, I. Bobrov, K. Kravtsov, S. Kulik, and S. Molotkov. "Inherent security of phase coding quantum key distribution systems against detector blinding attacks". In: Laser Physics Letters 15.9 (2018), p. 095203. DOI: 10.1088/1612-202X/aad1c9.

Barrett2013 J. Barrett, R. Colbeck, and A. Kent. "Memory Attacks on Device-Independent Quantum Cryptography". In: Phys. Rev. Lett. 110 (2013), p. 010503. DOI: 10.1103/PhysRevLett.110.010503.

Beaudry2008 N. J. Beaudry, T. Moroder, and N. Lütkenhaus. "Squashing Models for Optical Measurements in Quantum Communication". In: Phys. Rev. Lett. 101 (2008). DOI: https://doi.org/10.1103/PhysRevLett.101.093601.

Bennett2014 Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: Theoretical Computer Science 560 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 7–11. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. URL: https://www.sciencedirect.com/science/article/pii/S0304397514004241.

Bethune2000 D.S. Bethune and W.P. Risk. “An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light”. In: IEEE J. Quantum Electron. 36.3 (Mar. 2000). Conference Name: IEEE J. Quantum Electron., pp. 340–347. ISSN: 1558-1713. DOI: 10.1109/3.825881.

Biswas2021 A. Biswas, A. Banerji, P. Chandravashi, R. Kumar, and R. Singh. “Experimental Side Channel Analysis of BB84 QKD Source”. In: IEEE Journal of Quantum Electronics 57.6 (2021), pp. 1–7. DOI: 10.1109/JQE.2021.3111332.

Bochkov2019 M. Bochkov and A. Trushechkin. “Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds”. In: Phys. Rev. A 99 (2019), p. 032308. DOI: 10.1103/PhysRevA.99.032308.

Bourassa2021 J. Bourassa, A. Gnanapandithan, L. Qian, and H. Lo. “Measurement device-independent quantum key distribution with passive, time-dependent source side-channels”. In: Phys. Rev. A 106 (2022), p. 062618. DOI: 10.1103/PhysRevA.106.062618.

Brassard2000 G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders. “Limitations on Practical Quantum Cryptography”. In: Phys. Rev. Lett. 85 (2000), p. 1330. DOI: 10.1103/PhysRevLett.85.1330.

Braunstein2012 S. Braunstein and S. Pirandola. “Side-channel-free quantum key distribution”. In: Phys. Rev. Lett. 108 (2012), p. 130502. DOI: 10.1103/PhysRevLett.108.130502.

Bugge2014 A. Bugge, S. Sauge, A. Ghazali, J. Skaar, L. Lydersen, and V. Makarov. “Laser Damage Helps the Eavesdropper in Quantum Cryptography”. In: Phys. Rev. Lett. 112 (2014), p. 070503. DOI: 10.1103/PhysRevLett.112.070503.

Cao2015 Zhu Cao, Zhen Zhang, Hoi-Kwong Lo, and Xiongfeng Ma. “Discrete-phase-randomized coherent state source and its application in quantum key distribution”. In: New Journal of Physics 17.5 (May 2015), p. 053014. DOI: 10.1088/1367-2630/17/5/053014. URL: https://dx.doi.org/10.1088/1367-2630/17/5/053014.

Carter1979 J.Lawrence Carter and Mark N. Wegman. “Universal classes of hash functions”. In: Journal of Computer and System Sciences 18.2 (1979), pp. 143–154. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(79)90044-8. URL: https://www.sciencedirect.com/science/article/pii/0022000079900448.

Chaiwongkhot2019 P. Chaiwongkhot, K. Kuntz, Y. Zhang, A. Huang, J. Bourgoin, S. Sajeed, N. ütkenhaus, T. Jennewein, and V. Makarov. “Eavesdropper’s ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence”. In: Phys. Rev. A 99 (2019), p. 062315. DOI: 10.1103/PhysRevA.99.062315.

Chaiwongkhot2022 P. Chaiwongkhot, J. Zhong, A. Huang, H. Qin, S. Shi, and V. Makarov. “Faking photon number on a transition-edge sensor”. In: EPJ Quantum Technology 9 (2022), p. 23. DOI: 10.1140/epjqt/s40507-022-00141-2.

Chau2002 H. F. Chau. “Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate”. In: American Physical Society (2002). DOI: 10.1103/PhysRevA.66.060302.

Chistiakov2019 V. Chistiakov, A. Huang, V. Egorov, and V. Makarov. “Controlling single-photon detector ID210 with bright light”. In: Opt. Express 27.22 (2019), pp. 32253–32262. DOI: 10.1364/OE.27.032253.

CEM Common Methodology for Information Technology Security Evaluation. https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf. Accessed: 2023-08-18.

CurrasLorenzo2023 Guillermo Currás-Lorenzo, Margarida Pereira, Go Kato, Marcos Curty, and Kiyoshi Tamaki. A security framework for quantum key distribution implementations. arXiv:2305.05930 [quant-ph]. May 2023. DOI: 10.48550/arXiv.2305.05930. URL: http://arxiv.org/abs/2305.05930 (visited on 06/12/2023).

CurrasLorenzo2022 G. Currs-Lorenzo, K. Tamaki, and M. Curty. "Security of decoy-state quantum key distribution with imperfect phase randomization". In: Preprint arXiv:2210.08183 (2022). DOI: 10.48550/arXiv.2210.08183.

Curty2019a M. Curty, K. Azuma, and H. Lo. "Simple security proof of twin-field type quantum key distribution protocol". In: npj Quantum Information 5 (2019). DOI: https://doi.org/10.1038/s41534-019-0175-6.

Curty2019 M. Curty and H. Lo. "Foiling covert channels and malicious classical post-processing units in quantum key distribution". In: npj Quantum Information 5 (2019), p. 14. DOI: 10.1038/s41534-019-0131-5.

Curty2010b Marcos Curty, Xiongfeng Ma, Hoi-Kwong Lo, and Norbert Lütkenhaus. "Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals". In: Phys. Rev. A 82 (5 Nov. 2010), p. 052325. DOI: 10.1103/PhysRevA.82.052325. URL: https://link.aps.org/doi/10.1103/PhysRevA.82.052325.

Curty2010 Marcos Curty, Xiongfeng Ma, Bing Qi, and Tobias Moroder. "Passive decoy-state quantum key distribution with practical light sources". In: Physical Review A 81.2 (Feb. 2010). Publisher: American Physical Society, p. 022310. DOI: 10.1103/PhysRevA.81.022310. URL: https://link.aps.org/doi/10.1103/PhysRevA.81.022310 (visited on 06/12/2023).

AlDarwbi2022 M. Al-Darwbi, A. Ghorbani, and A. Lashkari. "QKeyShield: A Practical Receiver-Device-Independent Entanglement-Swapping-Based Quantum Key Distribution". In: IEEE Access 10 (2022), pp. 107685–107702. DOI: 10.1109/ACCESS.2022.3212787.

Derkach2016 I. Derkach, V. Usenko, and R. Filip. "Preventing side-channel effects in continuous-variable quantum key distribution". In: Phys. Rev. A 93.3 (2016). DOI: 10.1103/PhysRevA.93.032309.

Derkach2017 I. Derkach, V. Usenko, and R. Filip. "Continuous-variable quantum key distribution with a leakage from state preparation". In: Phys. Rev. A 96.6 (2017). DOI: 10.1103/PhysRevA.96.062309.

Dixon2017 A. Dixon, J. Dynes, M. Lucamarini, B. Frhlich, A. Sharpe, A. Plews, W. Tam, Z. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. Shields. "Quantum key distribution with hacking countermeasures and long term field trial". In: Scientific Reports 7 (2017), p. 1978. DOI: 10.1038/s41598-017-01884-0.

Dong2014 Z. Dong, N. Yu, Z. Wei, J. Wang, and Z. Zhang. "An attack aimed at active phase compensation in one-way phase-encoded QKD systems". In: Eur. Phys. J. D 68 (2014), p. 230. DOI: 10.1140/epjd/e2014-40693-6.

Duplinskiy2019 A. Duplinskiy and D. Sych. "Bounding light source side channels in QKD via Hong-Ou-Mandel interference". In: Phys. Rev. A 104 (2021), p. 012601. DOI: 10.1103/PhysRevA.104.012601.

Elezov2019 M. Elezov, R. Ozhegov, G. Goltsman, and V. Makarov. "Countermeasure against bright-light attack on superconducting nanowire single-photon detector in quantum key distribution". In: Opt. Express 27.21 (2019), pp. 30979–30988. DOI: 10.1364/OE.27.030979.

Elezov2015 M. Elezov, R. Ozhegov, Y. Kurochkin, G. Goltsman, and V. Makarov. "Countermeasures against blinding attack on superconducting nanowire detectors for QKD". In: Eur. Phys. J. Conf. 103 (2015), p. 10002. DOI: 10.1051/epjconf/201510310002.

Fatin2021 M. Fatin and S. Sajeed. "Generalized efficiency mismatch attack to bypass the detection-scrambling countermeasure". In: Opt. Express 29.11 (2021), pp. 16073–16086. DOI: 10.1364/OE.419338.

