Toward standardization of Quantum Key Distribution

by

Poompong Chaiwongkhot

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2020

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Bing Qi (Research Scientist, Oak Ridge National Laboratory)
Supervisor(s):	Thomas Jennewein Professor, Dept. of Physics and Astronomy, University of Waterloo Norbert Lütkenhaus Professor, Dept. of Physics and Astronomy, University of Waterloo
Internal Member:	Kyung Soo Choi Professor, Dept. of Physics and Astronomy, University of Waterloo
Internal-External Member:	Michal Bajcsy Associate Professor, Dept. of Electrical and Computer Engineering, University of Waterloo
Other Member(s):	Michele Mosca Professor, Dept. of Combinatoric and Optimization, University of Waterloo

Author's declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Information security becomes an inseparable part of our everyday life. An encryption method widely used today is public-key encryption. The security of this method is based on a hard to solve mathematical problems against an adversary with limited computational power. Such an assumption could be broken as our understanding of the mathematics being improved or new computation tools being developed. One such tool that poses a threat to the public key encryption is a quantum computer. As a result, a new encryption method with a new security assumption is required.

Quantum key distribution is a point-to-point symmetric key distribution method with security based on the law of physics. In theory, the key generated by QKD is information-theoretic secured. However, in practice, physical devices could have flaws or possess some behaviors deviated from the theoretical model. These imperfections could open security loopholes for an adversary to exploit, compromising the security. Thus the security verification and system characterization of practical implementation of QKD are necessary. The necessity of this verification is further emphasized as several QKD systems are being commercialized and used in several discrete communication links today.

To extend this new encryption system's practical implementation on a wider network scale requires a set of standards or common practices for developers and service providers to follow. This set of rules is set to ensure the compatibility of different device models in the network and ensure the security of each component in the system, which would affect the security of the system as a whole.

To fulfill standardization and certification criteria, a record of best practice on security analysis, system design, device characterization, and security verification of QKD implementation is required. The research projects throughout my Ph.D. study contribute toward this practice. These studies also address some issues and provide possible solutions to the development of a standard for QKD. This thesis is a collection of six experimental studies on performance evaluation and security verification of different components of practical quantum key distribution systems.

The first study is a comparison between the performance of the QKD system with quantum dot (QD) as a single-photon source and the performance of QKD with weak-coherent pulsed (WCP) source. The result shows that the QKD with QD could generate the key at higher channel loss than WCP QKD using the same laser source. This result shows the potential of QKD with a single-photon source as a candidate for secret key distribution over high channel loss, such as up-link satellite-based QKD.

The second study is a theoretical study on the method to characterize the QKD system against the Trojan-horse attack being considered as a standard for the QKD system. The result shows a possible loophole of this method against a more powerful adversary than assumed in the previously proposed model. An improved version of characterization against a more general form of Trojan-horse attack has been proposed.

The third experiment is on the information leakage from a free-space QKD receiver due to detector backflash, a photon produced by the detector upon detection. The result shows that the backflash photons carry the information of the 'clicked' detector that could be transmitted back to the channel and discriminated by Eve. An experimental demonstration of this attack has been performed. Countermeasure both in theory and practical setup has been proposed.

The next experiment is on the effect of atmospheric turbulence on Eve's spatial-mode detection efficiency mismatch attack on the free-space QKD system. We show that, by using a phase-only spatial light modulator (SLM) and hologram created by Zernike polynomials, atmospheric turbulence with various strength covered from sea level to upper atmosphere can be experimentally emulated in the lab environment. We then use that setup to show the limit of the distance that Eve's attack is successful. The theoretical limit of the attack distance also shown.

In the fifth study, we use the SLM and Zernike polynomial holograms to characterize a free-space QKD system against spatial mode attack. The result shows that, with higher-order spatial modes and finer control of wavefront intensity distribution, Eve could bypass the countermeasure proposed in our previous study. We proposed a more robust version of countermeasure against spatial mode attack. The new countermeasure is verified by the SLM setup.

The last study is on the fake-state attack on the transition edge sensor (TES). The result shows that TES's voltage response can be deterministically controlled by Eve using bright laser through the input channel. It also shows that the photon number result from TES can be controlled by Eve. An attack model exploiting this imperfection has been shown.

In addition to the contribution to the standardization of the QKD system, I hope that the result of this thesis would emphasize the necessity of security verification of the QKD system and the verification of countermeasure and characterization method against more general attack model. Although the unconditional security, promised in theory, could not yet be achieved, this loop of hacking and patching should provide us information and insight on which security level could be claimed from the practical QKD devices implementing today.

Acknowledgements

I would like to thank my supervisors Thomas Jennewein, Vadim Makarov, and Norbert Lütkenhaus for their helpful advice and their patience in introducing me to both theoretical and practical aspects of QKD and beyond. I would like to thank all present and past members of the quantum hacking lab and quantum photonics lab, especially Shihan Sajeed, Katanya Kuntz, Hao Qin, and Anqi Huang for all constructive debates, discussions, and assistance in my research. Thanks to Jia Lin, Brendon Higgins, and Jean-Philippe Bourgoin for their assistance, advice, and suggestions on theory and experimental setup. Thanks to all collaborators around the world for being great hosts and provide fantastic research experiences.

Thanks to my parents and my family, who encouraged and provided mental support throughout the study. Thanks to DPST scholarship, Institute for Quantum Computing (IQC) and Cryptoworks21 for materials and financial support. Finally, Thanks to all IQC members and the University of Waterloo Thai Student Association (UW-TSA) members, who provide a friendly and supportive environment that made my life here be much more than studies and research. Thanks to all Quantum Technology Foundation, Thailand (QTFT) members for all support, and friendly thought-inducing discussions. Thanks to Waterloo table-top gaming community and all online gaming communities around the world for help making my free-time more enjoyable and harsh time not so hard to bear.

Dedication

For our understanding...

Table of Contents

List of Figures

List of Tables

Abbreviations

APD Avalanche photo diode 19

BB84 Bennett-Brassard 1984 5

PMT Photon multiplier tube 19

PNS Photon number splitting attack 9

QD Quantum dots 3

QKD Quantum key distribution 2

RSA Rivest–Shamir–Adleman protocol 1

SLM spatial-light modulator 56

SNSPD Superconducting nanowire single-photon detector 19

TES Transition edge sensor 19, 79

WCP Weak coherent pulsed laser 9

Chapter 1

Introduction

The word cryptography (derived from the Greek words 'cryptos' means hidden or secret, and 'graphei' means write) is a study of methods to secure the communication between legitimate parties –often called Alice and Bob– against an adversary –often called eavesdropper or Eve. As secure communication becomes an inseparable part of our daily life, the importance of the development of cryptosystems and the understanding of its counterpart, cryptanalytic, the study of analyzing ciphertext and decipher the encrypted data by the third party is undeniable.

Modern cryptography assumes that an adversary is familiar with all the devices used in the cryptosystem and has full knowledge of the protocol – the processes used to generate and distribute the key. This assumption is also known as Kerckhoffs's principle [68]. Eve also knows all the possible messages and ciphertext that might be sent. Today's secure communication protocols often rely on "presumably" hard-to-solve mathematical problems. For instance, the ubiquitous public key distribution protocol known as Rivest–Shamir–Adleman protocol (RSA) [132] utilizes the multiplication of two large prime numbers to exchange the secret key between two parties. The security of this protocol, which prevents fast decryption, is based on the assumption that it is incredibly difficult, for today's computer to solve using the best-known algorithm within the lifetime of the encrypted message, to find the two large prime numbers (factorization) given the multiplication result. However, this scheme may fail if solutions to relevant mathematical problems arise, either via a faster decryption algorithm or via new technologies and tools that offer new ways to solve problems. The encryption method relied on the assumption of hard-to-solve problems are often called classical cryptography.

An emerging quantum technology that can potentially solve many hard mathematical

problems is a scalable quantum computer. Peter Shor has shown theoretically that, if a scalable quantum computer can be built, it can crack the factorization problem exponentially faster than today's best classical computer [146]. To ensure secure transmission protocols in the quantum era, the field of Quantum-safe Cryptography emerged.

Quantum-safe cryptography is a collective term for the study of cryptographic tools that are safe against the computation power of quantum computers and quantum algorithms. There are two main approaches to achieve this new security level, namely post-quantum cryptography and quantum cryptography.

Post-quantum cryptography (the name means classical cryptography after quantum computer emerged) focused on finding new protocols mathematical problems that are hard-to-solve for quantum computers and known quantum algorithms. This approach has an advantage that the protocols are relatively easy to implement without retooling existing classical communication infrastructure. However, their reliance on the hard-to-solve problem could not guarantee long term security. As new technology emerged and our understanding of the quantum algorithm developed.

Quantum cryptography (the name means cryptography based on the law of quantum mechanics), on the other hand, is a study of secure communication where its security based on the law of physics and mathematical proof, which is almost impossible to defy or break. One of the most well-studied topics in this field is Quantum key distribution (QKD), which focuses on secure generation and distribution of symmetric secret key–a secret identical random bit string between parties.

QKD has been developed rapidly over the past decades. It is one of the quantum technology that has reached the point of practical use and commercialization. To guarantee security across various devices models and platform, several drafts of international standardization and certification of a practical QKD system is being developed and proposed by various organizations around the world. Toward that goal of standardized security of QKD implementation, it is essential to include the latest understanding from theoretical security analysis, as well as best practices from a practical implementation point of view.

This thesis is a record of a series of experiments and security verification on QKD systems throughout my Ph.D. study. This thesis is structured in a hope to provide the readers a broad scope of QKD system development, from the practical implementation point of view, from comparing advantages and disadvantages of different choices of QKD protocols, to improvement device characterization methods, to series of security verification of QKD system. These records could be used in the standardization documents on the practical implementation of QKD being developed. Lastly, we will discuss a practice and criteria introduced for security auditing, where the physical implementation of the QKD

systems that have passed the security statement and standardization certification criteria being scrutinized for possible leftover loopholes and vulnerabilities.

The content of this thesis is divided as follows. In Chapter 2, we discuss the security of secure communication from the formal definition of secure communication to the security proof of QKD protocols. The following chapters are a record of experiments on QKD systems that provide insight on the development of the QKD system, from protocol's performance evaluation to developing and improvement of QKD devices characterization method, to security verification of QKD systems. Chapter III present a study of the Quantum dots (QD) as a single-photon source and its performance compared with conventional weak coherent pulsed QKD protocol. Chapter IV is a study on a standardization proposal for device characterization as a countermeasure against the Trojan horse attack. We propose an improvement of the characterization procedure to take into account a more powerful variant of the attack, which was not included in the original proposal.

Chapter 2

Security of secret communication

This chapter will provide a formal definition, framework and tools to understanding the security of QKD. In this scenario the two legitimate parties Alice and Bob would like to communicate secretly, while Eve would like to eavesdrop the conversation.

2.1 Security of cryptosystem

The security of a cryptosystem is defined as follows [1]

Let $\mathcal{M}$ be a set of all possible messages, $\mathcal{C}$ is a set of all possible cryptogram or encrypted messages which might be transmitted through the public channel. A cryptosystem is perfectly secure if

$$p(M) = p(M|C) \quad \forall M \in \mathcal{M} \quad and \quad \forall C \in \mathcal{C} \tag{2.1}$$

where $p(M)$ is a priori probability distribution of message and $p(M|C)$ is a posterioi probability distribution of the message as viewed by Eve after learning about C.

In other words, Eve does not gain additional information about the message from the cryptogram. This secure communication can be achieved with an encryption scheme called one-time pad. [145]

The one-time pad is a scheme in which two parties – often called Alice and Bob – encrypt and decrypt the message using a shared secret key. Without loss of generality, the set of messages $\mathcal{M}$ can be defined as a binary string of length m, $\mathcal{M} = \{0,1\}^{\oplus m}$ and the set

[1] The following contents in this section are summarized from [105, 11, 89].

of all possible keys $\mathcal{K} = \{0,1\}^{\oplus m}$ where the key K was picked randomly with probability $p(K) = \frac{1}{2^m}$. The one-time-pad scheme works as follows:

Alice and Bob exchange the key K beforehand, in secret.

Alice obtains the encrypted message C by the message by performing bit-wise XOR between message M and key K,

$$C = M \oplus K. \tag{2.2}$$

The encrypted message is sent to Bob via a public channel where Eve can take a copy of it. After receiving C, Bob applies a bit-wise XOR between his key and the encrypted message C. If there is no error in the channel, Bob will get

$$M_{Bob} = K \oplus C = K \oplus K \oplus M = M. \tag{2.3}$$

From here, it can be easily shown that for any message $M, M' \in \mathcal{K}$ and key $K \in \mathcal{K}$ such that $M \oplus K = C$ there exist $K' = M' \oplus M \oplus K \in \mathcal{K}$ such that $M' \oplus K' = C$. This means that by learning, C, Eve's chance to 'guess' the right message, M, is equal to the probability that the key K would be selected. In other words, the security of the cryptosystem is as high as the security of the key itself.

This key distribution and sending an encrypted message over an untrusted channel has an advantage over a secure direct communication method. It allows the protocol to abort in the middle of the key exchange without leaking any critical information about the message. Both parties can stop and restart their protocol as much time as necessary until they are certain that they got a secure key. The next challenge is since modern cryptography needs to support long-range communication while providing the ability to detect malicious activities in the channel and abort the protocol. For that, many schemes and protocols for 'Key Distribution' have been developed.

2.2 BB84 protocol

The first QKD protocol being introduced is Bennett-Brassard 1984 (BB84) protocol. It was named after C. Bennett and G. Brassard [13] who introduced this protocol in 1984. This protocol is the first successfully implemented QKD protocol and still being studied and developed until today [13, 36, 86, 51]. The definition of the protocol is as followed.

Quantum phase

- (Signal preparation and transmission) Alice prepare series of qubit state, each bit is picked randomly from one of the four states $|0\rangle, |1\rangle$ in X basis , or its linear combination $|+\rangle = |0\rangle + |1\rangle$, $|-\rangle = |0\rangle - |1\rangle$ in Z basis. Alice records the bit value and sends the state to Bob.

- (Measurement) For each time slot, Bob locally picks, at random, one of the two bases of measurement, $(0, 1)$ or $(+, -)$, he performs the measurement, record the measurement result and the basis he chose in each bit.

Classical phase

- (Parameter estimation) Alice an Bob randomly choose a small portion of their data as a test set to evaluate the statistical variables in their data. For example, they might disclose some detection results to compare the distribution of detection across each detector in Bob and the value that Alice sent. From there, they design whether a key can be generated from the remaining data. If not, they abort the protocol. Other variables, such as error rate, can be used further in the post-processing step.

- (Sifting) Via a classical authenticated channel, Bob sends the index of slots that he detected signal and their corresponding measurement basis. Alice keeps only the slots in which the basis of measurement match her preparation, and discard the rest. Then, he sends the index of those keeping slots to Bob. Bob discard all other slots.

- (Keymap) They map each remaining slot into a respective binary bit. For example, $|0\rangle$ and $|+\rangle$ to bit 0 and $|1\rangle$ and $|-\rangle$ to bit 1. The bit string obtained from this step is called the sifted key.

- (Error correction) Alice and Bob execute an error correction algorithm to correct any error in their raw key. If the error rate exceeds a certain threshold of Q, terminate the protocol.

- (Privacy Amplification) Alice and Bob apply a 2-universal hash function on their remaining bit string to eliminate Eve's information about the secret key. The dimension of the hash function is determined by Eve's information estimated during parameter estimation and error correction step. The bit string as a result of this step is the secret key.

In general, any quantum states which contain two non-orthogonal bases can be used for QKD. In practical implementation, however, the quantum state of photons such as polarization or phase are prime candidates for the task. This is due to its long coherence time as well as the ease of manipulation and transmission.

One of the obvious examples for the security of QKD is the ability to detect a man in the middle or intercept and resend attack. In this attack, Eve measures each pulse from Alice, then generates and sends Bob a state according to her measurement result. Without information about the choice of basis from Alice, the only strategy available to Eve is to pick a basis of measurement at random. This attack has a 50% chance that her choice of basis does not match that of Bob. These wrong basis choices could induce as high as 25% bit error rate in Bob. Alice and Bob could detect this during parameter estimation and error correction steps and terminate the protocol. With more rigorous analysis, it can be shown that QKD is secure against any attack allowed by the law of physics.

2.2.1 Security analysis and key rate equation

In this section, we provide an overview of the security of the BB84 QKD protocol from the theoretical perspective. With limited time, detection, and transmission efficiency, only a finite amount of quantum bit can be exchanged during each quantum phase. As a result, there are some statistical deviation and failure probability that needed to be taken into account. This finite size effect occurred from the fact that a small sample taken from a finite population might not contain the same statistical properties as the population as a whole. Take this into account, R. Renner [129] has given a general definition of secure key:

Definition 2.2.1 *A QKD protocol is called ϵ-secure, if after the execution of the protocol, there exists a density matrix ρ_E so that the following inequality holds.*

$$\frac{1}{2}\left\|\rho_{ABE} - \rho_{ABE}^{ideal}\right\| < \epsilon \tag{2.4}$$

Here, ρ_{ABE} is the state of the overall system as viewed by Eve can be written as,

$$\rho_{ABE} = \sum_{k}\sum_{k'} p(k,k') \left|K\right\rangle \left\langle K\right| \otimes \left|K'\right\rangle \left\langle K'\right| \otimes \rho_E^{(K,K')} \tag{2.5}$$

where $|K\rangle$ and $|K'\rangle$ [2] be a state that represents the possible classical key shared by Alice and Bob, respectively, at the end of the protocol, $\rho_E^{(K,K')}$ is the quantum state hold by Eve

[2] More detail about Dirac notations and density matrix can be seen in [62, 105].

which might contain information about keys.

$$\rho_{ABE}^{ideal} = \sum_{k} p(k,k') \frac{1}{\mathcal{K}} |K\rangle \langle K| \otimes \rho_E \tag{2.6}$$

is the ideal overall state at the end of an ideal protocol where Eve's quantum state is independent of the states in Alice and Bob's hand.

The ref. [129, 70, 139] provide a core theorem for the privacy amplification.

$$\frac{1}{2} \left\| \rho_{ABE} - \rho_{ABE}^{ideal} \right\| < 2^{-\frac{1}{2}(H_{min}(A|E)-l)} < \epsilon_{PA} \tag{2.7}$$

for some $\epsilon_{PA} > 0$ where $H_{min}(A|E)$ is the minimal entropy of state A for the states known by Eve E. l is the length of the key after privacy amplification. Hence, the key rate for the key of length l distilled from the raw key of size n is

$$\begin{aligned} R = \frac{l}{N} &= q \frac{H_{min}(A|E)}{N} - 2\log(1/\epsilon_{PA}) \\ &\geq q \left(S(A|E) - leak_{EC}) - 2\log(1/\epsilon_{PA}) - 7\sqrt{\frac{1}{n} log(\frac{2}{\epsilon'})} \right) \end{aligned} \tag{2.8}$$

where q is the sifting factor, n is sifted key size, usually 1/2 for a symmetric basis choice. $S(A|E)$ is the conditional Holevo quality of each quantum signal share by Alice and Bob as seen by Eve. The last two terms are finite-size correction terms for privacy amplification failure probability, and for using smooth-min entropy and Holevo quantity as an estimation for Eve's information. The term $leak_{EC} = h(e) - \log \sqrt{3 \log (2/\epsilon_{EC})/n}$ is a portion of information disclosed during the error correction step. The last term is a correction term for error correction's failure probability due to the finite size effect.

From [50, 33], for BB84 protocol, the therm $S(A|E)$ is bounded by 1-h(e) where $h(e) = -e \log e - (1-e) \log (1-e)$, and e is observed error rate between Alice and Bob. Together, the key rate equation for BB84 protocol under finite size effect can be written as

$$\frac{l}{N} \geq q(1 - h(e)) - f h(e) - \log \sqrt{3 \log (2/\epsilon_{EC})/n} - 2\log(1/\epsilon_{PA})/n - 7\sqrt{\frac{1}{n} log(\frac{2}{\epsilon'})}) \tag{2.9}$$

where $f > 1$ is the error correction inefficiency. It can be seen that as $n \to 0$ we have an asymptotic key rate for BB84 with ideal error correction code l/N = 1/2(1-2h(e)).

2.3 BB84 protocol with imperfect source

One of widely used photon source for quantum optics experiment is laser. Ideally, light pulse emitted from laser source is in a coherent state. A coherent state $|\alpha\rangle$ is defined as an eigenstate of the annihilation operator $\hat{a}$. The coherent state can be written as a combination of Fock state:

$$|\alpha\rangle = e^{-\frac{\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.10}$$

From this equation, the probability of having n photon in a pulse is $P(n) = |\langle n| |\alpha\rangle|^2 = e^{\frac{\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}$, which is a Poissonian distribution with mean photon number $\mu = |\alpha|^2$. As mean photon number and pulses intensity are proportional to each other for laser source, we may use these terms interchangeably later on.

2.3.1 Multi-photon pulses and PNS attack

From Eq. (2.10), if a laser source is attenuated such that the mean photon number $\mu < 1$, a majority of the non-empty pulse will be single-photon pulses. This so-called Weak coherent pulsed laser (WCP) source is widely used in various quantum optics studies, including QKD. This source has a non-zero chance of producing multi-photon pulses. If it was used in the QKD system, it would allow Eve to perform an attack on the QKD system, namely Photon number splitting attack (PNS) attack. Eve's attack strategy on a QKD system with a chance of multi-photon pulses is as followed.

(Quantum phase) Alice and Bob's quantum channel is replaced by a lossless channel. For each incoming pulse from Alice, Eve determines the photon number using quantum non-demolition (QND) measurement, which does not disturb the quantum state. For each multi-photon pulse, Eve keeps one photon in her quantum memory and passes the rest to Bob. For single-photon pulses, she takes advantage of her lossless channel by blocking some of the pulses to maintain Bob's total detection rate. If the single-photon emission rate cannot keep up with original Alice and Bob's line loss, she blocks some multi-photon pulses to maintain the detection rate.

(Classical phase) Eve listens to Alice and Bob's communication in the classical channel and measure photons in her memory using the correct basis announced by Alice and Bob.

With this strategy, if the probability of multi-photon pulse is too high so that Eve able to block all single-photon pulses, Eve will gain full information about the key. Otherwise, Eve still gains higher information about the key than estimated in the ideal situation analyzed in the previous section.

To make this attack into account and continue using the WCP source, the post-processing and key rate equation of Alice and Bob needed to be modified. By characterizing the source, the probability of getting a multi-photon pulse, P_{multi} can be determined. Alice and Bob need to assume the worst case where Eve gains full information about every multi-photon pulse sent by Alice. Furthermore, they can estimate the detection rate, P_{det} of the signal by characterizing Bob's receiver, and the channel condition without Eve present. From that, Alice and Bob can rule out Eve's information on their key. In addition, Alice and Bob need to assume that the bits that Eve gained information of were detected by Bob, passed all post-processing, and be part of the final key. Let $A = (P_{det} - P_{multi})/P_{det}$ [51, 89, 131] The modified asymptotic key rate equation becomes

$$\frac{l}{n} = \frac{A}{2}(1 - h(\frac{e}{A}) - leak_{EC}) \tag{2.11}$$

By characterizing their devices and find the value of A, Alice and Bob can generate a key using a weak coherent source. This analysis not only applied to WCP source, but it also works for other types of photon source that has a probability of emitting multi-photon pulses. The task for Alice and Bob is to characterize the source and find the multi-photon probability.

2.3.2 Decoy-state protocol

The disadvantage of the multi-photon portion subtraction method is that the key exchange at a longer distance (higher loss) is viable only if the source has a lower multi-photon probability. For the WCP source, the pulse intensity has to be lowered. That, in turn, reduces the secret key size per session. To improve the performance of the QKD system, a new QKD protocol with WCP source has been introduced; Decoy-state protocol. The protocol definition of a decoy-state QKD is similar to the BB84 protocol, with the following changes in some steps.

Quantum phase

- (Signal preparation) In addition to choosing a bit value and basis, Alice also selects an intensity at random from a predetermined set of signal intensity μ and any number of decoy intensities $\nu_i < \mu$.

Classical phase

- (Parameter estimation) Alice can announce the intensity setting for each pulse so that both she and Bob have a set of detection probability and error rates for each intensity setting. From here, they can either abort the protocol if those variables deviated from the expected value, or continue the key distillation out of the set of detection from the signal state.

If Eve performs PNS attack on each pulse from Alice and captures one photon from each multi-photon pulse, the photon statistics in each set of intensity would change. Since each photon pulse contains a certain number of photons and no information about intensity setting, Eve cannot determine each pulse's intensity setting only by measuring the photon number individually.

Following the BB84 approach discussed in the previous section, we have the key rate for decoy state protocol after privacy amplification [95, 86, 28]:

$$\frac{l}{n} = q(-Q_\mu f(e) h(e_\mu) + Q_1(1 - h(e_1))) - \Delta \tag{2.12}$$

where q = 1/2 is sifting factor, μ is signal state intensity, $Q_m u$ is the gain of detection for the signal state, Q_1 is the gain of single-photon state. f(e)¿1 is the inefficiency of error correction. Δ is a finite size correction. Since these protocols perform parameter estimation, error correction, and privacy amplification like the BB84 protocol, all Δ terms from that analysis also apply here.