Fedorov2019 A. Fedorov, I. Gerhardt, A. Huang, J. Jogenfors, Y. Kurochkin, A. Lamas-Linares, J. Larsson, G. Leuchs, L. Lydersen, V. Makarov, and J. Skaar. "Comment on 'Inherent security of phase coding quantum key dis- tribution systems against detector blinding attack' [Laser Phys. Lett. 15, 095203 (2018)]". In: Laser Phys. Lett. 16 (2019), p. 019401. DOI: 10.1088/1612-202X/aad1c9.

Fei2015 Y. Fei, M. Gao, W. Wang, C. Li, and Z. Ma. "Practical attacks on decoy-state quantum-key-distribution systems with detector efficiency mismatch". In: Phys. Rev. A 91 (2015), p. 052305. DOI: 10.1103/PhysRevA.91.052305.

Fei2018b Y. Fei, X. Meng, M. Gao, Z. Ma, and H. Wang. "Exploiting wavelength-dependent beam splitter to attack the calibration of practical quantum key distribution systems". In: Optik 170 (2018), pp. 368–375. DOI: 10.1016/j.ijleo.2018.05.089.

Fei2018 Y. Fei, X. Meng, M. Gao, Y. Yang, H. Wang, and Z. Ma. "Strong light illumination on gainswitched semiconductor lasers helps the eavesdropper in practical quantum key distribution systems". In: Optics Communications 419 (2018), pp. 83–89. DOI: 10.1016/j.optcom.2018.03.029.

Felix2001 S. Felix, N. Gisin, A. Stefanov, and H. Zbinden. "Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses". In: Journal of Modern Optics 48 (2001), pp. 2009–2021. DOI: 10.1080/09500340108240903.

Ferenczi2007 A. Ferenczi, P. Grangier, and F. Grosshans. "Calibration Attack and Defense in Continuous Variable Quantum Key Distribution". In: 2007. DOI: 10.1364/IQEC.2007.IC_13. URL: https://opg.optica.org/abstract.cfm?URI=IQEC-2007-IC_13.

Fujiwara2013 M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki. "Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack". In: Opt. Express 21.5 (2013), pp. 6304–6312. DOI: 10.1364/oe.21.006304.

Fung2007 C. Fung, B. Qi, K. Tamaki, and H. Lo. "Phase-remapping attack in practical quantum-key-distribution systems". In: Phys. Rev. A 75 (2007), p. 032314. DOI: 10.1103/PhysRevA.75.032314.

Fung2009 C. Fung, K. Tamaki, B. Qi, H. Lo, and X. Ma. "Security proof of quantum key distribution with detection efficiency mismatch". In: Quantum Information and Computation 9 (2009), pp. 131–165. DOI: 10.26421/QIC9.1-2-8.

Fung2011 C.-H. F. Fung, H. F. Chau, and H.-K. Lo. "Universal Squash Model For Optical Communications Using Linear Optics And Threshold Detectors". In: Phys. Rev. A 84 (2011). DOI: https://doi.org/10.1103/PhysRevA.84.020303.

Fung2006 Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo. "Performance of two quantum-key-distribution protocols". In: Phys. Rev. A 73 (1 Jan. 2006), p. 012337. DOI: 10.1103/PhysRevA.73.012337. URL: https://link.aps.org/doi/10.1103/PhysRevA.73.012337.

Gabdulkhakov2018 I. Gabdulkhakov, O. Morozov, G. Morozov, M. Zastela, A. Tyajelova, and L. Sarvarova. “Frequency coding quantum key distribution channel based on serial photons amplitude modulation and phase commutation”. In: vol. 10774. 2018. DOI: 10.1117/12.2322488.

Gaidash2022 A. Gaidash, G. Miroshnichenko, and A. Kozubov. “Subcarrier wave quantum key distribution with leaky and flawed devices”. In: J. Opt. Soc. Am. B 39.2 (2022), pp. 577–585. DOI: 10.1364/JOSAB.439776.

Gao2022 B. Gao, Z. Wu, W. Shi, Y. Liu, D. Wang, C. Yu, A. Huang, and J. Wu. “Strong pulse illumination hacks self-differencing avalanche photodiode detectors in a high-speed quantum key distribution system”. In: Preprint arXiv:2205.04177 (2022).

Gao2023 Yuanfei Gao and Zhiliang Yuan. “Suppression of patterning effect using IQ modulator for high-speed quantum key distribution systems”. In: Opt. Lett. 48.4 (Feb. 2023), pp. 1068–1071. DOI: 10.1364/OL.481374. URL: https://opg.optica.org/ol/abstract.cfm?URI=ol-48-4-1068.

GarciaEscartin2020 J. Garcia-Escartin, S. Sajeed, and V. Makarov. “Attacking quantum key distribution by light injection via ventilation openings”. In: PLOS ONE 15.8 (2020), e0236630. DOI: 10.1371/journal.pone.0236630.

Gerhardt2011 I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”. In: Nature Communications 2 (2011), p. 349. DOI: 10.1038/ncomms1348.

Gerhardt2011a I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer. “Experimentally Faking the Violation of Bells Inequalities”. In: Phys. Rev. Lett. 107 (2011), p. 170404. DOI: 10.1103/PhysRevLett.107.170404.

Gisin2006 N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. “Trojan-horse attacks on quantum-key-distribution systems”. In: Phys. Rev. A 73 (2006), p. 022320. DOI: 10.1103/PhysRevA.73.022320.

Gisin2002 Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. “Quantum cryptography”. In: Reviews of Modern Physics 74.1 (2002), pp. 145–196. ISSN: 1079-7114. URL: http://rmp.aps.org/abstract/RMP/v74/i1/p145%5C_1.

Gottesman2004 D. Gottesman, H. Lo, N. Lütkenhaus, and J. Preskill. “Security of quantum key distribution with imperfect devices”. In: Quantum Information and Computation (2004). DOI: 10.26421/QIC4.5-1.

Gras2020 G. Gras, N. Sultana, A. Huang, T. Jennewein, F. Bussires, V. Makarov, and H. Zbinden. “Optical control of single-photon negative-feedback avalanche diode detector”. In: J. Appl. Phys. 127 (2020), p. 094502. DOI: 10.1063/1.5140824.

Grosshans2003 Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. “Quantum key distribution using gaussian-modulated coherent states”. In: Nature 421.6920 (2003), pp. 238–241. ISSN: 0028-0836. DOI: 10.1038/nature01289. URL: https://www.nature.com/articles/nature01289%20http://www.nature.com/articles/nature01289.

Gruenenfelder2020 F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden. “Performance and security of 5 GHz repetition rate polarization-based quantum key distribution”. In: Appl. Phys. Lett. 117 (2020), p. 144003. DOI: 10.1063/5.0021468.

Guo2017 Y. Guo, C. Xie, Q. Liao, W. Zhao, G. Zeng, and D. Huang. “Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel”. In: Phys. Rev. A 96 (2017), p. 022320. DOI: 10.1103/PhysRevA.96.022320.

Hajomer2022 A. Hajomer, N. Jain, H. Mani, H. Chin, U. Andersen, and T. Gehring. "Modulation leakage-free continuous-variable quantum key distribution". In: Npj Quantum Inf. 8.1 (2022), pp. 1–8. DOI: 10.1038/s41534-022-00640-1.

Haeseler2008 H. Häseler, T. Moroder, and N. Lütkenhaus. "Testing quantum devices: Practical entanglement verification in bipartite optical systems". In: Phys. Rev. A 77 (2008), p. 032303. DOI: 10.1103/PhysRevA.77.032303.

He2020 D. He, Y. Qian, S. Wang, W. Chen, Z. Yin, G. Guo, and Z. HAn. "Robust countermeasure against detector control attack in a practical quantum key distribution system: reply". In: Optica 7.10 (2020), pp. 1415–1416. DOI: 10.1364/OPTICA.403917.

Hegazy2022 S. Hegazy, S. Obayya, and B. Saleh. "Randomized ancillary qubit overcomes detector-control and intercept-resend hacking of quantum key distribution". In: Journal of Lightwave Technology (2022). DOI: 10.1109/JLT.2022.3198108.

Honjo2013 T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki. "Countermeasure against tailored bright illumination attack for DPS-QKD". In: Opt. Express 21.3 (2013), pp. 2667–2673. DOI: 10.1364/OE.21.002667.

Hu2010 Jia-Zhong Hu and Xiang-Bin Wang. "Reexamination of the decoy-state quantum key distribution with an unstable source". In: Phys. Rev. A 82 (1 July 2010), p. 012331. DOI: 10.1103/PhysRevA.82.012331. URL: https://link.aps.org/doi/10.1103/PhysRevA.82.012331.

Huang2020 A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov. "Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution". In: Phys. Rev. Appl. 13 (2020), p. 034017. DOI: 10.1103/PhysRevApplied.13.034017.

Huang2019 A. Huang, . Navarrete, S. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov. "Laser seeding attack in quantum key distribution". In: Phys. Rev. Appl. 12 (2019), p. 064043. DOI: 10.1103/PhysRevApplied.12.064043.

Huang2016 A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legre, and V. Makarov. "Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption". In: IEEE Journal of Quantum Electronics 52.11 (2016), pp. 1–11. DOI: 10.1109/JQE.2016.2611443.