The goal of this analysis is to write a bound of the key rate as a function of observables for Alice and Bob. First, let Y_i be the yield of the i-photon state i.e., condition probability of detection in Bob given i-photon pulse is sent from Alice. Y_0 is background count (including noise detection and detector's darkcount). The gain of i-photon state can be written as

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-mu}, \tag{2.13}$$

given Alice's source is WCP. Furthermore, the quantum bit error rate (QBER) for i-photon state is given by

$$e_i = \frac{e_0 Y_0 + e_d \eta_i}{Y_i} \tag{2.14}$$

where e_d is probability of a photon hitting error detector (caused by device imperfection), e_0 is probability of noise detection is an error, typically 1/2. We have an overall gain for signal state:

$$Q_\mu = \sum_0^\infty Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}. \tag{2.15}$$

The total QBER is given by

$$E_\mu Q_\mu = \sum_0^\infty e_i Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{2.16}$$

If Alice and Bob have an infinite number of decoy states and infinite lengths of the key for characterization, they could calculate the value of gain and error rate precisely for each state. In practice, however, Alice and Bob could set only a limited set of decoy and a limited number of key exchange. By substitute Eq. (2.14) to the key rate equation, the problem is simplified to finding the bound of e_1, Y_1, and Y_0. Here we consider the one decoy case where Alice set one level of decoy ν and one level of signal $\mu > \nu$

From Eq. (2.14), the contribution of $i \geq 2$ terms can be written as

$$\sum_2^\infty Y_i \frac{\mu^i}{i!} e^{-\mu} = Q_\mu e^\mu - Y_0 - Y_1 \mu, \tag{2.17}$$

Consider the decoy part, we have

$$\begin{aligned} Q_\nu &= \sum_0^\infty Y_i \frac{\nu^i}{i!} e^{-\nu} \\ &\leq Y_1 \nu + \nu^2/\mu^2 (Q_m u - Y_0 - Y_1 \mu) \end{aligned} \tag{2.18}$$

Here, we use the fact that $a^i \leq a^2$ for all $a < 1$ and $i > 2$, along with Eq. (2.17). Solving this equation we have lower bound of Y_1

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \tag{2.19}$$

Since Alice and Bob have no way to calculate Y_0 in this scenario, they need to assume the worst-case and let Eve puck Y_0 for them. For Eve, it benefits her most if she picks Y_0 to be 0 since she wants to minimize noise detection in Bob and gain more information from non-empty detection. Thus the lower bound of Y_1 as a function of observables for Alice and Bob is

$$Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2}) \tag{2.20}$$

Similarly, by considering QBER of signal and decoy part, we could derive an upper bound of e_1,

$$e_1 \leq \frac{E_\mu Q_\mu e^\mu}{Y_1^L} \tag{2.21}$$

Substitute these to the key rate equation; we have the key rate bound as a function of observables. Alice and Bob have a limited amount of exchange signals, and they need to limit the amount of decoy-state portion of the key to maximizing their secure key rate. The statistical deviation of $Q_\mu, Q_\nu, E_\mu,$, and E_ν is unavoidable. From the analysis in [28], we have the correction terms for decoy-state variables

$$\begin{aligned} \Delta_Q\mu &= u\sqrt{Q_\mu/N_\mu} \\ \Delta_Q\nu &= u\sqrt{Q_\nu/N_\nu} \\ \Delta_{Q\mu E\mu} &= u\sqrt{2E_\mu Q_\mu/N_\mu} \\ \Delta_{Q\nu E\nu} &= u\sqrt{2E_\nu Q_\nu/N_\nu} \end{aligned} \tag{2.22}$$

where N_μ/N_ν is the number of signal/decoy sent by Alice, respectively. u is the number of standard deviation from the central value. The lower acceptable probability of failure is required in the protocol; the higher u need to be. The factor of 2 in the last two equations is from the sifting ratio.

So far, we have discussed the theoretical aspect of QKD. These are important tools for the analyses and experiments in various QKD systems in the following chapters.

Chapter 3

Practical implementation of QKD

The theoretical analysis of QKD shows a high level of security, unachievable by its classical counterpart. Although quantum cryptography's security criteria shifted from computational difficulty in classical communication to the physical property of light, one condition remains; the security of the whole cryptography system is as weak as the weakest link. Since the security assumption of QKD relies on the law of physics, it is unavoidable that the security of QKD is also dictated by its physical implementation. Any imperfections in the physical implementation, any deviation from the model in security proof of a QKD scheme can lead to side-channels that could be exploited by an eavesdropper (Eve) and compromise security. The QKD protocol discussed so far is secured if the following assumption holds:

1. **Eve can listen to the classical channel, but she cannot tamper the message transmitted through this classical channel** This can be achieved by classical (or post-quantum) authentication protocols [25, 115, 2]. This assumption means that Alice and Bob need to share a secret bit for the first round of key distribution. Assuming that the authentication is strong enough that an adversary cannot crack the authentication key before the first quantum key distribution session is finished, a small portion of the newly generated secret key during the session can be used for authentication for the next round. As a result, a QKD system can turn a short-length, short-live to be an infinitely long secure key, given enough time.

2. **Eve is physically isolated from Alice's and Bob's devices** This isolation included all key generating and measurement devices, computation tools, as well as their data storage. This assumption, along with no-cloning theorem [117, 168], stated that Eve could not faithfully copy and store information of the quantum stage through the

quantum channel without communicating with Alice, provides forward security for the key generated by QKD. If Eve does not have a technology or method to interfere with and learn about the quantum state (without being noticed) during the key exchange, Eve cannot store the quantum state and retroactively measure the exchanged quantum state when the technology allows in the future. Thus, the key remains secure. In practice, however, this assumption can be broken by a so-called side-channel attack. The discussion about these side channels and respective countermeasures shall be discussed in the next chapters.

3. **Alice's and Bob's physical devices behave as modeled** In theory, this is handle by assumptions in security proof. This assumption might include device characterization and countermeasures against known attacks. In practice, Alice and Bob should study of devices' characteristics both within expected working parameters and outside their normal working regime. This is because Eve's side channel could alter the properties of the devices, opening a loophole for an attack.

In this chapter, we will discuss the practical implementation of the QKD system, from the requirements of important components to possible vulnerabilities caused by deviation from the theoretical model and imperfection of the devices. We will then discuss some examples of possible side-channel attacks exploiting those vulnerabilities and possible countermeasures.

3.1 QKD devices

This section is a brief discussion of some key physical devices that could fulfill the important part of the QKD model.

3.1.1 Photon sources

A QKD system encodes and distributes the key via the quantum state of the photon. The first key component for the QKD system we will discuss is the photon source.

Ideal single-photon source

The security of the QKD system relies on the fact that the state of a single photon cannot be reliably duplicated by a third party without additional communication. This is known

as no-cloning theorem [117, 168]. Most security models of QKD start from the encryption of single-photon pulses. An ideal single-photon source, as the name suggested, is a device that generates one photon in each time slot. So far, this ideal device has yet to be realized.

Weak coherent pulsed source

As discussed briefly in Chapter 2, the coherent state is an eigenstate of the annihilation operator. This state can be generated by laser pulses attenuated such that the mean photon number of a pulsed laser in each time slot is less than 1. Since photon number distribution of pulsed laser (or coherent state) follows Poissonian distribution, most of the non-empty emission will be single-photon pulsed. The multi-photon part of the source can be handled by characterizing the source and subtract the appropriate amount of raw key in the privacy amplification step or employing decoy-state protocol. This weak coherent pulsed source (WCP) is widely used in many QKD systems [141, 86, 148, 3, 15, 81, 123].

Sub-Poissonian photon source

As our understanding of material science and quantum optics developed, many near-ideal single-photon sources have been introduced. A well-known source is the heralding single-photon source. By sending a bright laser through some non-linear crystal, such as beta barium borate (BBO), a pair of entangled photons can be generated by a parametric down-conversion process and transmitted at a certain angle [45]. If a photon is detected in an angle from the incident beam path, it confirms the presence of a single-photon pulse in the opposite angle. Although the probability of generating multiple photons from this photon source can be drastically lower than the WCP source, the probability of generating entangle photons per incident pulse is also low. This probabilistic emission can be overcome by using quantum memory to store the state of photons before the key exchange. This state can be read out to fill each time slot of the key exchange.

Another interesting sub-Poissonian photon source is the quantum dot (QD) [106, 108] [71, 34, 170]. Quantum dot is three-dimensional confinement that traps an electron-hole pair in two distinct electronic states. The electron can be excited by a laser pulse with appropriate energy (wavelength) and emits an entangled photon pair in a deterministic path. Since the quantum dot has near-unity quantum efficiency at low temperatures, it can generate single-photon pulses with a high repetition rate and single-photon quality. In principle, these parameters are only limited by the photon collection apparatus. The properties and performance of QD as a single-photon source for QKD shall be discussed in Chapter 4.

3.1.2 Optical mode and state-encoding devices

In a QKD system, the information is encoded and carried by the optical mode of photons. An optical mode is an orthonormal basis solution of Maxwell's equation in classical electrodynamics. Linear optical devices can be used to manipulate optical modes. The following are some examples of optical modes used in QKD encryption.

Polarization

The polarization of a photon refers to the vibrational plane of the electric field of that photon [53, 100]. A BB84 state can be encoded in horizontal-vertical (H-V) linearly polarized basis or its linear combinations in the diagonal (D-A) basis or left-right (L-R) circular basis. These modes can be manipulated by a polarizing beam splitter (PBS), which lets only specific linear polarization to a certain path, and a combination of half-wave plate and quarter-wave plate which transform a known input polarization photon to another polarization depend on the orientation of their optical axes.

Phase

The phase of the electromagnetic field of a photon can be shifted by a phase shifter devices. These devices can be a delay line that changes the optical path's length or some material that changes its reflective index based on an applied voltage [100]. Some of the examples of QKD using phase encoding are described in [30, 3, 153, 154]

Time-bin

The time of arrival of photon pulses can be used to encode the BB84 states. By dividing each time slot into 'early' and 'late' sub-slot using optical such as Mach-Zehnder interferometer in both sender and receiver, constructive interference between the pulses in two adjacent time slots can be used to determine the path each pulse takes and assign respective bit value for the key [156, 101, 66].

3.1.3 Quantum channel

Quantum channel is part of the QKD model that separates Alice and Bob, where the quantum state is sent through. In general, this channel is assumed to be controlled by Eve. In practice, there are two types of channels:

Fiber optics

Fiber optics is a device that guides photons from one end to another, using the total reflection phenomenon of a photon passing through two mediums with a different refractive index [100]. It is widely used in classical optical communication. The advantage of this channel is the ease of deployment. The disadvantage is the relatively high photon loss. Since this loss cannot be overcome by amplifying the signal strength as usually done in classical optics, this limits the distance of communication between two parties [153, 150, 83]. Furthermore, without specialized fiber optics [113], this type of channel suffers high distortion in polarization state while able to maintain phase information at long distances. Thus, phase encoding is widely used through the single-mode fiber optics channel [141, 118, 3].

Free-space channel

Free-space QKD sends the quantum states through vacuum or air. This type of channel suffers relatively lower channel loss compares to that of fiber-optics. Thus, this channel could cover a longer distance [143, 171, 84, 119]. This channel enables a platform that could extend the QKD coverage to the global scale, the satellite-based QKD [15, 81, 123]. The downside of this channel is the requirement of a line of sight between Alice and Bob. A long-distance ground-based, however, free-space QKD suffers from Earth's geography and curvature. It also suffers by phase and wavefront distortion due to atmospheric turbulence. The atmospheric turbulence model and its effect on the free-space QKD system, including Eve, shall be discussed in the respective experiment in Chapter 6.

3.1.4 State discrimination and detection devices

The general concept of the QKD receiver is to send distinct states into distinct paths inside the receiver and detect by a detector at the end of the path. The state discrimination apparatus in the receiver usually follows the same concept as the encoding device. A set of wave plates and PBS can be used to discriminate against the polarization state. On the other hand, the interferometer and phase shifter can be used to discriminate phase and time-bin encoding. From there, the photon signals are sent to the detector. These detectors have to be sensitive to the single-photon signal [52]. There are many types and models of photon detectors used in the QKD system. They can be separate into two categories:

Threshold detector or bucket detector

The threshold detector is one of the most commonly used in QKD due to ease of implementation and maintenance. This type of detector transforms a non-empty optical signal pulse into an electronic pulse or 'click'. There are several parameters used to determine the performance of each detector [52]. For example, the probability of a photon sent to the detector ended up being registered as clicked is called 'detection efficiency'. The higher efficiency, the better. On the other hand, the probability that the detector 'click' without photon sent is called 'darkcount'. A darkcount could be caused by a short circuit or temperature fluctuation in the device. This darkcount could cause an error in the detection. Thus, an ideal detector has to have this parameter as low as possible. This signal does not contain information on photon energy or photon number. Other parameters, such as wavelength-dependent efficiency, also needed to be considered. The examples of these detectors are:

Photon multiplier tube (PMT) This device uses a series of cathode plates with incrementally stronger biased voltage to multiply single electron scattered from a photoelectric medium to be a measurable electronic pulse [59]. This type of detector is widely used for its larger sensitive area and relatively low dark count rate [52].

Avalanche photo diode (APD) this device operated by reverse biasing the photodiode such that a trigger by single-photon could induce a measurable pulse of current through the diode [20]. This type of detector has a high detection rate and could detect photons in several bands of wavelength depend on the detector's materials [52].

Superconducting nanowire single-photon detector (SNSPD) This detector detects the change in resistivity of superconducting material when hit by a photon [134, 69]. SNSPD has high detection efficiency and relatively low darkcount [52].

Photon-number resolving detector

In contrast to the bucket detector, the electrical signal photon number resolving detector is proportional to the photon energy being detected. An example of this type of detector is a Transition edge sensor (TES) [14, 35].

TES photon detector is a micro-calorimeter which consists of an absorber, a sensitive thermometer, and a weak thermal link to a heat bath. The energy of photons absorbed in the detector is measured through the change of resistance of the thermometer. TES could achieved the highest detection efficiency among single-photon detector detectors up to 95% for 1550-nm detection efficiency, with very low darkcount [82, 41, 107, 52]. The

photon number resolving in other types of detector such as SNSPD or PMT has also been studied [102, 162].

3.2 Attacks on QKD system

Cryptography is a game of cat-and-mouse between the legitimate parties and eavesdroppers. To understand the extent of security that could be expected or claimed on a cryptography system design, one needs to understand existing vulnerabilities in the system and attack models that could exploit those vulnerabilities. In this section, we will discuss these vulnerabilities and attacks.

3.2.1 Theoretical attack

Assuming the physical apparatus that could fulfill all requirements and conditions in the theoretical model, the only possible opening in the system for Eve to attack is the quantum state in the quantum channel. The strength of Eve's attack can be divided into three categories based on here ability to interact with the quantum signal.

Individual attack

In this attack, Eve uses the same strategy to probe each signal from Alice to Bob independently throughout the key exchange step. For each state A' from Alice, she attaches her ancilla state, E. She then performs unitary operator on both A' and E and passes A' to Bob. She then stores E in quantum memory, and measure the state at the time of her choosing to maximize the knowledge. She then follows the post-processing step of Alice and Bob to gain some information about the secret key. An example of an individual attack is the intercept-and-resend attack.

Collective attack

She probes each signal from Alice, similar to the individual attack. However, she listens to Alice and Bob's classical communication before designing the most optimal way to collectively measure state E to maximize the information on the key.

Coherent attack

This type of attack is the most general type of attack. Instead of interacting with each signal individually, Eve interacts with all signals coherently, and attach one ancillary E to all signals. She can measure her ancillary state E at any time to maximize information.

3.2.2 Side-channel attack

In reality, a practical device can behave differently from what is designed for or required by the system. Some are intrinsic properties of the device, while some can be induced or controlled by Eve. These flaws could open loop-hole for attacks on the system [160, 97, 125, 76, 93, 169, 44, 166, 67, 138, 135, 99, 136, 104, 137]. In addition to some attacks discussed earlier in this thesis, we will discuss some examples of attacks made available by physical implementation flaws.

Detector efficiency mismatch attack

One of the assumptions of a QKD receiver is that all the detectors have the same detection efficiency. In practice, however, the detectors could possess a discrepancy in detection efficiency under certain conditions, for example, in gated APD detector where the detectors are activated (biased) only when the expected arrival time of the signal, there the gate signal in each channel might not activate at an exact same time. If that occurs, in addition to intercept and resend attack, Eve could selectively shift the arrival time of the signal to the point that only the detector of her choice has a chance to detect the signal, reducing the chance of her being detected. [125, 155]

Another form of detection efficiency mismatch attack is in the free-space QKD system [138, 110]. In this attack, Eve alters the angle of arrival of the signal such that by the internal reflection or imperfection of optical alignment in Bob, the photon beam misses all unwanted detectors and detected only by the detector of her choice, masking her intercept-and-resend attack. More detail of this attack shall be discussed in Chapter 6.

Wavelength-dependent attack

In practice, each detector or internal optical devices in Bob could have different sensitivity to different wavelength [48, 57, 84, 149]. This flaw could allow Eve to manipulate the detection results by changing the signal's wavelength to Bob.

Trojan horse attack

The security assumption of QKD states that the choice of state in Alice and the choice of basis of measurement in Bob is not known to Eve. In practice, however, Eve could send a bright laser pulse at the time of the state preparation or basis measurement has been chosen. If there are reflective surfaces behind the encoding component in Alice or Bob, the reflected light could carry information of that device setting back to Eve, providing her more information about the key [46, 65, 147].

Detector control attack

In this attack, Eve takes control of the detection result in Bob by altering the property of the detectors. An example of this type of attack is the blinding attack on APD [96]. In normal operation, APD is in a Geiger mode where reverse biasing above the threshold such that the trigger by single-photon could cause measurable current from the detector. However, by sending bright CW laser with appropriate brightness through the quantum channel, Eve could lower the bias voltage across APD such that the APD is in the linear mode, no longer sensitive to single-photon pulses (blinded) while a certain bright pulse could induce a proportional electrical signal. Eve can then perform intercept-and-resend attack and send her state as a bright pulse such that if Bob's basis choice matches that of hers, the response signal is higher than Bob's threshold, triggering a 'click', while the pulse is split in the different basis causing a below the threshold signal and not being registered. Similar attack on other detectors has been demonstrated [93, 90, 167, 140, 55]. A variant of this attack on the TES detector shall be discussed in Chapter 6.

Chapter 4

Quantum dot as a single-photon source for satellite-based QKD

Author contributions

I reviewed the theoretical analysis and calculated the estimated key rate for both WCP and quantum dot QKD system. Thomas Jennewein, Brendon L. Higgins, and I design the experiment setup. Sara Hosseini, Arash Ahmadi, and Michael E Reimer help prepare quantum dot. I programmed the devices' control and post-processing. I derive the equation multi-photon probability with B. Higgins

Satellite-based QKD is a platform developed to extend the range of secure communication across the globe. Major challenges to the key generation of this platform are the channel transmission loss as well as limited fly-by time [15, 123]. In addition, post-processing cost to handle imperfections of the photon source, such as multi-photon generation [58, 95], further limits the chance of a successful key exchange during each satellite pass. Since the operation cost of such a QKD system is high, having a system that can reliably generate a secure key is crucial. This post-processing cost could be improved with a true single-photon source. An ideal candidate is a semiconductor quantum dot [144], especially when it is embedded in a photonic nanostructure [106, 108] [71]. A quantum dot emits on-demand single photons, while the nanostructure around it guarantees the efficient and directional light extraction [34, 170]. If the photonic nanostructure surrounding the quantum dot relative to its position is designed carefully, it creates a platform that could reliably generate single-photon pulses with high rate and purity[128, 164]. Although single-photon sources'

development using a semiconductor quantum dot is progressed rapidly, its application has yet clearly demonstrated, especially for QKD. Most of the previous studies have been conducted at the proof-of-concept level showing that the QKD with quantum dot source can generate key up to the sifting step [60, 54][152].

This study compares the performance of a BB84 QKD system using a single-photon source with a decoy-state BB84 system utilizing a weak coherent pulsed laser as the photon source. Two different pumping methods were applied to excite the quantum dot; non-resonant pumping scheme and two-photon resonant excitation scheme. We use the key-rate equation with the finite-size effect from Ref. [16, 28] for the QKD system based on decoy-state and the key rate equation from Ref. [19] to estimate the performance of the QKD system using the quantum dot as the single-photon source. For both cases, we model our calculation based on realistic conditions for satellite-based QKD, including channel loss, fly-by time windows, noise, and finite-size effect. We also include coupling losses from quantum dot emitter to the output source. [16, 19, 28].

4.1 Experiment setup

The sender part (Alice) of the system under study utilizes a polarizer and a half-wave plate to encode one of the four polarization (Horizontal H, Vertical V, Diagonal D, and Anti-diagonal A) to each photon pulses from photon source. The photons then passed through the ND filters used to emulate channel loss. The beam then sent through the free-space channel toward the receiver (Bob).

The QKD receiver under study uses a passive basis choice to analyze and detect polarization-encoded light. Compared to active basis choice, a passive basis choice design simplifies the system and reduces the number of active elements, as is generally desirable for a satellite payload [16]. Its telescope consists of a focusing lens L1 (diameter of 50 mm with a focal length $f = 250$ mm), and a collimating lens L2 (diameter of 5 mm with $f = 11$ mm). The collimated beam of $\lesssim 2$ mm diameter then passes through a 50:50 beam splitter BS, and a pair of polarization beam splitters PBS1 and PBS2. The purpose of PBS2 is to increase the polarization extinction ratio in the reflected path from PBS1. The four lenses L3 focus the beams into four multi-mode fibers, each with a core diameter of 105 μm, which are connected to single-photon detectors. The detection in each detector is recorded using a time-tagging system.

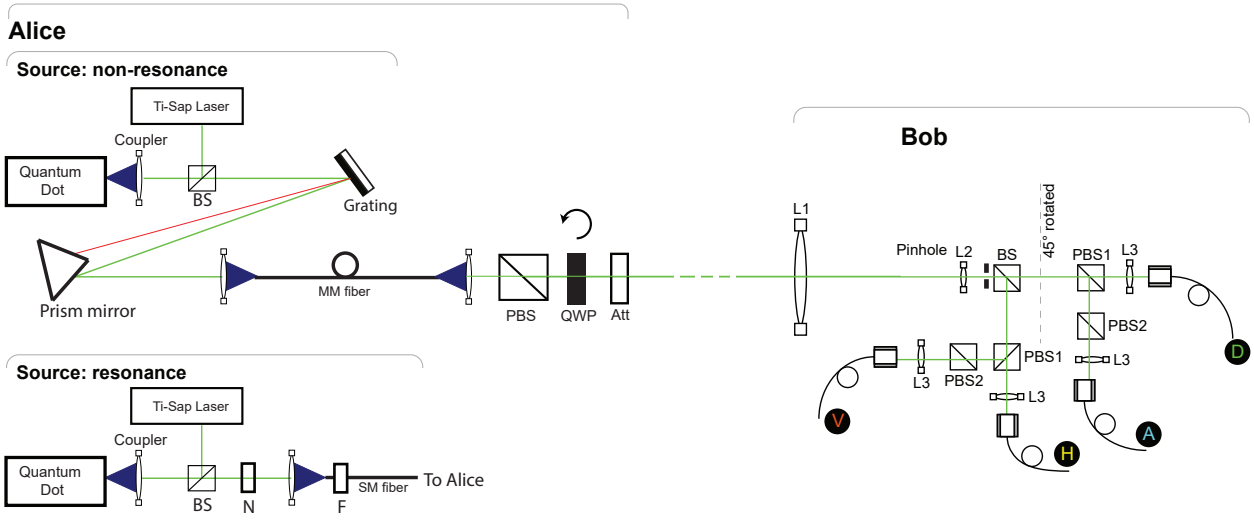

Figure 4.1: Experimental setup. For the WCP QKD experiment, the photon pulses are sent directly from Ti:Sapphire laser to the QKD setup. For q. dot QKD, the quantum dot is excited with the pulsed laser from Ti:Sapphire laser. A grating and a wedge mirror are used to separate exciton pulses from bi-exciton pulses. The photons then sent to the QKD system under test. In Alice, the polarization state is selected by a PBS and a half-wave plate HWP mounted on a rotational stage. For each set of data collection, the polarization is fixed to one of the four linear polarization orientation, horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A). The key generation rate is an average of these four polarization settings. In a real implementation, the state preparation could be done using one of the following setup. The first is to use a fiber-based polarization modulator, which has a typical insertion loss of 4dB and a repetition rate of 1GHz [1]. Another option is to passively coupling together four QDs with dedicated polarization orientation. The state can be selected by sending an excitation laser pulse to respective QD for intended polarization in each time slot. This setup could reach the GHz level repetition rate. A set of attenuator Att is used to select signal and decoy intensity in the weak-coherent pulse (WCP) experiment, as well as simulate channel loss. For the resonance excitation experiment, the source is replaced with the lower setup where notch filter N and a single-mode fiber-coupled band-pass filter F are used to separate reflected laser from single-photon emission.

4.2 Weak-coherent pulse QKD

For weak-coherent QKD, the photon pulses from the Ti:Sapphire laser (The Coherent, Mira Optima 900-P) is passed through an attenuator to reduce the mean photon number per pulse, $\mu = 0.5$ for signal pulses and $\nu = 0.1$ for decoy pulses. Other parameters are set following the study of satellite QKD in Ref. [15]. In our experiment, we record a series of pulses in each channel transmission loss value, one polarization at a time. Each series is recorded over 100 s, a typical usable link time of a QKD satellite. The statistical detection rate, the error rate on the decoy, and the signal state are used to calculate the secret key length. The key length of a decoy-state QKD with two intensity level can be written as

$$L \geq nK_{\mu}\left[Y_1^L(1-h(E_1^U)) - fh(E) - Q_{\mu}\Delta/n_{\mu}\right], \tag{4.1}$$

where n and n_{μ} are respectively total number of transmitted photon pulses and number of detected signal pulses respectively. Y_1^L and E_1^2 is respectively lower bound of single photon gain and upper bound of QBER with a correction for finite size effect on decoy state characterization [28], q =1/2 is sifting basis ratio, K_{μ} is fraction of pulse that are signal state $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy, $fh(E)$ is information leakage during error correction for an observed error rate E and error correction code efficiency f. Δ is a correction term owing to the statistical deviation due to finite size effect [28, 58, 95, 16]

A set of neutral density filters is inserted between Alice and Bob set up to simulate transmission channel losses. The experimental raw key rate in each channel loss is an average between all four polarization orientations in Alice. The estimated and experimental key size as a function of channel loss is shown by the red line and red dots, respectively, in 4.6.

4.3 Quantum Key Distribution with a sub-poissonian photon source

In this experiment, we replaced the laser pulses signal and attenuator in the decoy-state system with the single-photon signal from a wurtzite InAsP quantum dot embedded in a tapered InP nanowire Ref.[128, 29]. We used off-resonant or incoherent pulsed pumping scheme to excite the quantum dot. In this scheme, the quantum dot is excited above the band-gap, which is the excitation at 830nm, the wurtzite InP nanowire band-gap

transition Ref.[40]. The photoluminescence (PL) of the quantum dot that we used is shown in Fig. 4.2. The spectrum was captured by a single grating imaging spectrometer (Acton SpecttraPro SP-2750). It was off-resonance excitation by 830nm laser pulses from a Titanium-sapphire laser at 420nW of power. The laser has a repetition rate of 76.4MHz. The quantum dot emits exciton photons at 892.67nm and biexciton photons at 894.2nm. In order to separate these two emission lines, we sent the quantum dot emission to a polarization-independent transmission grating (Lightsmyth T-1500-875) with 1504 grooves per millimeter. The photons from the excitonic emission at 892.67nm were coupled to a multi-mode optical fiber and sent to the QKD setup, as shown in Fig. 4.1. This setup does not have an active switching device. In this QKD security analysis, we assume that the phases of each photon pulse emitted from quantum dot are independent. For a practical implementation, the phase randomization could be achieved by one of the following options. The first is to use a fiber-based phase modulator, which has a typical insertion loss of 4dB and a maximum repetition rate of 10MHz [4]. Second is using a free-space Pockels cell, which has a speed limit of 20MHz [5]. Another option is to passively couple together four QDs with dedicated polarization orientation. The polarization state can be selected by sending an excitation laser pulse to respective QD for intended polarization in each time slot. This setup could modulate polarization and achieve phase randomization at the GHz level repetition rate and insertion loss of 3dB.