Huang2018 A. Huang, S. Sun, Z. Liu, and V. Makarov. "Decoy state quantum key distribution with imperfect source". In: Phys. Rev. A 98, 01233 98 (2018), p. 012330. DOI: 10.1103/PhysRevA.98.012330.

Huang2014 J. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Yin, S. Wang, W. Chen, G. Guo, and Z. Han. "Quantum hacking on quantum key distribution using homodyne detection". In: Phys. Rev. A 89 (2014), p. 032304. DOI: 10.1103/PhysRevA.89.032304.

Huang2013 J. Huang, C. Weedbrook, Z. Yin, S. Wang, H. Li, W. Chen, G. Guo, and Z. Han. "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack". In: Phys. Rev. A 87 (2013), p. 062329. DOI: 10.1103/PhysRevA.87.062329.

Huang2017 P. Huang, J. Huang, T. Wang, H. Li, D. Huang, and G. Zeng. "Robust continuous-variable quantum key distribution against practical attacks". In: Phys. Rev. A 95.5 (2017), p. 052302. DOI: 10.1103/PhysRevA.95.052302.

Huang2019b W. Huang, Y. Mao, C. Xie, and D. Huang. "Quantum hacking of free-space continuous-variable quantum key distribution by using a machine-learning technique". In: Phys. Rev. A 100 (2019), p. 012316. DOI: 10.1103/PhysRevA.100.012316.

Huang2019a W. Huang, W. Zhang, and Y. Huang. "Elimination of Spatial Side-Channel Information for Compact Quantum Key Distribution Senders". In: J. Electron. Sci. Technol. 17.3 (2019), pp. 195–203. DOI: 10.11989/JEST.1674-862X.90416014.

Hwang2003 W. Hwang. “Quantum Key Distribution with High Loss: Toward Global Secure Communication”. In: Phys. Rev. Lett. 91 (2003), p. 057901. DOI: 10.1103/PhysRevLett.91.057901.

Ioannou2022 M. Ioannou, M. Pereira, D. Rusca, F. Grnenfelder, A. Boaron, M. Perrenoud, A. Abbott, P. Sekatski, J. Bancal, N. Maring, H. Zbinden, and N. Brunner. “Receiver-device-independent quantum key distribution”. In: Quantum 6 (2022), p. 718. DOI: 10.22331/q-2022-05-24-718.

Iwakoshi2015 T. Iwakoshi. “Faked state attacks on realistic round robin DPS quantum key distribution systems and countermeasure”. In: vol. 9505. 2015. DOI: 10.1117/12.2176770.

Jain2014 N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs. “Trojan-horse attacks threaten the security of practical quantum cryptography”. In: New Journal of Physics 16 (2014), p. 123030. DOI: 10.1088/1367-2630/16/12/123030.

Jain2021 N. Jain, I. Derkach, H. Chin, R. Filip, U. Andersen, V. Usenko, and T. Gehring. “Modulation leakage vulnerability in continuous-variable quantum key distribution”. In: Quantum Science and Technology 6.4 (2021), p. 045001. DOI: 10.1088/2058-9565/ac0d4c.

Jain2016 N. Jain and G. Kanter. “Upconversion-based receivers for quantum hacking-resistant quantum key distribution”. In: Quantum Inf Process 15.7 (2016), pp. 2863–2879. DOI: 10.1007/s11128-016-1315-y.

Jain2016a N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs. “Attacks on practical quantum key distribution systems (and how to prevent them)”. In: Contemporary Physics 57.3 (2016), pp. 366–387. DOI: 10.1080/00107514.2016.1148333.

Jain2015 N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs. “Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems”. In: IEEE Journal of Selected Topics in Quantum Electronics 21.3 (2015), pp. 168–177. DOI: doi:10.1109/JSTQE.2014.2365585.

Jain2011 N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs. “Device Calibration Impacts Security of Quantum Key Distribution”. In: Phys. Rev. Lett. 107 (2011), p. 110501. DOI: 10.1103/PhysRevLett.107.110501.

Jiang2012 M. Jiang, S. Sun, C. Li, and L. Liang. “Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states”. In: Phys. Rev. A 86 (2012), p. 032310. DOI: 10.1103/PhysRevA.86.032310.

Jiang2014 M. Jiang, S. Sun, C. Li, and L. Liang. “Frequency shift attack on plug-and-play quantum key distribution systems”. In: Journal of Modern Optics 61 (2014), p. 147. DOI: 10.1080/09500340.2013.872309.

Jiang2013 M. Jiang, S. Sun, G. Tang, X. Ma, C. Li, and L. Liang. “Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems”. In: Phys. Rev. A 88 (2013), p. 062335. DOI: 10.1103/PhysRevA.88.062335.

Jogenfors2015 J. Jogenfors, A. Elhassan, J. Ahrens, M. Bourennane, and J. Larsson. “Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution”. In: Science Advances 1.11 (2015). DOI: 10.1126/sciadv.1500793.

JILHAS Joint Interpretation Library Hardware Attacks Subgroup. https://sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3.2.pdf. Accessed: 2023-09-28.

Jouguet2013 P. Jouguet, S. Kunz-Jacques, and E. Diamanti. “Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution”. In: Phys. Rev. A 87 (2013), p. 062313. DOI: 10.1103/PhysRevA.87.062313.

Jouguet2012 P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier. "Analysis of imperfections in practical continuous-variable quantum key distribution". In: Phys. Rev. A 86 (2012), p. 032309. DOI: 10.1103/PhysRevA.86.032309.

Kepferman2018 J. Kepferman and S. Arnon. "Zero-error attacks on a quantum key distribution FSO system". In: OSA Continuum 1.3 (2018), pp. 1079–1086. DOI: 10.1364/OSAC.1.001079.

Kikuchi2015 Kazuro Kikuchi. "Fundamentals of coherent optical fiber communications". In: Journal of Lightwave Technology 34.1 (2015), pp. 157–179.

Kim2021 G. Kim, D. Park, H. Kim, and S. Hong. "Side Channel Vulnerability in Parity Computation of Generic Key Reconciliation Process on QKD". In: 2021, pp. 257–261. DOI: 10.1109/ICTC52510.2021.9620820.

Kim2018 S. Kim, S. Jin, Y. Lee, B. Park, H. Kim, and S. Hong. "Single Trace Side Channel Analysis on Quantum Key Distribution". In: 2018, pp. 736–739. DOI: 10.1109/ICTC.2018.8539703.

Ko2017 H. Ko, B. Choi, J. Choe, K. Kim, J. Kim, and C. Youn. "Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system". In: Opt. Express 25.17 (2017), p. 2004520055. DOI: 10.1364/OE.25.020045.

Ko2017a H. Ko, B. Choi, J. Choe, K. Kim, J. Kim, and C. Youn. "High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers". In: Photonics Research 6.3 (2018), pp. 214–219. DOI: 10.1364/PRJ.6.000214.

Ko2016 H. Ko, K. Lim, J. Oh, and J. Rhee. "Informatic analysis for hidden pulse attack exploiting spectral characteristics of optics in plug-and-play quantum key distribution system". In: Quantum Inf Process 15.10 (2016), pp. 4265–4282. DOI: 10.1007/s11128-016-1400-2.

Koashi2004 M. Koashi. "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse". In: Phys. Rev. Lett. 93 (2004), p. 120501. DOI: 10.1103/PhysRevLett.93.120501.

Koashi2008 M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto. "Security of entanglement-based quantum key distribution with practical detectors". In: (2008). arXiv: 0804.0891 [quant-ph].

Kobayashi2014 T. Kobayashi, A. Tomita, and A. Okamoto. "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser". In: Phys. Rev. A 90 (2014), p. 032320. DOI: 10.1103/PhysRevA.90.032320.

KoehlerSidki2018 A. Koehler-Sidki, J. Dynes, M. Lucamarini, G. Roberts, A. Sharpe, Z. Yuan, and A. Shields. "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution". In: Phys. Rev. Appl. 9 (2018), p. 044027. DOI: 10.1103/PhysRevApplied.9.044027.

KoehlerSidki2019 A. Koehler-Sidki, J. Dynes, A. Martinez, M. Lucamarini, G. Roberts, A. Sharpe, Z. Yuan, and A. Shields. "Intrinsic Mitigation of the After-Gate Attack in Quantum Key Distribution through Fast-Gated Delayed Detection". In: Phys. Rev. Appl. 12.2 (2019). DOI: 10.1103/PhysRevApplied.12.024050.

KoehlerSidki2018a A. Koehler-Sidki, M. Lucamarini, J. Dynes, G. Roberts, A. Sharpe, Z. Yuan, and A. Shields. "Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation". In: Phys. Rev. A 98 (2018), p. 022327. DOI: 10.1103/PhysRevA.98.022327.

Kong2022 L. Kong, W. Liu, F. Jing, and C. He. "Practical security analysis of continuous-variable quantum key distribution with an unbalanced heterodyne detector". In: Chinese Physics B 31.7 (2022). DOI: 10.1088/1674-1056/ac4102.