The QD source in this study has an internal loss of $15dB$ due to photon generation and collection's imperfections, resulting in a pulse rate of 2.6MHz. We chose the photons from exciton emission as they have a higher rate compared to the biexcitonic emission. This can be seen in Fig. 4.2.

As a figure of merit, the source has $g^2(0)$ of 0.015 while excited off-resonant. However, $g^2(0)$ drops to less than 0.0015 when applying the two-photon resonant excitation scheme (See Fig. 4.3). Although there is a special emphasis in semiconductor quantum optics on the measurement of the second-order correlation function $g^2(0)$, recently it has been shown that $g^2(0) < \frac{1}{2}$ only suggests non-zero single-photon contribution in the quantum state of the light, without giving the exact probability of single or multi-photon emission Ref.[121]. This suggests that our source could still emit multiple-photon pulses. These multi-photons permit an adversary Eve to perform a photon number splitting attack (PNS attack) and gain information about the key. Taken this into account, we have the lower bound of key

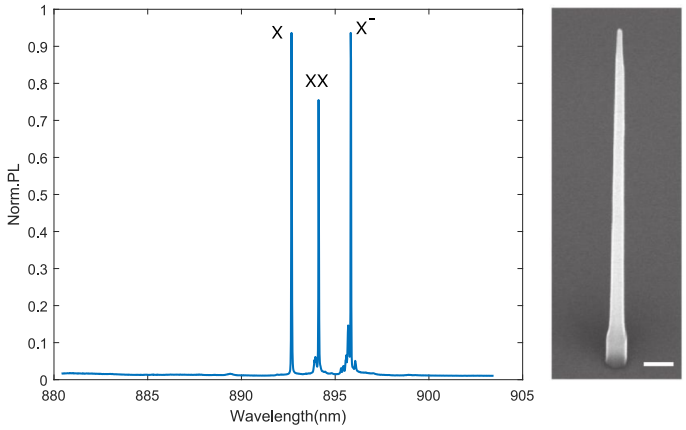

Figure 4.2: Spectrum of the QD emission excited at 830 nm, above band-gap non-resonant excitation (NRE) scheme. The spectrum shows three peaks attributed to the exciton (X), biexciton (XX), and charged exciton or trion (T). The spectrum was taken by an imaging spectrometer using a 1200 grooves/mm grating. Photo shows nanowirestructure of the QD under study.

length per satellite pass for the BB84QKD using quantum dot under the finite-size effect,

$$\begin{aligned} L \quad \geq \quad & nA\left(1-h\left(\frac{\tilde{E}}{A}\right)\right) - n\ leak_{\mathrm{EC}} \\ & - 7n\sqrt{\frac{1}{n}\log_2\frac{2}{\tilde{\varepsilon}}} - 2\log_2\frac{1}{\varepsilon_{\mathrm{PA}}} - \log_2\frac{2}{\varepsilon_{\mathrm{EC}}}, \end{aligned} \tag{4.2}$$

where n is the number of sifted key, $\tilde{E} = E + \frac{1}{2}\sqrt{\{2\ln(1/\varepsilon_{\mathrm{PE}}) + 2\ln(n+1)\}(1/n)}$ takes into account a chance that the error rate estimated from a sifted key of size n in the protocol might deviate from the actual value [130, 19, 142], $\varepsilon_{\mathrm{PE}}$ is the probability that such deviation occurs. The single photon detection probability $A = (p_{\mathrm{det}} - p_{\mathrm{multi}})/p_{\mathrm{det}}$ is a correction term ruling-out Eve's information due to multi-photon pulses [88], where p_{det} is the probability of detection and p_{multi} is the probability of a multi-photon pulse generated by Alice. Since the photon number distribution of the quantum dot is not known, the direct calculation of the multi-photon pulse probability from a coherent state mean photon number does not apply. Instead, we employ an alternative method to establish an upper bound, P_m.

First, we notice from examining key exchange data using the four-detector receiver apparatus that the frequency of three-way coincidence detection is vanishingly small. From

our observation, the probability of having more than two detectors 'click' within the same time slot (5 ns) is less than 10^{-9} per detection, which is more than four orders of magnitude lower than the double clicks probability. The probability of this triple-click falls within the range of detection incidence due to background noise in the channel and darkcounts from the detectors. This result implies that contributions beyond two photons may be neglected compared to the pulses with two photons or lower.

We characterize the remaining two-photon contribution by examining detection events of a train of photon pulses emitted from the quantum dot passing through a 50:50 beam-splitter, with each output is coupled to an APD. The setup has coupling efficiency $\eta_t = 10\%$. The APD has detection efficiency $\eta_d = 60\%$. From a 10 hours data collection time we assess the number of coincident events C, where both detectors 'click' within the 5 ns window. With emission of i-photon Fock-states at probabilities given by p_i,

$$C = \frac{1}{2} p_2 \eta^2 + \mathcal{O}(\eta D) + \mathcal{O}(D^2), \tag{4.3}$$

where detection efficiency of the testing device is given by $\eta = \eta_t \eta_d$, and D is darkcount probability. We similarly also determine the number of 'solitary' events S where only one detector clicks within the window,

$$S = p_1 \eta + p_2 \eta (\tfrac{3}{2} - \eta) + \mathcal{O}(D). \tag{4.4}$$

In this setup, the probability of darkcount per detection event is lower than 10^{-7} per detection. Thus, the contribution of darkcounts in C and S is negligible. By combining Eq. (4.4) and Eq. (4.3), we find

$$p_2 = \frac{2K p_1}{\eta - 3K + 2K\eta}, \tag{4.5}$$

where $K \equiv C/S$. So long as the assumption that higher photon terms can be neglected holds, we arrive at a bound for P_m,

$$P_m \leq \frac{2KR}{\eta - 3K + 2K\eta}, \tag{4.6}$$

making use of the probability of nonempty pulses $R = p_1 + p_2 \geq p_1$, which can be measured directly from the source. From our measurement, we found K $= 1.1 \times 10^{-5}$, $\eta = 0.06$, and R $= 0.033$. Substitute these variables into Eq. (4.6), we got $P_m \leq 4.5 \times 10^{-6}$.

4.3.1 Resonant excitation (TPE) scheme

There are two methods to pump the quantum dot to the excited state. The first one is the non-resonant or incoherent pumping scheme, as we mentioned before. In this scheme, the quantum dot is excited above the band-gap. This scheme is more common and easier to implement. However, it limits the coherence and indistinguishability of the emitted photons and increases the chance of multi-photon emission due to the charge capture in the quantum dot potential. This problem can be overcome by resonant two-photon coherent excitation (TPE) scheme to coherently populate the biexcitonic state in the quantum dot. A resonant two-photon excitation (TPE) scheme was previously applied in a self-assembled quantum dot Ref.[109]. Here, we implement this scheme to wurtzite InAsP quantum dot embedded in a tapered InP nanowire. A shaped laser pulse with the wavelength of 893.367 nm is used to excite the ground state of the quantum dot to the virtual excitation state situated between the exciton and biexciton emission lines, as shown in Fig. 4.3. Hence, the laser wavelength is chosen to be between the two emission lines in the quantum dot. Pump intensity is set to the (so-called π pulse) where the inversion of the quantum dot from the ground to the biexcitonic state is most probable. In this case, one can deterministically populate a biexciton after each pulse with near-unity fidelity and near-zero multi-photon emission. The challenge of this experiment is to suppress the scattered excitation laser light. Previously, the polarization-suppression technique was used to implement this scheme [9]. Here, we used three notch filters (OptiGrate BNF-894-OD4) to attenuate the laser scattering. Fig. 4.4 (b) shows the photoluminescence spectrum of the quantum dot under a two-photon resonant excitation scheme (TPE). The intensities of the exciton (X) and biexciton (XX) emission lines are similar, and the charged exciton emission is suppressed considerably.

4.3.2 g^2 measurement

We measured $g^2(0)$ correlation using Hanbury Brown and Twiss (HBT) setup. After correcting for the APDs darkcounts, the $g^2(0)$ for the non-resonant scheme is found to be 0.015, and for the two-photon resonance excitation scheme is less than 0.0015 as shown in Fig. 4.5. It proves that the two-photon resonance excitation reduces the probability of multi-photon emission dramatically.

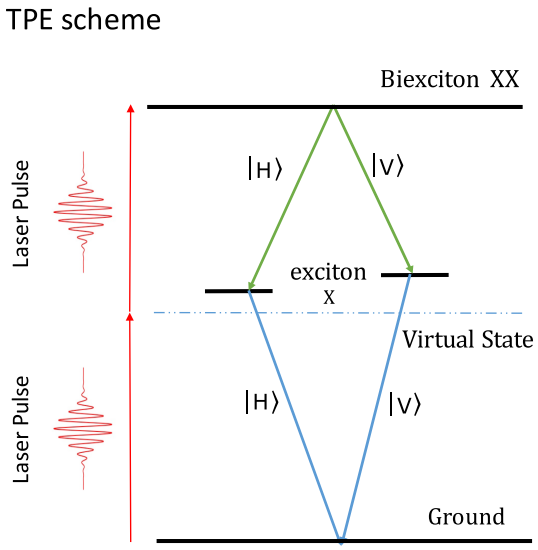

Figure 4.3: Two-photon resonant excitation scheme. A shaped pulse laser excites two electrons from the ground state to the virtual state, that its energy is situated between the exciton and biexciton emission lines.

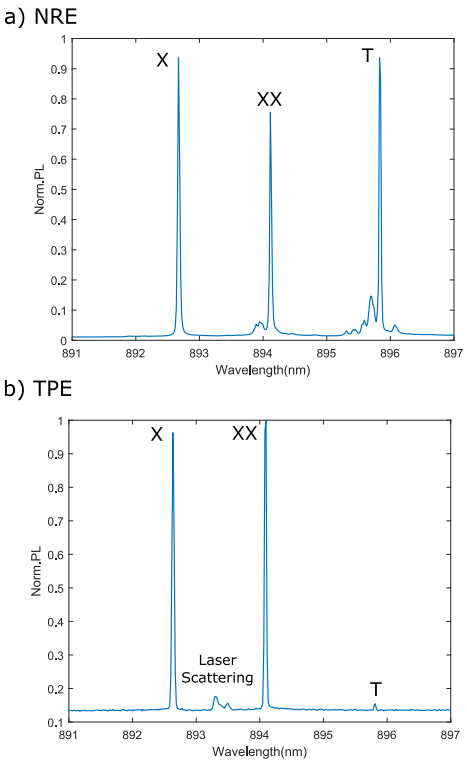

Figure 4.4: Spectrum of the QD emission excited at a) 830 nm, above band-gap non-resonant excitation (NRE) scheme. The spectrum shows three peaks attributed to the exciton (X), biexciton (XX), and charged exciton or trion (T) b) two-photon resonant excitation scheme using excitation laser at 893.367 nm. The exciton (X) and biexciton (XX) have almost the same intensities, and the trion (T) has been suppressed dramatically. This proves that exciton and biexciton photons are emitted in pairs, and no charge is captured that can result in charged exciton emission. The small peak between the exciton and biexciton emission lines is due to the scattered laser light residual. Both spectrums were taken by an imaging spectrometer using a 1200 grooves/mm grating

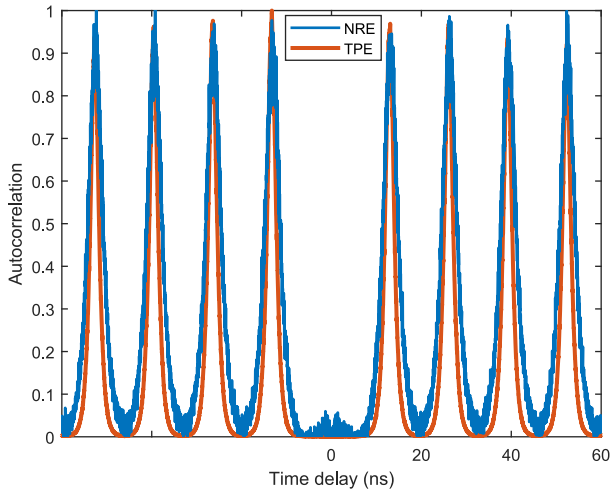

Figure 4.5: Autocorrelation histograms, under non-resonant-excitation scheme (blue curve) and two-photon resonant excitation scheme (red curve). The data are presented without any corrections.

4.4 Result and discussion

Using the parameters found in the measurement, we can calculate the Quantum dot QKD system's key rate using Eq. (4.2). The experimental result and theoretical simulation are shown in Fig. 4.6. The effective loss tolerance of the Quantum dot QKD system excited off-resonance using a pulsed laser with nearly 80MHz repetition rate is $\approx 25dB$ (green line in Fig. 4.6), higher than the decoy-state protocol with 80MHz repetition rate (red line).

The performance of Quantum dot QKD can be improved by reducing the source's internal loss. We calculate the key rate for a QKD system with the Quantum dot source under the test but without internal loss. The result shows that, if the internal loss of the source is eliminated, the loss tolerance of the system could reach 32dB (blue line in Fig. 4.6), surpassing a decoy-state QKD system with 300MHz repetition rate (black line in Fig. 4.6).

Although the Quantum dot under the study improves the performance of QKD system; it has been excited using the off-resonance excitation scheme, which is not an optimal performance of the quantum dot source. Applying two-photon resonance excitation will reduce the multi-photon emission and the lifetime of the quantum dot excited state. Since the repetition rate of quantum dots is limited by the lifetime of the excited state, this will help to excite the source with a higher excitation rate resulting in the higher count

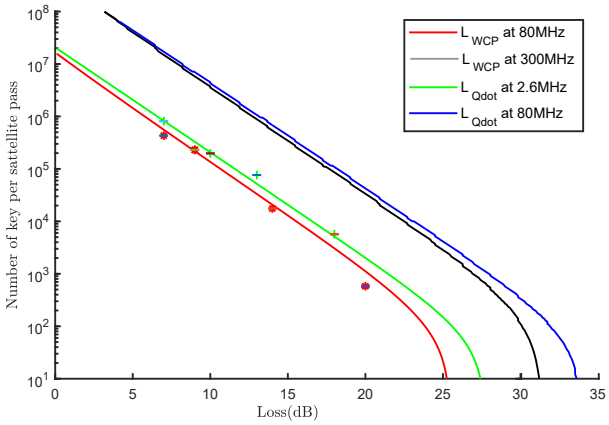

Figure 4.6: Secret key size over 100s key exchange (with finite-size effect) as a function of channel loss. (Red) Decoy-state with 80MHz, (Green) Quantum dot-QKD with 80MHz excitation frequency and 10dB internal loss, (Blue) theoretical calculation of the Quantum dot QKD system with 80MHz excitation frequency and no internal loss, (black) theoretical calculation of decoy-state at 300MHz. In this comparison, we assumed that the phase of the photons in each pulse of both WCP and QD are independent. In practice, the phase randomization device would induce $\approx 3\ dB$ internal loss in both cases. The key generation rates in both cases would be proportionally lower. The advantage of QD-QKD still hold.

rate. The state-of-the-art quantum dot that benefits from the careful design of polarized microcavities has a lifetime of $\approx 60ps$ [164], and can be driven on resonance by up to GHz-frequency level pulsed laser. This is equivalent to the frequency used in high-speed WCP QKD today [49, 32, 165]. This result demonstrates that quantum dot can indeed be a promising source for BB84 QKD protocol.

4.5 Conclusion

This study compares the performance of Quantum dot QKD and WCP QKD under the finite-size effect. We propose a method to characterize and calculate an upper bound of multi-photon emission. The experimental result shows that a quantum dot QKD system with a 76.4MHz repetition rate and 15dB internal loss could outperform a decoy-state QKD with the same repetition rate, especially at high channel transmission loss. The performance of Quantum dot QKD could be improved further by reducing the internal loss and increasing the photon generation rate. This result shows that QKD with a single-

photon source could be a candidate for secure communication with high channel loss, for example, satellite-based QKD. We hope this would spark an interest in the development of QKD with a true single-photon source. We also hope that this study will raise attention toward further development of quantum dot as a single-photon source, as well as other single-photon source applications in general.

Chapter 5

Generalized reflective index characterization on QKD sysyem

Author contributions
Vadim Makarov, Norbert Lütkenhaus, and Martin Ward provided advice on the existing characterization model. I calculate and analyze the characterization method against a generalized attack. With Vadim Makarov, we proposed an improved characterization methodology

Trojan-horse attack on a quantum key distribution (QKD) system uses the reflection of bright light back from the system's internal components. This reflected light might pass through encryption/decryption components, carrying secret information to an eavesdropper Eve. Several studies have demonstrated the feasibility of this attack [160, 46, 63, 64, 147, 137]. A modified security proof has been derived that calculates the key rate in the presence of a characterized upper-bounded level of backreflection, with the characterization guaranteed by a series of passive optical components [87]. The latter study also outlines an experimental characterization method for the backreflection level. A similar methodology is present in the current draft of a group specification for characterization and countermeasure against the Trojan-horse attack [6], written by the industry specification group on the quantum key distribution (ISG-QKD) at the European Telecommunications Standards Institute (ETSI). Here we show that this drafted methodology underestimates the backreflection. We model how Eve can carefully modulate the phase and timing of each Trojan-horse pulse and significantly increase the intensity of reflected light via the interference effect.

This Comment serves as a brief critical remark on the currently available methodology in Refs. [87, 6].

5.0.1 Problem with characterization method

In order to upper-bound the intensity of reflected Trojan-horse pulses, reflectivity characterization of the QKD system's internal components has been proposed [87, 6]. The proposed method focuses on signal encoding and transmitting side of the system (Alice). The optical components in Alice are divided into two blocks [Fig. 5.1(a)]. First, the front block consists of an optical filter (F), isolator (I), and attenuator (A). Trojan-horse pulses reflected from these components do not pass through the encoding device, i.e., the phase modulator (PM). Thus, those reflected pulses do not carry information about the PM setting to Eve. Second, the backreflection block [Fig. 5.1(b)] consists of a polarizing beamsplitter (PBS), beamsplitter (BS), air gap, intensity modulator (IM), connectors (J2, J3, J4), and the PM itself. The Trojan-horse pulses reflected off these components might pass through the PM. Hence, the method proposed in Ref. [87] assumes that the total intensity that could carry phase information of the PM could be determined by a sum of the total reflectivity of all the components in this block, and a physical limit of Eve's incoming Trojan pulse intensity. Eve's intensity limit is assumed to be a fiber damage threshold at the entrance of the system. The characterization of component's reflectivity is done by sending pulsed laser into the backreflection block and performing optical time-domain reflectometry, as shown in Fig. 5.1(b). The measured intensities of reflected pulses from all the components are then summed together (Sec. IV B in Ref. [87]), giving the total reflectivity. However, with this method, the actual reflectivity Eve could achieve would be underestimated.

Eve can send multiple laser pulses with proper time delay such that all backreflected pulses pass the last component behind the PM at the same time. Furthermore, she can tune the phase of each pulse such that all the reflected pulses pass through the last component in-phase and interfere constructively. This results in a higher reflected intensity than expected in the original method.

For example, let's consider two laser pulses with input amplitude E_1 and E_2 reflected from two surfaces with reflectance r_1 and r_2. Let the phase difference between the two

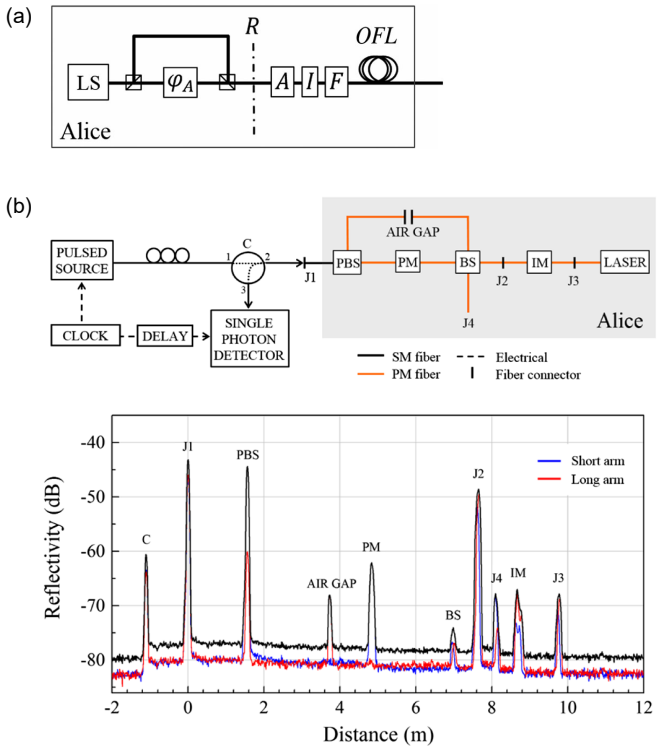

Figure 5.1: Reflection from different components of a QKD system under test (reprinted from Ref. [87]). (a) The components inside the QKD system under test are divided into two block separated by R dashed line: the front block to the right, and backreflection block to the left. (b) Experimental setup for reflectivity characterisation and an optical time-domain reflectometry trace showing reflectivity of each component.

pulses be ϕ. The total intensity of the backreflected pulse is

$$\begin{aligned} I &= (E_1 r_1 + E_2 r_2 e^{i\phi})(E_1 r_1 + E_2 r_2 e^{-i\phi}) \\ &= (E_1 r_1)^2 + (E_2 r_2)^2 + E_1 r_1 E_2 r_2 (e^{i\phi} + e^{-i\phi}) \\ &= (E_1 r_1)^2 + (E_2 r_2)^2 + 2E_1 r_1 E_2 r_2 \cos\phi \\ &\leq (E_1 r_1 + E_2 r_2)^2. \end{aligned}$$

One can see that if the two pulses are in phase ($\phi = 0$), the total intensity is higher than the sum of individual intensities. To give a clearer picture, let us assume that input amplitudes are equal $E_1 = E_2 = 1$, and the pulses reflect from a glass surface with reflectivity of 4%. The total reflected intensity will be as high as $\approx 16\%$ instead of $\approx 8\%$ expected from the sum of the reflection intensities. A similar concept is used to create a Bragg reflector where multiple layers of weakly reflecting materials could yield a total reflectivity approaching unity when the thickness of each layer matches the wavelength of the input light. The difference in our case is that Eve tunes the phase of each of her input pulse to compensate for the phase shift between the reflecting components instead of controlling the path length between the reflective surfaces. As an alternative to the active phase tuning, she could wait until a natural drift of the optical delays inside Alice randomly aligns the phases of her pulses for constructive interference, and execute the Trojan-horse attack in the limited time while the phases remain aligned.

A similar calculation could be done for a larger number of reflective surfaces. From this analysis, the general form of upper bound of reflected intensity is $I = [\sum_i (E_i r_i))]^2$, where E_i is the input amplitude at component i, and r_i is the reflectivity of that component. Figure 5.1(b) shows the reflectivity of each component inside a sample QKD system presented in Ref. [87]. We use this data to showcase the discrepancy between the two methods. We follow the original method and use the sum of reflections in the short and long arms (black trace in the plot) from all the components in the backreflection block (grey-shaded in the scheme). The reflectivities we have read from the plot are approximately -45 dB for PBS, -67.5 for air-gap, -62.5 for PM, -72.5 for BS, -50 for J2, -67.5 for J4, -65 for IM, and -67.5 dB for J3. Our calculated sum reflectivity is -42.74 dB, which matches -42.87 dB given in Ref. [87]. However the total reflectivity when all the reflected pulses are in-phase is -36.58 dB, i.e., significantly higher.

5.0.2 Solutions

We see two possible ways to tackle this problem. The first method is to change the total reflected light formula from $I = \sum_i (E_i r_i)^2$ (or equivalent expression of mean photon

number $\mu = \sum_i \mu_i$ as used in Ref. [87] to $I = [\sum_i (E_i r_i)]^2$. This will give a tighter bound on reflectivity, assuming all reflective surfaces at all possible wavelengths are characterized. However, fulfilling the latter assumption in practice may be challenging. A metrological method would need to be developed carefully.

An alternative is to assume the worst case that the total reflectivity from Alice's back-reflection block is unity, and assume that intensity of Eve's Trojan-horse pulse is reduced only by transmission loss in Alice's components in the front block. Although this method gives a pessimistic bound of reflection, it takes care of all unknown reflective surfaces and wavelength-dependent characteristics that might not have been characterized. This would also simplify the characterization procedures significantly. In fact, this option is already included in the draft group specification [6] in its Sec. 6.3. We advise the users to consider this method as their primary until a better option is developed.

5.0.3 Further deviation from model

In addition to the issue discussed above, another deviation of the model in the characterization method is that the reflected pulses from the front-block components (A, I, and F) are being neglected. Eve might treat these reflected pulses as, for example, additional coherent light sources serving as local oscillators, and this part of the scheme serving as her homodyne detector. We could neither prove nor disprove that the presence of these backreflections gives Eve an advantage. This deviation from the model needs to be studied.

5.0.4 Conclusion

We have shown that the experimental characterization method for QKD systems outlined in Refs. [87, 6] is insufficient, and an improved method should be developed. We have given a simple calculation and an example based on experimental data that shows that Eve could induce higher reflected intensity than originally predicted. We have suggested two possible solutions: a unity reflectivity assumption (which is already an option in the draft group specification [6]), and modification of the upper-bound reflectivity formula. Lastly, a further investigation of possible attacks taking advantage of reflections from the front-block components is encouraged.

Chapter 6

Security verification of practical QKD systems

Many cryptographic schemes experienced many unexpected behaviors of the physical device that deviated from theoretical assumptions. Worst, some of those flaws open side-channels for Eve or hackers to exploit, compromising the security. To improve the security of practical implementation, the developers need to characterize their system and close the existing loophole, while hackers continue to seek unknown loopholes in the patched system. This presumably unending loop of attacking and patching, in turn, drove the development of classical communications to the level of security we have today.

Many QKD protocols and schemes have been introduced in the past decades. Many proof-of-concept experiments have been realized; some developed to be fully functional QKD systems; some evolved even further to commercialization. As we learned from the classical system, no matter how high the level of security of the protocol is promised in theory, it is utmost necessary to test the function of the real system. Not only does this make sure that it is working as predicted in theory, but it also tests its resilience against any disturbance of Eve. Some of the systems have already been put to the testing and patching loop[138, 63, 67, 151, 91, 125, 97, 160]. Many vulnerabilities have been found, and many countermeasures have been developed. By repeating these loops of hacking and patching, the level of security, promised in theory, can be reached, eventually.

This section is a collection of examples of security verification of practical quantum key distribution systems. The goal of these studies is to find imperfections of the physical implementation of the respective QKD system or device under test. We then use that information to model possible attack models and introduce possible countermeasures. In

some cases, the countermeasure itself has been tested. This loop of testing(hacking) and introducing countermeasure(patching) is an important step toward the standardization of QKD, and the unconditional security promised in theory.

6.1 Eavesdropping and countermeasures for backflash side channel in quantum cryptography

This section is cited from our study "Eavesdropping and countermeasures for backflash side channel in quantum cryptography" published in [122].