Kumar2021 Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaume. "Experimental Vulnerability Analysis of QKD Based on Attack Ratings". In: Sci Rep 11 (2021). URL: https://www.nature.com/articles/s41598-021-87574-4.

KunzJacques2015 S. Kunz-Jacques and P. Jouguet. "Robust shot-noise measurement for continuous-variable quantum key distribution". In: Phys. Rev. A 91 (2015), p. 022307. DOI: 10.1103/PhysRevA.91.022307.

Kurtsiefer2001 C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. "The breakdown flash of silicon avalanche photodiodes - back door for eavesdropper attacks?" In: Journal of Modern Optics 48.13 (2001), pp. 2039–2047. DOI: 10.1080/09500340108240905.

LamasLinares2007 A. Lamas-Linares and C. Kurtsiefer. "Breaking a quantum key distribution system through a timing side channel". In: Opt. Express 15.15 (2007), pp. 9388–9393. DOI: 10.1364/OE.15.009388.

Lee2016 M. Lee, B. Park, M. Woo, C. Park, Y. Kim, S. Han, and S. Moon. "Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme". In: Phys. Rev. A 94 (2016), p. 062321. DOI: 10.1103/PhysRevA.94.062321.

Lee2017 M. Lee, M. Woo, J. Jung, Y. Kim, S. Han, and S. Moon. "Free-space QKD system hacking by wavelength control using an external laser". In: Opt. Express 25.10 (2017), pp. 11124–11131. DOI: 10.1364/OE.25.011124.

Lee2019 M. Lee, M. Woo, Y. Kim, Y. Cho, S. Han, and S. Moon. "Quantum hacking on a free-space quantum key distribution system without measuring quantum signals". In: J. Opt. Soc. Am. B 36.3 (2019), B77–B82. DOI: 10.1364/JOSAB.36.000B77.

Legre2012 M. Legre and G. Ribordy. "Apparatus and method for the detection of attacks taking control of the single photon detectors of a quantum cryptography apparatus by randomly changing their efficiency". In: Intl. Patent WO 2012/046135 A2. (2012).

Li2022 D. Li, Y. Tang, Y. Zhao, L. Zhou, Y. Zhao, and S. Tang. "Security of Optical Beam Splitter in Quantum Key Distribution". In: Photonics 9.8 (2022). DOI: 10.3390/photonics9080527.

Li2011 H. Li, S. Wang, J. Huang, W. Chen, Z. Yin, F. Li, Z. Zhou, D. Liu, Y. Zhang, G. Guo, W. Bao, and Z. Han. "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources". In: Phys. Rev. A 84 (2011), p. 062308. DOI: 10.1103/PhysRevA.84.062308.

Li2021 W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W. Liu, X. Jiang, S. Liao, C. Peng, M. Curty, F. Xu, and J. Pan. "Experimental quantum key distribution secure against malicious devices". In: Phys. Rev. Appl. 15 (2021), p. 034081. DOI: 10.1103/PhysRevApplied.15.034081.

Lim2014a C. Lim, N. Walenta, M. Legre, N. Gisin, and H. Zbinden. "Random Variation of Detector Efficiency: A Countermeasure against Detector Blinding Attacks for Quantum Key Distribution". In: IEEE Journal of Selected Topics in Quantum Electronics 21.3 (2015), pp. 192–196. DOI: 10.1109/JSTQE.2015.2389528.

Liu2014 Q. Liu, A. Lamas-Linares, C. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt. "A universal setup for active control of a single-photon detector". In: Rev. Sci. Instrum. 85 (2014), p. 013108. DOI: 10.1063/1.4854615.

Liu2011 W. Liu, S. Sun, L. Liang, and J. Yuan. "Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution". In: Phys. Rev. A 83 (2011), p. 042326. DOI: 10.1103/PhysRevA.83.042326.

Liu2017 Weiqi Liu, Jinye Peng, Peng Huang, Duan Huang, and Guihua Zeng. "Monitoring of continuous-variable quantum key distribution system in real environment". EN. In: Optics Express 25.16 (Aug. 2017). Publisher: Optica Publishing Group, pp. 19429–19443. ISSN: 1094-4087. DOI: 10.1364/OE.25.019429. URL: https://opg.optica.org/oe/abstract.cfm?uri=oe-25-16-19429 (visited on 05/01/2023).

Liu2014a X. Liu, B. Zhang, J. Wang, C. Tang, J. Zhao, and S. Zhang. "Eavesdropping on counterfactual quantum key distribution with finite resources". In: Phys. Rev. A 90.2 (2014). DOI: 10.1103/PhysRevA.90.022318.

Lizama2012 L. Lizama, J. Mauricio Lopez, E. De Carlos Lopez, and S. Venegas-Andraca. "Enhancing Quantum Key Distribution (QKD) to address quantum hacking". In: 2012 Iberoamerican Conference on Electronics Engineering and Computer Science. Vol. 3. 2012, pp. 80–88. DOI: 10.1016/j.protcy.2012.03.009.

Lo2012 H. Lo, M. Curty, and B. Qi. "Measurement-device-independent quantum key distribution". In: Phys. Rev. Lett. 108 (2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503.

Lo2005 H. Lo, X. Ma, and K. Chen. "Decoy State Quantum Key Distribution". In: Phys. Rev. Lett. 94 (2005), p. 230504. DOI: 10.1103/PhysRevLett.94.230504.

Lo2007 H. Lo and J. Preskill. "Security of quantum key distribution using weak coherent states with nonrandom phases". In: Quant. Inf. Comput. 8 (2007), pp. 431–458. DOI: 10.26421/QIC7.5-6-2.

Lo2014 Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. "Secure quantum key distribution". In: Nature Photonics 8.8 (2014), pp. 595–604. ISSN: 1749-4885. URL: http://dx.doi.org/10.1038/nphoton.2014.149%2010.1038/nphoton.2014.149.

Lu2013 H. Lu, C. Fung, and Q. Cai. "Two-way deterministic quantum key distribution against detector-side-channel attacks". In: Phys. Rev. A 88.4 (2013). DOI: 10.1103/PhysRevA.88.044302.

Lu2021 Y. Lu, M. Jiang, Y. Wang, X. Zhang, F. Liu, C. Zhou, H. Li, and W. Bao. "Practical analysis of sending or not-sending twin-field quantum key distribution with frequency side channels". In: Applied Sciences 11.20 (2021), p. 9560. DOI: 10.3390/app11209560.

Lucamarini2015 M. Lucamarini, I. Choi, M. Ward, J. Dynes, Z. Yuan, and A. Shields. "Practical security bounds against the trojan-horse attack in quantum key distribution". In: Phys. Rev. X 5.3 (2015), pp. 1–19. DOI: 10.1103/PhysRevX.5.031030.

Lucamarini2018 M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields. "Overcoming the ratedistance limit of quantum key distribution without quantum repeaters". In: Nature 557.7705 (2018), pp. 400–403. DOI: 10.1038/s41586-018-0066-6.

Luetkenhaus1999 N. Lütkenhaus. "Estimates for practical quantum cryptography". In: Phys. Rev. A 59 (1999), p. 3301. DOI: 10.1103/PhysRevA.59.3301.

Luetkenhaus2000 N. Lütkenhaus. "Security against individual attacks for realistic quantum key distribution". In: Phys. Rev. A 61 (2000), p. 052304. DOI: 10.1103/PhysRevA.61.052304.

Luetkenhaus2002 N. Lütkenhaus and M. Jahma. "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack". In: New Journal of Physics 4 (2002), p. 44. DOI: 10.1088/1367-2630/4/1/344.

Lydersen2011 L. Lydersen, M. Akhlaghi, A. Majedi, J. Skaar, and V. Makarov. "Controlling a superconducting nanowire single-photon detector using tailored bright illumination". In: New Journal of Physics 13.11 (2011), p. 113042. DOI: 10.1088/1367-2630/13/11/113042.

Lydersen2011b L. Lydersen, N. Jain, C. Wittmann, . Mary, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. “Superlinear threshold detectors in quantum cryptography”. In: Phys. Rev. A 84 (2011), p. 032320. DOI: 10.1103/PhysRevA.84.032320.

Lydersen2011c L. Lydersen, V. Makarov, and J. Skaar. “Comment on Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography [Appl. Phys. Lett. 98, 231104 (2011)]”. In: Appl. Phys. Lett. 99 (2011), p. 196101. DOI: 10.1063/1.3658806.

Lydersen2011d L. Lydersen, V. Makarov, and J. Skaar. “Secure gated detection scheme for quantum cryptography”. In: Phys. Rev. A 83 (2011), p. 032306. DOI: 10.1103/PhysRevA.83.032306.

Lydersen2011a L. Lydersen, J. Skaar, and V. Makarov. “Tailored bright illumination attack on distributed-phase-reference protocols”. In: Journal of Modern Optics 58 (2011), p. 680. DOI: 10.1080/09500340.2011.565889.

Lydersen2010a L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: Nature Photon 4 (2010), p. 686. DOI: 10.1038/nphoton.2010.214.

Lydersen2010b L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. “Reply to ”Avoiding the Detector Blinding Attack on Quantum Cryptography””. In: Nature Photon 4 (2010), p. 801. DOI: 10.1038/nphoton.2010.278.