Author contributions
With Paulo Vinicius Pereira Pinheiro Rolf T Horn, Jean-Philippe Bourgoin, and Shihan Sajeed, we experimentally characterize the backflash photon characteristics of the device under test. With Paulo Vinicius Pereira Pinheiro, and Vadim Makarov, we design and perform experiment on QKD receiver prototype. I analyzed and designed an attack model based on the experiment results. Norbert Lütkenhaus and Thomas Jennewein provided advice on countermeasures.

The security of QKD requires that the choice of basis of Bob's measurement is not known to Eve. It has been known for a long time [112] that a reverse-biased p-n junction in a silicon avalanche photodiode in Geiger mode emits light upon the detection of a photon. Chynoweth and McKay [24] reported a detailed study of the phenomenon and predicted that the light emission originates due to the recombination of the energetic electrons and holes in the avalanche breakdown region. Subsequently, several other papers stated distinct possible causes for the phenomenon and quantified this emission [163, 23, 43, 75, 10, 116, 56]. In 2001, Kurtsiefer and his coworkers [74] raised the question: can this emission from the detectors employed in practical quantum communication systems affect the security? The outcome of their study suggested that the backflash photons might leak information about the detection to Eve, though the leakage of information was not quantified. Recently, a study about the backflash in InGaAs/InP avalanche photodiodes (APDs) was done [103]. The latter also suggests the possibility that Eve could measure the state of backflash photons and learn about detection in the receiver without causing errors in the key.

The quantum state of the backflash photons is not expected to be correlated to that of the photon that triggered the effect. However, and unfortunately, from a security point of view, the backflash photons may pass through other security-critical components of Bob's receiver and carry out information about the state of those components back to

the channel. For example, in polarization-based QKD with a passive basis-choice scheme, backflash photons from the horizontal (vertical) detectors will come out into the channel horizontally (vertically) polarized when they pass different arms of polarization beam-splitters (PBSes). In this case, Eve can measure the polarization of the backflash photons and predict with high probability which detector they originated from, thus compromising the security. Another possible method of distinguishing backflash photons from different channels is monitoring the difference in time delay of backflash photons from each channel. However, for the device studied in this article, preliminary tests have shown that the difference in time delay of backflash between channels is not sufficiently distinguishable to be used to determine the source of backflash. Thus, we do not investigate the latter method here.

This section is organized as follows. In Section 6.1.1, we characterize backflash emission probability from APD and photomultiplier tube (PMT) instead of InGaAs/InP studied in Ref. [103]. Furthermore, in Section 6.1.2, we characterize backflash photons from a free-space polarization encoding receiver and use that information to demonstrate a practical attack on the receiver. We also quantify the information leakage to Eve in this attack scheme. In Section 6.1.4, we introduce a countermeasure for this attack that reduces the reverse transmission efficiency of the receiver from the detectors to channel to reduce information leakage. We also introduce a characterization procedure and modify the key rate equation to take into account the remaining information leakage. We conclude in Section 6.4.4.

6.1.1 Characterization of backflash emission

In order to study the effect of backflash photon emission during the avalanche breakdown, a series of experiments are conducted on two different types of detectors. The first device tested is a Si-APD detector module (Excelitas SPCM-AQRH-12-FC) with a circular active area of 180 μm and peak photon detection efficiency of 0.7 at 700 nm [7]. The second device tested is a PMT (Hamamatsu H7422P-40), which has a GaAsP photocathode, with 5 mm diameter and a peak photon detection efficiency of 0.4 at 580 nm [8]. Both are thermoelectrically cooled.

Si avalanche photodiode

The first step in quantifying the information leakage is to find the probability of backflash P_b, i.e., the probability that a detection (click) leads to emission of at least one photon

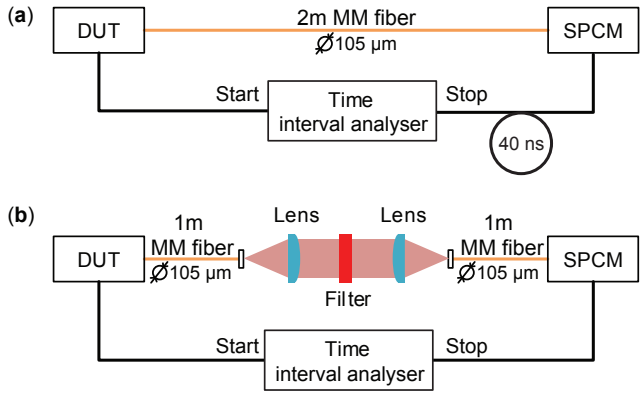

Figure 6.1: Setup for measuring probability of backflash emission. (a) Two identical APDs are connected with a 2 m long multimode (MM) fiber causing 10 ns optical delay between the two detectors. An electronic delay line of 40 ns is added so that the backflash photons from SPCM could also be recorded. (b) To perform spectral analysis, a free-space interference narrowpass filter is added to the setup. The filter represents one often used at the entrance of a practical QKD receiver.

that leaks out of the detector. To find the value of P_b, we perform a measurement using the setup in Fig. 6.1(a). Two identical APD modules, one marked as device under test (DUT) and another marked as single-photon counting module (SPCM), are connected by a 2 m long 105 μm core diameter multimode fiber (Thorlabs M43L01). Click coincidences between them are recorded by a time interval analyzer (Stanford Research Systems SR620). In this setup, we record clicks caused by dark counts in the DUT. We record until the total clicks in DUT reach $N = 10^6$, and plot the histograms of coincidence clicks between the two detectors in Fig. 6.2. The right-most peak represents the backflash photons from DUT coupled through the fiber and detected by SPCM, which occur ≈ 10 ns after the detections in DUT owing to the optical delay. We have added a 40 ns electrical delay so that the coincidence click appears at a delay of ≈ 50 ns in the plot. This also allows us to see the backflash from SPCM recorded by DUT, which is the left-most peak having a similar shape but time-inversed. The shape of the coincidence peak roughly matches that of the current flowing through the APD I_{APD}, which we have measured using a small resistor added at the APD's cathode and a wideband differential oscilloscope probe. We divide the histogram into three regions. Region I shows rapid increase in coincidence counts that resembles the exponential increase of the number of avalanche electrons flowing through the APD. Region II shows decay in the coincidence counts resembling the decrease of avalanche electrons owing to the voltage across the APD dropping as its capacitance discharges. Region III is

where the voltage across the APD is further lowered below breakdown by the quenching circuit. At that time the photon emission drops to near zero. The rough match between the current shape and the photon emission suggests that the backflash photons originate from the electric current across the APD during the avalanche.

We count coincident clicks C within the right-hand peak. Here, we take into account channel transmission efficiency $T = 0.97$, and average detection efficiency of the SPCM in 500–900 nm spectral band $\eta = 0.6$ [7]. Since the SPCM can only detect photons efficiently in this narrow spectral band, our measurement provides only a lower bound estimate of $P_b \gtrsim C/(\eta T N)$. We note that this and subsequent calculations of backflash probability are approximate in the case where $P_b \ll 1$. For this specific setup, there are 37643 coincident detections, corresponding to $P_b \gtrsim 0.065$. Furthermore, we have measured the electrical charge flowing through the APD per avalanche, by monitoring the current consumption from the high-voltage bias source. We have found that the APD under test passes on average $n_{\mathrm{e}^-} = 2.7 \times 10^8$ electrons through the APD per avalanche. The probability of backflash photon emission per avalanche electron $P_{\mathrm{e}^-} \gtrsim P_b/n_{\mathrm{e}^-} = 2.4 \times 10^{-10}$. We remark that a detector circuit that reduces n_{e^-} would be expected to have lower backflash.

While the wideband measurement above is imprecise, many free-space QKD setups employ a narrowband spectral filter at Bob's entrance, in order to cut background light entering Bob [18, 57, 73, 72, 15]. The same filter would restrict the backflash emission to the narrow band that can be measured much more precisely in our setup. We have added a free-space narrowpass filter with center wavelength of 808 nm and bandwidth of 3 nm [see Fig. 6.1(b)], in order to mimic spectral filter inside a practical QKD receiver [15]. We have repeated the counting process and found 2306 coincident detections. At this specific wavelength, the SPCM has detection efficiency of 0.62 [7]. The coupling efficiency of the channel in this setup is $T = 0.83$. The probability of at least one backflash photon leaking through this filter is $P_b^{\mathrm{filter}} = 4.5 \times 10^{-3}$. The spectral filter indeed reduces the emission significantly, which reduces the information leakage as we prove later in Section 6.1.4.

We have performed another measurement to characterize the spectral distribution of the backflash photons, using a sensitive spectrum analyzer (Acton Spectrapro 2750). Unfortunately, we could not fully calibrate the spectrum analyzer for this specific setup, and the result is only qualitative. The measurement indicates that the backflash emission is broadband, spanning continuously from 550 nm to >1000 nm with a gentle peak around 900 nm (see Section 6.1.3). This broadband characteristic leads to the possibility of including a narrow bandpass spectral filter in the system. The filter limits the wavelength range in which the backflash probability needs to be characterised, reduces the backflash emission from Bob, and thus reduces the information leakage.

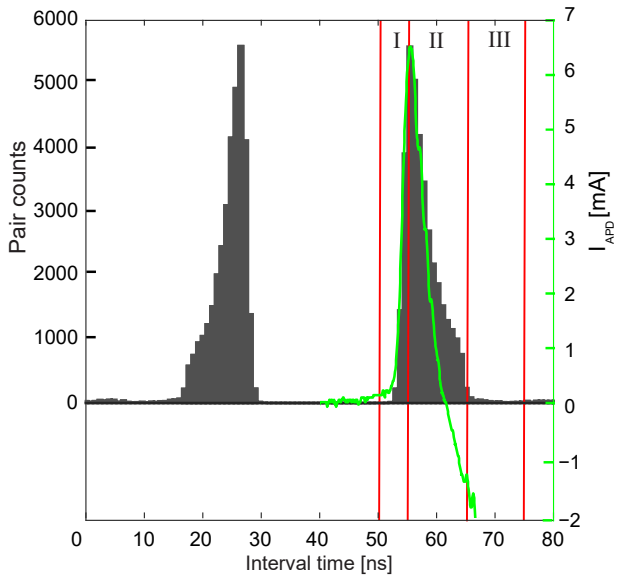

Figure 6.2: Histogram of time-intervals (dark grey) measured from the coincident clicks from the setup in Fig. 6.1. The peak on the right is backflash from DUT detected by SPCM. Regions I, II, and III of the histogram represent different stages of detector operation cycle. The shape of histogram resembles the APD current I_{APD} (green line, measured separately). The current shape is not exact owing to a finite common-mode rejection ratio of the differential probe used to measure I_{APD}. The apparent abrupt drop of current at the border between regions II and III is common-mode interference from the quenching circuit that lowers the bias voltage and thus ends the avalanche. This coincides with a drop of photon emission almost to zero. The peak on the left is backflash from SPCM detected by DUT.

Photomultiplier tube

Photomultiplier tube (PMT) is another type of detector widely used for its larger sensitive area and moderate dark count rate [52]. We have replaced DUT in Fig. 6.1 (a) with a PMT unit. Since the dark count rate of the PMT is low, additional weak laser pulses have been coupled to the active area of PMT to induce clicks. After recording 10^6 counts in the PMT, we have found fewer than 100 coincidences for both the fiber and free-space setups. This coincidence level is close to the dark count level of the SPCM, implying that the probability of backflash in PMT is negligible within the spectral range of our measurement.

6.1.2 Eavesdropping experiment

In this section, we experimentally quantify Eve's ability to identify which detector the backflash photons originated from, by measuring the backflash photon's polarization state. Bob's receiver used in this test is an integrated receiver built by INO (National Optics Institute of Canada) designed for a free-space passive polarization encoding QKD system running at 785 nm. Fig. 6.3 shows its optical scheme. The receiver consists of a pinhole to prevent spatial mode attack [135], coupling lens to focus incoming beam into optical fibers, and an integrated optics module. The latter consists of a beamsplitter (BS) to passively select the basis of measurement and PBSes in each basis to discriminate the four polarizations of the incoming photons: horizontal (H), vertical (V), diagonal (D), and antidiagonal (A). Next, we characterize the backflash emission as a possible side channel.

Reverse loss and extinction ratio

As the photons back-propagate through the setup, they experience the reverse loss of the receiver, i.e., the loss from originating detector to the channel input. This could reduce probability that backflash photon leaks into the channel. The setup shown in Fig. 6.4 is used to estimate this loss. An 808 nm laser (wavelength close to the operating wavelength of the receiver) is connected to the receiver's output multimode fiber, one channel at a time. The laser power at the end of receiver's fiber is $P_1 = 40\ \mu$W. We adjust the polarization controller PC to maximize throughput power, providing an upper bound of the reverse transmission. We then measure laser power P_2 emitted at the front of the receiver module, between the focusing lens and receiver's pinhole in 6.4. The reverse transmission efficiency of the receiver for the optimum polarization is then $T_b = P_2/P_1$. We have measured the average reverse transmission efficiency over all four channels of this receiver $T_b \approx 0.091$

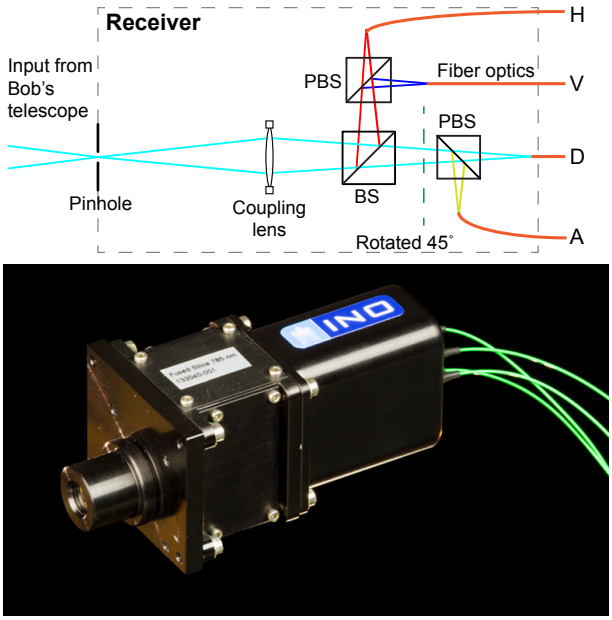

Figure 6.3: Receiver designed by INO working as a passive basis choice polarization analyzer at 785 nm. Top: the important optical components consists of a pinhole, coupling lens, beamsplitter (BS), and polarizing beamsplitters (PBSes). Bottom: photo of the receiver. Four multimode fibers lead to the four detectors (not shown).