Lydersen2010c L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. “Thermal blinding of gated detectors in quantum cryptography”. In: Opt. Express 18 (2010), pp. 27938–27954. DOI: 10.1364/OE.18.027938.

Ma2016 H. Ma, W. Bao, H. Li, and C. Chou. “Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack”. In: Chinese Physics B 25.8 (2016). DOI: 10.1088/1674-1056/25/8/080309.

Ma2014 X. Ma, S. Sun, M. Jiang, M. Gui, Y. Zhou, and L. Liang. “Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator”. In: Phys. Rev. A 89.3 (2014), p. 032310. DOI: 10.1103/PhysRevA.89.032310.

Ma2013a X. Ma, S. Sun, M. Jiang, and L. Liang. “Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems”. In: Phys. Rev. A 88 (2013), p. 022339. DOI: 10.1103/PhysRevA.88.022339.

Ma2013 X. Ma, S. Sun, M. Jiang, and L. Liang. “Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol”. In: Phys. Rev. A 87 (2013), p. 052309. DOI: 10.1103/PhysRevA.87.052309.

Mailloux2016 L. Mailloux, D. Hodson, M. Grimaila, R. Engle, C. Mclaughlin, and G. Baumgartner. “Using modeling and simulation to study photon number splitting attacks”. In: IEEE Access 4 (2016), pp. 2188–2197. DOI: 10.1109/ACCESS.2016.2555759.

Makarov2009 V. Makarov. “Controlling passively quenched single photon detectors by bright light”. In: New Journal of Physics 11 (2009), p. 065003. DOI: 10.1088/1367-2630/11/6/065003.

Makarov2006 V. Makarov, A. Anisimov, and J. Skaar. “Effects of detector efficiency mismatch on security of quantum cryptosystems”. In: Phys. Rev. A 74 (2006), p. 022313. DOI: 10.1103/PhysRevA.74.022313.

Makarov2016 V. Makarov, J. Bourgoin, P. Chaiwongkhot, M. Gagn, T. Jennewein, S. Kaiser, R. Kashyap, M. Legr, C. Minshull, and S. Sajeed. "Creation of backdoors in quantum communications via laser damage". In: Phys. Rev. A 94 (2016), 030302(R). DOI: 10.1103/PhysRevA.94.030302.

Makarov2005 V. Makarov and D. Hjelme. "Faked states attack on quantum cryptosystem". In: Journal of Modern Optics 52.5 (2005), pp. 691–705. DOI: 10.1080/09500340410001730986.

Makarov2008a V. Makarov and J. Skaar. "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols". In: Quant. Inf. Comp. 8 (2008), pp. 0622–0635.

Mao2020a Y. Mao, W. Huang, H. Zhong, Y. Wang, H. Qin, Y. Guo, and D. Huang. "Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution". In: New Journal of Physics 22.8 (2020). DOI: 10.1088/1367-2630/aba8d4.

Mao2020 Y. Mao, Y. Wang, W. Huang, H. Qin, D. Huang, and Y. Guo. "Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution". In: Phys. Rev. A 101.6 (2020), p. 062320. DOI: 10.1103/PhysRevA.101.062320.

Maroey2017 Ø. Marøy, V. Makarov, and J. Skaar. "Secure detection in quantum key distribution by real-time calibration of receiver". In: Quantum Sci. Technol. 2.4 (2017), p. 044013. DOI: 10.1088/2058-9565/aa83c9.

Meda2017 A. Meda, I. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese. "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution". In: Light Sci. Appl. 6 (2017), e16261. DOI: 10.1038/lsa.2016.261.

Meda2018 A. Meda, I. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese. "Quantum key distribution security threat: the backflash light case". In: Quantum Technologies 2018. Vol. 10674. 2018. DOI: 10.1117/12.2307704.

Metger2022 Tony Metger and Renato Renner. "Security of quantum key distribution from generalised entropy accumulation". In: (Mar. 2022). arXiv:2203.04993 [quant-ph]. DOI: 10.48550/arXiv.2203.04993. URL: http://arxiv.org/abs/2203.04993 (visited on 08/18/2023).

Mizutani2018 A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H. Lo, and K. Tamaki. "Quantum key distribution with setting-choice-independently correlated light sources". In: npj Quantum Information 5 (2019), p. 8. DOI: 10.1038/s41534-018-0122-y.

Molotkov2013 S. Molotkov. "On the quantum-mechanical bound on the loss of information through side channels in quantum cryptography". In: Jetp Lett. 97.10 (2013), pp. 604–610. DOI: 10.1134/S002136401310007X.

Molotkov2019a S. Molotkov. "Energy Conservation in Distributed Interference as a Guarantee for Detecting a Detector Blinding Attack in Quantum Cryptography". In: J. Exp. Theor. Phys. 128.1 (2019), pp. 45–51. DOI: 10.1134/S1063776119010151.

Molotkov2020c S. Molotkov. "On the Side Quantum-Classical Binary Channel of Information Leakage with Gaussian Noise". In: Jetp Lett. 111.9 (2020), pp. 506–511. DOI: 10.1134/S0021364020090088.

Molotkov2020a S. Molotkov. "Robustness of Quantum Cryptography Systems with Phase-Time Coding against Active Probing Attacks". In: J. Exp. Theor. Phys. 131.6 (2020), pp. 877–894. DOI: 10.1134/S1063776120110138.

Molotkov2020 S. Molotkov. “Trojan Horse Attacks, Decoy State Method, and Side Channels of Information Leakage in Quantum Cryptography”. In: J. Exp. Theor. Phys. 130.6 (2020), pp. 809–832. DOI: 10.1134/S1063776120050064.

Molotkov2020d S. Molotkov and K. Balygin. “Side channels of information leakage in quantum cryptography based on geometrically uniform coherent states”. In: Laser Physics 30.6 (2020). DOI: 10.1088/1555-6611/ab8298.

Molotkov2019 S. Molotkov, K. Balygin, A. Klimov, and S. Kulik. “Active sensing and side channels of information leakage in quantum cryptography”. In: Laser Physics 29.12 (2019), p. 124001. DOI: 10.1088/1555-6611/ab4bd9.

Nagamatsu2016 Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki. “Security of quantum key distribution with light sources that are not independently and identically distributed”. In: Phys. Rev. A 93 (2016), p. 042325. DOI: 10.1103/PhysRevA.93.042325.

Nasedkin2022 B. Nasedkin, F. Kiselev, I. Filipov, D. Tolochko, A. Ismagilov, V. Chistiakov, A. Gaidash, A. Tcypkin, A. Kozubov, and V. Egorov. “Quantum key distribution component loopholes in 1500-2100 nm range perspective for Trojan-horse attacks”. In: Preprint arXiv:2211.16815 (2022).

Nauerth2009 S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter. “Information leakage via side channels in freespace BB84 quantum cryptography”. In: New Journal of Physics 11.6 (2009), p. 065001. DOI: 10.1088/1367-2630/11/6/065001.

Navarrete2022 A. Navarrete and M. Curty. “Improved Finite-Key Security Analysis of Quantum Key Distribution Against Trojan-Horse Attacks”. In: Quantum Science and Technology 7.3 (2022), p. 035021. DOI: 10.1088/2058-9565/ac74dc.

Nikiforov2018 O. Nikiforov, A. Sauer, J. Schickel, A. Weber, G. Alber, H. Mantel, and T. Walther. “Side-Channel Analysis of Privacy Amplification in Postprocessing Software for a Quantum Key Distribution System”. In: Technical Report TUD-CS-2018-0024 (2018).

Pahali2022 M. Pahali, K. Durak, and U. Tefek. “Cryptographic security concerns on timestamp sharing via a public channel in quantum-key-distribution systems”. In: Phys. Rev. A 106.1 (2022). DOI: 10.1103/PhysRevA.106.012611.

Pan2020 Y. Pan, L. Zhang, and D. Huang. “Practical Security Bounds against Trojan Horse Attacks in Continuous-Variable Quantum Key Distribution”. In: Applied Sciences 10.21 (2020), p. 7788. DOI: 10.3390/app10217788.

Pang2020 X. Pang, A. Yang, C. Zhang, J. Dou, H. Li, J. Gao, and X. Jin. “Hacking Quantum Key Distribution via Injection Locking”. In: Phys. Rev. Appl. 13 (2020), p. 034008. DOI: 10.1103/PhysRevApplied.13.034008.

Park2020 D. Park, D. Heo, S. Kim, and S. Hong. “Single Trace Attack on Key Reconciliation Process for Quantum Key Distribution”. In: 2020, pp. 209–213. DOI: 10.1109/ICTC49870.2020.9289209.

Park2021 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”. In: ICT Express 7.1 (2021), pp. 36–40. DOI: 10.1016/j.icte.2021.01.013.

Peng2023 Qingquan Peng, Binwu Gao, Konstantin Zaitsev, Dongyang Wang, Jiangfang Ding, Yingwen Liu, Qin Liao, Ying Guo, Anqi Huang, and Junjie Wu. “Security boundaries of an optical power limiter for protecting quantum key distribution systems”. In: (2023). arXiv: 2303.12355 [quant-ph].

Pereira2022 M. Pereira, G. Currs-Lorenzo, . Navarrete, A. Mizutani, G. Kato, M. Curty, and K. Tamaki. "Modified BB84 quantum key distribution protocol robust to source imperfections". In: Preprint arXiv:2210.11754 (2022). DOI: 10.48550/arXiv.2210.11754.

Pereira2020 M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki. "Quantum key distribution with correlated sources". In: Science Advances 6.37 (2020), eaaz4487. DOI: DOI: 10.1126/sciadv.aaz4487.

Pinheiro2018 P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. Horn, J. Bourgoin, T. Jennewein, N. Ltkenhaus, and V. Makarov. "Eavesdropping and countermeasures for backflash side channel in quantum cryptography". In: Opt. Express 26.16 (2018), pp. 21020–21032. DOI: 10.1364/OE.26.021020.

Pirandola2015 S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. Braunstein, S. Lloyd, T. Gehring, C. Jacobsen, and U. Andersen. "High-rate measurement-device-independent quantum cryptography". In: Nature Photon 9 (2015), pp. 397–402. DOI: 10.1038/nphoton.2015.83.

Pirandola2020 Stefano Pirandola, Ulrik Lund Andersen, Luca Banchi, Mario Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. "Advances in quantum cryptography". In: Advances in Optics and Photonics 12.4 (2020), pp. 1012–1236. DOI: 10.1364/AOP.361502. URL: http://aop.osa.org/abstract.cfm?URI=aop-12-4-1012.

Ponosova2022 A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang. "Protecting fiber-optic quantum key distribution sources against light-injection attacks". In: PRX Quantum 3 (2022), p. 040307. DOI: 10.1103/PRXQuantum.3.040307.

Portmann2022 Christopher Portmann and Renato Renner. "Security in quantum cryptography". In: Rev. Mod. Phys. 94 (2 June 2022), p. 025008. DOI: 10.1103/RevModPhys.94.025008. URL: https://link.aps.org/doi/10.1103/RevModPhys.94.025008.

Qi2007 B. Qi, C. Fung, H. Lo, and X. Ma. "Time-shift attack in practical quantum cryptosystems". In: Quant. Inf. Comp. 7 (2007), pp. 073–082. DOI: 10.26421/QIC7.1-2-3.

Qi2015 Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. "Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection". In: Physical Review X 5.4 (Oct. 2015). arXiv: 1503.00662, p. 041009. ISSN: 2160-3308. DOI: 10.1103/PhysRevX.5.041009. URL: https://link.aps.org/doi/10.1103/PhysRevX.5.041009.

Qian2018 Y. Qian, D. He, S. Wang, W. Chen, Z. Yin, G. Guo, and Z. Han. "Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors". In: Phys. Rev. Appl. 10 (2018), p. 064062. DOI: 10.1103/PhysRevApplied.10.064062.

Qian2019 Y. Qian, D. He, S. Wang, W. Chen, Z. Yin, G. Guo, and Z. Han. "Robust countermeasure against detector control attack in a practical quantum key distribution system". In: Optica 6.9 (2019), pp. 1178–1184. DOI: 10.1364/OPTICA.6.001178.

Qian2020 Y. Qian, D. He, S. Wang, W. Chen, Z. Yin, G. Guo, and Z. Han. "Erratum: Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors [Phys. Rev. Applied 10, 064062 (2018)]". In: Phys. Rev. Appl. 13 (2020), p. 039901. DOI: 10.1103/PhysRevApplied.13.039901.

Qin2016 H. Qin, R. Kumar, and R. Allaume. "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution". In: Phys. Rev. A 94 (2016), p. 012325. DOI: 10.1103/PhysRevA.94.012325.

Qin2018 H. Qin, R. Kumar, V. Makarov, and R. Alléaume. "Homodyne-detector-blinding attack in continuous-variable quantum key distribution". In: Phys. Rev. A 98 (2018), p. 012312. DOI: 10.1103/PhysRevA.98.012312.

Qin2013 Hao Qin, Rupesh Kumar, and Romain Alléaume. "Saturation attack on continuous-variable quantum key distribution system". In: ed. by Edward M. Carapezza, Keith L. Lewis, Richard C. Hollins, Thomas J. Merlet, Mark T. Gruneisen, Miloslav Dusek, and John G. Rarity. Vol. 8899. International Society for Optics and Photonics. SPIE Security + Defence, 2013, 88990N. DOI: 10.1117/12.2028543.

BSI-quantum_safe "Quantum-safe cryptography – fundamentals, current developments and recommendations". In: Federal Office for Information Security (Oct. 2021). URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=132646.

Rau2015 M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter. "Spatial Mode Side Channels in Free-Space QKD Implementations". In: IEEE Journal of Selected Topics in Quantum Electronics 21 (2015), pp. 187–191. DOI: 10.1109/JSTQE.2014.2372008.

Ren2019a S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White. "Noise and Security Analysis of Trusted Phase Noise Continuous Variable Quantum Key Distribution using a Local Local Oscillator". In: 2019. DOI: 10.1109/SPAWC.2019.8815501.

Ren2019 S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White. "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise". In: J. Opt. Soc. Am. B 36.3 (2019), B7–B15. DOI: 10.1364/JOSAB.36.0000B7.

Zbinden2000 Grégoire Ribordy, Jean-Daniel Gautier, Nicolas Gisin, Olivier Guinnard, and Hugo Zbinden. "Fast and user-friendly quantum key distribution". In: Journal of Modern Optics 47.2-3 (Feb. 2000), pp. 517–531. ISSN: 0950-0340. DOI: 10.1080/09500340008244057. URL: https://www.tandfonline.com/doi/abs/10.1080/09500340008244057 (visited on 06/12/2023).

Roberts2018 G. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields. "Patterning-effect-free intensity modulator for secure decoy-state quantum key distribution". In: Optics Letters 43.20 (2018), pp. 5110–5113. DOI: 10.1364/OL.43.005110.

Rogers2007 D. Rogers, J. Bienfang, A. Nakassis, H. Xu, and C. Clark. "Detector dead-time effects and paralyzability in high-speed quantum key distribution". In: New J. Phys. 9 (2007), p. 319. DOI: 10.1088/1367-2630/9/9/319.

Sagar2022 J. Sagar, E. Hastings, P. Zhang, M. Stefko, D. Lowndes, D. Oi, J. Rarity, and S. Joshi. "Design and test of optical payload for polarization encoded QKD for Nanosatellites". In: Preprint arXiv:2211.10814 (2022). DOI: 10.48550/arXiv.2211.10814.

Sajeed2015a S. Sajeed, P. Chaiwongkhot, J. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov. "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch". In: Phys. Rev. A 91 (2015), p. 062301. DOI: 10.1103/PhysRevA.91.062301.

Sajeed2017 S. Sajeed, C. Minshull, N. Jain, and V. Makarov. "Invisible Trojan-horse attack". In: Scientific Reports 7 (2017), p. 8403. DOI: 10.1038/s41598-017-08279-1.

Sajeed2015 S. Sajeed, I. Radchenko, S. Kaiser, J. Bourgoin, A. Pappa, L. Monat, M. Legr, and V. Makarov. "Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing". In: Phys. Rev. A 91 (2015), p. 032326. DOI: 10.1103/PhysRevA.91.032326.

Sauge2011 S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. “Controlling an actively-quenched single photon detector with bright light”. In: Opt. Express 19.23 (2011), pp. 23590–23600. DOI: 10.1364/OE.19.023590.

Scarani2004 V. Scarani, A. Acn, G. Ribordy, and N. Gisin. “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”. In: Phys. Rev. Lett. 92 (2004), p. 057901. DOI: 10.1103/PhysRevLett.92.057901.

Scarani2009 Valerio Scarani, Helle Bechmann-Pasquinucci, N. Cerf, Miloslav Dušek, N. Lütkenhaus, and Momtchil Peev. “The security of practical quantum key distribution”. In: Reviews of Modern Physics 81.3 (2009), pp. 1301–1350. ISSN: 0034-6861. DOI: 10.1103/RevModPhys.81.1301. URL: http://link.aps.org/doi/10.1103/RevModPhys.81.1301.

Shao2022 Y. Shao, Y. Li, H. Wang, Y. Pan, Y. Pi, Y. Zhang, W. Huang, and B. Xu. “Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator”. In: Phys. Rev. A 105 (2022), p. 032601. DOI: 10.1103/PhysRevA.105.032601.

Shen2022 Lijiong Shen and Christian Kurtsiefer. “Countering detector manipulation attacks in quantum communication through detector self-testing”. In: (2022). arXiv: 2204.06155 [quant-ph].

Shi2017 Y. Shi, J. Lim, H. Poh, P. Tan, P. Tan, A. Ling, and C. Kurtsiefer. “Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes”. In: Opt. Express 25 (2017), pp. 30388–30394. DOI: 10.1364/OE.25.030388.

Silva2015 T. da Silva, G. do Amaral, G. Xavier, G. Temporo, and J. von der Weid. “Safeguarding Quantum Key Distribution Through Detection Randomization”. In: IEEE Journal of Selected Topics in Quantum Electronics 21.3 (2015), pp. 159–167. DOI: doi:10.1109/JSTQE.2014.2361793.

Silva2012 T. da Silva, G. Xavier, G. Temporo, and J. von der Weid. “Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems”. In: Opt. Express 20.17 (2012), pp. 18911–18924. DOI: 10.1364/OE.20.018911.

Sixto2023 Xoel Sixto, Guillermo Currás-Lorenzo, Kiyoshi Tamaki, and Marcos Curty. “Secret key rate bounds for quantum key distribution with non-uniform phase randomization”. In: (2023). arXiv: 2304.03562 [quant-ph].

Soh2015 Daniel B S Soh, Constantin Brif, Patrick J. Coles, Norbert Luetkenhaus, Ryan M. Camacho, Junji Urayama, and Mohan Sarovar. “Self-referenced continuous-variable quantum key distribution protocol”. In: Physical Review X 5.4 (2015). arXiv: 1503.04763, pp. 1–15. ISSN: 21603308. DOI: 10.1103/PhysRevX.5.041010.

Stiller2015 B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, E. Diamanti, C. Marquardt, and G. Leuchs. “Quantum hacking of continuous-variable quantum key distribution systems: realtime Trojan-horse attacks”. In: CLEO: 2015. 2015, FF1A.7. DOI: 10.1364/CLEO_QELS.2015.FF1A.7.

Sun2014a Q. Sun, W. Wang, Y. Liu, F. Zhou, J. Pelc, M. Fejer, C. Peng, X. Chen, X. Ma, Q. Zhang, and J. Pan. “Experimental passive decoy-state quantum key distribution”. In: Laser Physics Letters 11.8 (2014). DOI: 10.1088/1612-2011/11/8/085202.

Sun2012 S. Sun, M. Gao, M. Jiang, C. Li, and L. Liang. “Partially random phase attack to the practical two-way quantum-key-distribution system”. In: Phys. Rev. A 85 (2012), p. 032304. DOI: 10.1103/PhysRevA.85.032304.

Sun2011 S. Sun, M. Jiang, and L. Liang. “Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system”. In: Phys. Rev. A 83 (2011), p. 062331. DOI: 10.1103/PhysRevA.83.062331.

Sun2014 S. Sun, M. Jiang, X. Ma, C. Li, and L. Liang. “Hacking on decoy-state quantum key distribution system with partial phase randomization”. In: Scientific Reports 4 (2014), p. 4759. DOI: 10.1038/srep04759.

Sun2021 S. Sun and F. Xu. “Security of quantum key distribution with source and detection imperfections”. In: New Journal of Physics 23 (2021), p. 023011. DOI: 10.1088/1367-2630/abdf9b.

Sun2015a S. Sun, F. Xu, M. Jiang, X. Ma, H. Lo, and L. Liang. “Effect of source tampering in the security of quantum cryptography”. In: Phys. Rev. A 92 (2015), p. 022304. DOI: 10.1103/PhysRevA.92.022304.

Sun2018 S.-H. Sun, M.-S. Jiang, X.-C. Ma, C.-Y. Li, and L.-M. Liang. “Retraction Note: Hacking on decoy-state quantum key distribution system with partial phase randomization”. In: Scientific Reports (2018). DOI: https://doi.org/10.1038/srep46943.

Sych2021 D. Sych, A. Duplinskiy, and D. Babukhin. “Practical security of quantum key distribution in the presence of side channels”. In: Journal of Physics: Conference Series 1984 (2021), p. 012001. DOI: 10.1088/1742-6596/1984/1/012001.

Tamaki2014 K. Tamaki, M. Curty, G. Kato, H. Lo, and K. Azuma. “Loss-tolerant quantum cryptography with imperfect sources”. In: Phys. Rev. A 90 (2014), p. 052314. DOI: 10.1103/PhysRevA.90.052314.

Tamaki2016 K. Tamaki, M. Curty, and M. Lucamarini. “Decoy-state quantum key distribution with a leaky source”. In: New Journal of Physics 18 (2016), p. 065008. DOI: 10.1088/1367-2630/18/6/065008.

Tamaki2009 K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe. “Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse”. In: Phys. Rev. A 80 (2009), p. 032302. DOI: 10.1103/PhysRevA.80.032302.

Tan2022 H. Tan, W. Zhang, L. Zhang, W. Li, S. Liao, and F. Xu. “External magnetic effect for the security of practical quantum key distribution”. In: Quantum Science and Technology 7.4 (2022). DOI: 10.1088/2058-9565/ac7d07.

Tan2021a Hao Tan, Wei Li, Likang Zhang, Kejin Wei, and Feihu Xu. “Chip-Based Quantum Key Distribution against Trojan-Horse Attack”. In: Phys. Rev. Appl. 15 (6 June 2021), p. 064038. DOI: 10.1103/PhysRevApplied.15.064038. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.15.064038.

Tan2021 X. Tan, Y. Guo, L. Zhang, J. Huang, J. Shi, and D. Huang. “Wavelength attack on atmospheric continuous-variable quantum key distribution”. In: Phys. Rev. A 103.1 (2021). DOI: 10.1103/PhysRevA.103.012417.

Tan2016 Y. Tan. “Quantum key distribution with prepare-and-measure Bell test”. In: Scientific Reports 6 (2016). DOI: 10.1038/srep35032.

Tang2013a Y. Tang, H. Yin, X. Ma, C. Fung, Y. Liu, H. Yong, T. Chen, C. Peng, Z. Chen, and J. Pan. “Source attack of decoy-state quantum key distribution using phase information”. In: Phys. Rev. A 88 (2013), p. 022308. DOI: 10.1103/PhysRevA.88.022308.

Tanner2014 M. Tanner, V. Makarov, and R. Hadfield. “Optimised quantum hacking of superconducting nanowire single-photon detectors”. In: Opt. Express 22.6 (2014), pp. 6734–6748. DOI: 10.1364/OE.22.006734.

Trushechkin2022 A. Trushechkin. “Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case”. In: Quantum 6 (2022), p. 771. DOI: 10.22331/q-2022-07-22-771.

Vakhitov2001 A. Vakhitov, V. Makarov, and D. Hjelme. “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography”. In: Journal of Modern Optics 48.13 (2001), pp. 2023–2038. DOI: 10.1080/09500340108240904.

Vinay2018 S. Vinay and P. Kok. “Burning the Trojan Horse: Defending against Side-Channel Attacks in QKD”. In: Phys. Rev. A 97 (2018), p. 042335. DOI: 10.1103/PhysRevA.97.042335.

Wang2020 F. Wang, J. Wu, W. Chen, S. Wang, D. He, Z. Yin, C. Zou, G. Guo, and Z. Han. “Quantum hacking perceiving for quantum key distribution using temporal ghost imaging”. In: Phys. Rev. Applie (2020). DOI: 10.1103/PhysRevApplied.15.034051.

Wang2013 W. Wang, M. Gao, and Z. Ma. “Effect of imperfect Faraday mirrors on the security of a Faraday-Michelson quantum cryptography system”. In: J. Phys. A: Math. Theor. 46 (2013), p. 455301. DOI: 10.1088/1751-8113/46/45/455301.

Wang2020a W. Wang, K. Tamaki, and M. Curty. “Measurement-Device-Independent Quantum Key Distribution with Leaky Sources”. In: Scientific Reports 11 (2021), p. 1678. DOI: 10.1038/s41598-021-81003-2.

Wang2022 W. Wang, R. Wang, V. Zapatero, L. Qian, B. Qi, M. Curty, and H. Lo. “Fully-Passive Quantum Key Distribution”. In: Preprint arXiv:2207.05916 (2022). DOI: 10.48550/arXiv.2207.05916.

Wang2018b Weilong Wang, Kiyoshi Tamaki, and Marcos Curty. “Finite-key security analysis for quantum key distribution with leaky sources”. en. In: New Journal of Physics 20.8 (Aug. 2018). Publisher: IOP Publishing, p. 083027. ISSN: 1367-2630. DOI: 10.1088/1367-2630/aad839. URL: https://dx.doi.org/10.1088/1367-2630/aad839 (visited on 06/12/2023).

Wang2005 X. Wang. “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography”. In: Phys. Rev. Lett. 94 (2005), p. 230503. DOI: 10.1103/PhysRevLett.94.230503.

Wang2008 Xiang-Bin Wang, Cheng-Zhi Peng, Jun Zhang, Lin Yang, and Jian-Wei Pan. “General theory of decoy-state quantum cryptography with source errors”. In: Phys. Rev. A 77 (4 Apr. 2008), p. 042311. DOI: 10.1103/PhysRevA.77.042311. URL: https://link.aps.org/doi/10.1103/PhysRevA.77.042311.

Wang2018c Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu. “Twin-field quantum key distribution with large misalignment error”. In: Phys. Rev. A 98 (6 Dec. 2018), p. 062323. DOI: 10.1103/PhysRevA.98.062323. URL: https://link.aps.org/doi/10.1103/PhysRevA.98.062323.

Weber2021 A. Weber, O. Nikiforov, A. Sauer, J. Schickel, G. Alber, H. Mantel, and T. Walther. “Cache-Side-Channel Quantification and Mitigation for Quantum Cryptography”. In: Computer Security - ESORICS 2021. Vol. 12973. 2021, pp. 235–256. DOI: 10.1007/978-3-030-88428-4_12.

Wegman1981 Mark N. Wegman and J.Lawrence Carter. “New hash functions and their use in authentication and set equality”. In: Journal of Computer and System Sciences 22.3 (1981), pp. 265–279. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(81)90033-7. URL: https://www.sciencedirect.com/science/article/pii/0022000081900337.

Wei2019a K. Wei, W. Zhang, Y. Tang, L. You, and F. Xu. “Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch”. In: Phys. Rev. A 100 (2019), p. 022325. DOI: 10.1103/PhysRevA.100.022325.

Weier2011 H. Weier, H. Krauss, M. Rau, M. Frst, S. Nauerth, and H. Weinfurter. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors". In: New Journal of Physics 13 (2011), p. 073024. DOI: 10.1088/1367-2630/13/7/073024.

Wiechers2011 C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. "After-gate attack on a quantum cryptosystem". In: New Journal of Physics 13 (2011), p. 013043. DOI: 10.1088/1367-2630/13/1/013043.

Wittmann2010 C. Wittmann, J. Fürst, C. Wiechers, D. Elser, H. Häseler, N. Lütkenhaus, and G. Leuchs. "Witnessing effective entanglement over a 2 km fiber channel". In: Opt. Express 18.5 (2010), pp. 4499–4509. DOI: 10.1364/OE.18.004499.

Wu2020 Z. Wu, A. Huang, H. Chen, S. Sun, J. Ding, X. Qiang, X. Fu, P. Xu, and J. Wu. "Hacking single-photon avalanche detector in quantum key distribution via pulse illumination". In: Opt. Express 28.17 (2020), pp. 25574–25590. DOI: 10.1364/OE.397962.

Wu2020b Z. Wu, A. Huang, X. Qiang, J. Ding, P. Xu, X. Fu, and J. Wu. "Robust countermeasure against detector control attack in a practical quantum key distribution system: comment". In: Optica 7.10 (2020), pp. 1391–1393. DOI: 10.1364/OPTICA.391325.

Xu2010 F. Xu, B. Qi, and H. Lo. "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system". In: New Journal of Physics 12 (2010), p. 113026. DOI: 10.1088/1367-2630/12/11/113026.

Xu2020 Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. "Secure quantum key distribution with realistic devices". In: Rev. Mod. Phys. 92 (2 May 2020), p. 025002. DOI: 10.1103/RevModPhys.92.025002. URL: https://link.aps.org/doi/10.1103/RevModPhys.92.025002.

Xu2006 H. Xu, L. Ma, J. Bienfang, and X. Tang. "Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems". In: CLEO (2006). DOI: 10.1109/CLEO.2006.4628713.

Xu2020a Hai Xu, Zong-Wen Yu, Cong Jiang, Xiao-Long Hu, and Xiang-Bin Wang. "Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate". In: Phys. Rev. A 101 (4 Apr. 2020), p. 042330. DOI: 10.1103/PhysRevA.101.042330. URL: https://link.aps.org/doi/10.1103/PhysRevA.101.042330.

Xu2022 S. Xu, Y. Li, Y. Mao, and Y. Guo. "Counteracting a Saturation Attack in Continuous-Variable Quantum Key Distribution Using an Adjustable Optical Filter Embedded in Homodyne Detector". In: Entropy 24.3 (2022), p. 383. DOI: 10.3390/e24030383.

Ye2020a M. Ye, J. Li, Y. Wang, P. Gao, X. Lu, and Y. Qian. "Quantum key distribution system against the probabilistic faint after-gate attack". In: Communications in Theoretical Physics 72.11 (2020). DOI: 10.1088/1572-9494/abb7d8.

Yoshino2018 K. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita. "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses". In: npj Quantum Information 4 (2018), p. 8. DOI: 10.1038/s41534-017-0057-8.

Yu2022 K. Yu, C. Zhang, X. Zhou, and Q. Wang. "Performance of passive decoy-state quantum key distribution with mismatched local detectors". In: Commun. Theor. Phys. 74.1 (2022). DOI: 10.1088/1572-9494/ac450d.

Yuan2010 Z. Yuan, J. Dynes, and A. Shields. "Avoiding the blinding attack in QKD". In: Nature Photon 4 (2010), pp. 800–801. DOI: 10.1038/nphoton.2010.269.

Yuan2011 Z. Yuan, J. Dynes, and A. Shields. "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography". In: Appl. Phys. Lett. 98 (2011), p. 231104. DOI: 10.1063/1.3597221.

Yuan2011a Z. Yuan, J. Dynes, and A. Shields. "Response to Comment on Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography [Appl. Phys. Lett. 99, 196101 (2011)]". In: Appl. Phys. Lett. 99 (2011), p. 196102. DOI: 10.1063/1.3658807.

Yuan2007 Z. L. Yuan, A. W. Sharpe, and A. J. Shields. "Unconditionally secure one-way quantum key distribution using decoy pulses". In: Applied Physics Letters 90.1 (Jan. 2007), p. 011118. ISSN: 0003-6951. DOI: 10.1063/1.2430685. eprint: https://pubs.aip.org/aip/apl/article-pdf/doi/10.1063/1.2430685/7851301/011118_1_online.pdf. URL: https://doi.org/10.1063/1.2430685.

Zapatero2021 V. Zapatero and M. Curty. "Secure quantum key distribution with a subset of malicious devices". In: npj Quantum Information 7 (2021), p. 26. DOI: 10.1038/s41534-020-00358-y.

Zapatero2021a V. Zapatero, . Navarrete, K. Tamaki, and M. Curty. "Security of quantum key distribution with intensity correlations". In: Quantum 5 (2021), p. 602. DOI: 10.22331/q-2021-12-07-602.

Zapatero2023 Víctor Zapatero, Wenyuan Wang, and Marcos Curty. "A fully passive transmitter for decoy-state quantum key distribution". In: Quantum Science and Technology 8.2 (Feb. 2023), p. 025014. DOI: 10.1088/2058-9565/acbc46. URL: https://dx.doi.org/10.1088/2058-9565/acbc46.

Zhang2021 G. Zhang, I. Primaatmaja, J. Haw, X. Gong, C. Wang, and C. Lim. "Securing practical quantum communication systems with optical power limiters". In: PRX Quantum 2 (2021), p. 030304. DOI: 10.1103/PRXQuantum.2.030304.

Zhang2022a X. Zhang, M. Jiang, Y. Wang, Y. Lu, H. Li, C. Zhou, Y. Zhou, and W. Bao. "Analysis of an injection-locking-loophole attack from an external source for quantum key distribution". In: Phys. Rev. A 106.6 (2022). DOI: 10.1103/PhysRevA.106.062412.

Zhang2021a Y. Zhang, P. Coles, A. Winick, J. Lin, and N. Lutkenhaus. "Security proof of practical quantum key distribution with detection-efficiency mismatch". In: Phys. Rev. Research 3 (2021), p. 013076. DOI: 10.1103/PhysRevResearch.3.013076.

Zhao2008 Y. Zhao, C. Fung, B. Qi, C. Chen, and H. Lo. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems". In: Phys. Rev. A 78 (2008), p. 042333. DOI: 10.1103/PhysRevA.78.042333.

Zhao2008a Y. Zhao, B. Qi, and H. Lo. "Quantum key distribution with an unknown and untrusted source". In: Phys. Rev. A 77 (2008), p. 052327. DOI: 10.1103/PhysRevA.77.052327.

Zhao2010 Y. Zhao, B. Qi, H. Lo, and L. Qian. "Security analysis of an untrusted source for quantum key distribution: passive approach". In: New Journal of Physics 12 (2010), p. 023024. DOI: 10.1088/1367-2630/12/2/023024.

Zhao2018 Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo. "Polarization attack on continuous-variable quantum key distribution". In: Journal of Physics B 52.1 (2018), p. 015501. DOI: 10.1088/1361-6455/aaf0b7.

Zhao2007 Yi Zhao, Bing Qi, and Hoi-Kwong Lo. “Experimental quantum key distribution with active phase randomization”. In: Applied Physics Letters 90.4 (Jan. 2007), p. 044106. ISSN: 0003-6951. DOI: 10.1063/1.2432296. eprint: https://pubs.aip.org/aip/apl/article-pdf/doi/10.1063/1.2432296/14364393/044106_1_online.pdf. URL: https://doi.org/10.1063/1.2432296.

Zheng2019 Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng. “Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack”. In: Opt. Express 27.19 (2019), pp. 27369–27384. DOI: 10.1364/OE.27.027369.

Zheng2020 Y. Zheng, W. Liu, Z. Cao, and J. Peng. “Monitoring scheme against local oscillator attacks for practical continuous-variable quantum-key-distribution systems in complex communication environments”. In: Phys. Rev. A 101.2 (2020). DOI: 10.1103/PhysRevA.101.022319.

Zheng2021 Y. Zheng, H. Shi, W. Pan, Q. Wang, and J. Mao. “Quantum Hacking on an Integrated Continuous-Variable Quantum Key Distribution System via Power Analysis”. In: Entropy 23.2 (2021). DOI: 10.3390/e23020176.