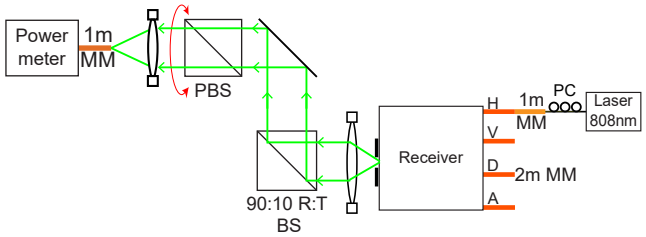

Figure 6.4: Setup for measurement of the reverse propagation loss and polarization extinction ratio. An 808 nm laser is connected to each of the output channels of the receiver, one at a time. A 90:10 reflection:transmission (R:T) ratio beamsplitter diverts the reverse propagating beam to the measurement unit. The latter consists of a fiber-coupled optical power meter, and a rotating PBS to measure power and polarization extinction ratio of the reverse propagation beam. A polarization controller PC is used to maximize throughput power from each receiver channel.

Table 6.1: Reverse propagating extinction ratio measurement of Bob's setup. The photons from H and V channel could be distinguished with high probability. The measured extinction ratios of A and D channels are low, presumably owing to polarization becoming elliptical at reflections in the measurement unit.

Output channel	max		min		Extinction ratio
	Angle (deg)	Power (μW)	Angle (deg)	Power (μW)	
H	3	25.0	91	0.15	167
V	94	19.8	1	0.03	660
D	315	20.7	223	1.94	10.7
A	49	23.5	141	3.69	6.4

(the individual values lie in the range 0.088 to 0.094). Assuming backflash photons are randomly polarized, their transmission should be approximately half of this upper bound.

Next, we demonstrate Eve's ability to distinguish the originating channel of backflash photon. For that, we measure polarization extinction ratio of the reverse emitted beam from the receiver. In Fig. 6.4, a 90:10 reflection:transmission (R:T) ratio beamsplitter is added to divert the outgoing beam from the receiver to a measurement unit consisting of a PBS and a fiber-coupled optical power meter. This additional setup has throughput efficiency $T_e = 0.60$. For each receiver channel input, we rotate the PBS to find a pair of angles that results in maximum and minimum power at the power meter. The optimal angles for each channel and respective extinction ratios are shown in Table 6.1. The drastically lower extinction ratio in D and A polarization is likely a result of polarization distortion caused by Fresnel effect on the dielectric mirror and the 90:10 BS used by Eve. These reflective surfaces were aligned at a certain angle along the axis corresponding to V polarization. This alignment distorted the diagonal polarization of the reflected beam, by inducing a phase difference between its H and V polarization components. In real eavesdropping, Eve can correct this polarization distortion using a phase compensator or waveplate. She can also split the incoming backflash photons into two PBSes oriented at the angles that yield the highest extinction ratios in both bases. This should allow her to distinguish the photons from all four channels with high probability.

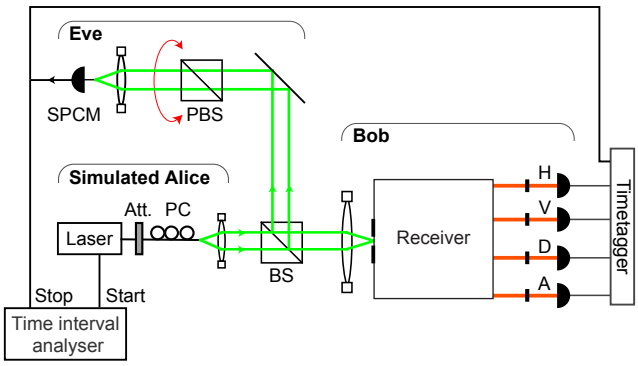

Figure 6.5: Eavesdropping setup for timing characterization and proof-of-principle attack. The 90:10 R:T BS diverts photons from Bob to Eve's detector. Eve's setup consists of a PBS that can be rotated to find the optimal angle for Eve to distinguish the source of backflash photon. The time interval analyser (TIA) is used to find the time delay of the backflash photon in the channel. The timetagging unit records coincidence time between Bob's and Eve's detections in the proof-of-principle attack.

Timing of backflash photons through the receiver

The previous experiment suggests that by measuring the polarization of the backflash photons, Eve could estimate which detector they originated from. However, in real life scenario, Eve's detection might not solely be from the backflash photons; it can be a result of stray light in the channel, reflection of Alice's signal from Bob's optical components or dark counts in Eve's detector – all unwanted noise. To avoid those unwanted signals, Eve needs to synchronize her measurement apparatus with Alice and Bob's signal pulses, and activate her detector at a specific time when the backflash photons are expected to arrive. The synchronization can be done by monitoring Alice's and Bob's signals prior to the eavesdropping. This section demonstrates a practical setup to measure timing characteristics of the backflash photons.

The experimental setup is shown in Fig. 6.5. A train of 3 ns wide laser pulses with 200 ns period is sent to Bob's receiver to simulate signals from Alice. The detector used as DUT in Section 6.1.1 is connected to one channel of the receiver at a time. A time interval analyzer (TIA) is used to record the coincidence time between the signal sent by Alice and Eve's SPCM clicks. In Fig. 6.6, we plot two histograms of the coincidence time from the APD in H channel. The green histogram is the coincidence time when DUT is powered off. Thus the detections in Eve resulted from reflections from the receiver's optical components. The positions of the peaks correspond to optical delay between reflective components in

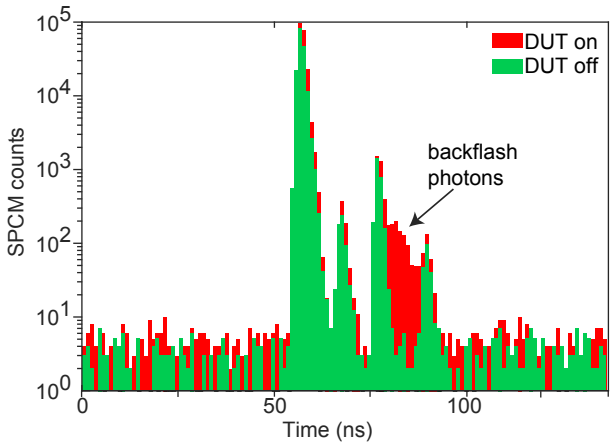

Figure 6.6: Histogram of time intervals between emitting Alice's laser pulse and detection in Eve's SPCM. The histogram with DUT powered on (red) has an area of coincidence peak well above the level when DUT is powered off (green). The timing of this area matches the optical time delay between Eve's receiver and DUT, indicating backflash emission. The other peaks are optical reflections in the setup (see text for details).

the setup and Eve's SPCM. The leftmost peak is a result of backreflection off the free-space optics at the front of Bob, such as his lenses and BS. The next peak matches the time delay from fiber splices in the receiver's fiber, indicated by short bars in Fig. 6.5. The third peak is the backreflection from the APD (in H channel only, as the fiber in the other channels has been terminated with matching gel that eliminates backreflections). The time delay of the right-most peak matches the round-trip of triple reflection between the APD and fiber splice. The red histogram is the coincidence time when DUT is powered on. Extra counts due to backflash photons can clearly be seen at 80–87 ns. The time delay matches optical delay between DUT and Eve's SPCM. Since the coincident counts of backflash events are ≈ 1.5 orders of magnitude higher than the back-reflection and noise level, the probability of Eve registering back-reflected pulses within this time window is small. Similar result could be seen when connecting the DUT to V, D, and A channels.

6.1.3 Spectral distribution measurement

Figure 6.7 shows the spectral distribution of backflash emission measured with a sensitive spectrum analyzer (Acton Spectrapro 2750). Due to difficulties we have encountered in spectrometer calibration, this measurement has a large margin of error comparing with

the narrow-band filter measurement at a specific wavelength. Thus, we omit this result from the main Article. Even so, this measurement shows some important characteristics of backflash emission. The backflash emission is broadband, spanning continuously across our range of measurement from 550 to 1000 nm with a gentle peak around 900 nm. This suggest the possibility of having backflash emission beyond our range of measurement. This emphasizes the necessity of adding the narrow-band filter to ease the characterization process and limit the information leakage.

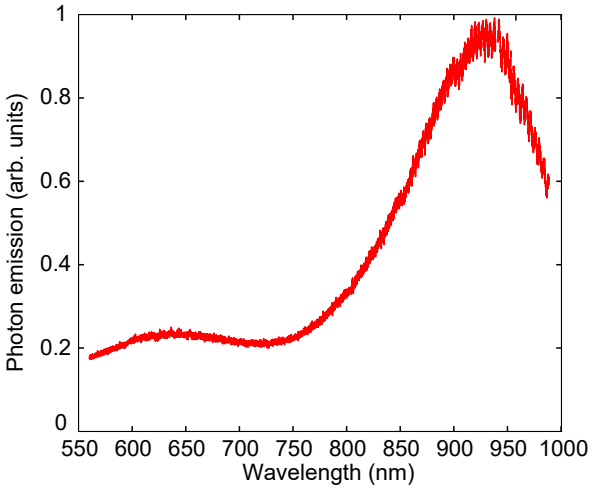

Figure 6.7: Spectral distribution of backflash.

Proof-of-principle eavesdropping demonstration

We next emphasize the threat of this attack by demonstrating Eve's performance using a practical setup, shown in Fig. 6.5. In this experiment, we demonstrate Eve's ability to distinguish backflash emissions in one basis, between H and V channels. We only consider those photons that are coupled back to the optical channel and thus could carry information to Eve. We first repeat the alignment procedure as described in Section 6.1.2 by sending laser beam through the receiver's fibers, and rotating the PBS in Eve to find two optimal angles where the detection rate from the laser sent through Bob's H channel is maximum but V channel is minimum, and vise versa. Bob is then equipped with four powered-on APDs, one at each channel of the receiver, as in a real QKD setup. As seen in Section 6.1.2, Eve needs to register the coincidence counts within a specific time window to filter out back-reflection events. For that, we replace TIA with a timetagger (Dotfast Consulting

78-ps resolution 8-channel module) set to register the events where Eve's detector clicks within 25–30 ns after Bob's detection, which matches the time delay between Bob's and Eve's detectors. A train of 3 ns wide laser pulses with 200 ns period are sent to Bob to simulate QKD signal pulses from Alice. For each orientation of Eve's PBS, we count the number of detections in Bob and coincidence count in Eve over 10 s. We record the ratio of coincidence events $R_{ij} = E_{ij}/B_i$, where B_i is the number of clicks in Bob's ith detector, and E_{ij} is the number of Eve's coincident clicks with Bob's ith detector when she sets her PBS angle to maximise clicks from Bob's channel j. For example, R_{HH} represents probability of a click in Bob's H channel causing a coincident click while Eve aligns her PBS to measure signal from H channel, i.e., the probability that Eve gets a correct detection.

The probability of Eve gaining information (about H channel detection) is the chance of getting correct detection (R_{HH}) less the chance that she gets a wrong detection (R_{HV}). Note that the backflash probability P_b and reverse transmission efficiency T_b are already accounted in these coincidence ratios. Our measurements show that, for Bob's H detection, $R_{HH} = 5.00 \times 10^{-3}$ and $R_{HV} = 1.45 \times 10^{-3}$, causing information leakage of 3.5×10^{-3}. For Bob's V detection, $R_{VV} = 5.69 \times 10^{-3}$ and $R_{VH} = 3.66 \times 10^{-3}$, causing information leakage of 2.0×10^{-3}. From the calibration measurements we have expected the information leakage to be less than $\eta T_e T_b P_b/2 = 1.1 \times 10^{-3}$, which poorly matches the leakage observed in the eavesdropping experiment. We could not explain this discrepancy.

This result shows that Eve could learn a fraction of Bob's detections by monitoring the backflash photons. On the one hand, the information leakage is small, and we don't have the spectral filter in Bob in this experiment. On the other hand, our Eve's setup is not an optimal one for the attack. Proper countermeasures both in physical implementation and in post-processing step need to be considered.

6.1.4 Countermeasure

In this section, we discuss about possible countermeasures for attacks exploiting backflash photons. For physical implementation, using PMT can eliminate the possibility of generating backflash photons (although this conclusion is subject to the limitations of our measurement in Section 6.1.1). Another possible countermeasure is using measurement-device-independent QKD (MDI-QKD) [85, 84], in which the detection outcomes are public, thus Eve gains no new information from the backflash. However implementation of MDI-QKD in free-space is challenging [126, 77, 31]. If a non-MDI-QKD system uses APDs, the information leakage could be limited by decreasing reverse transmission efficiency T_b either by adding narrow-band spectral filter as shown in Section 6.1.1, or an optical isolator.

These measures could reduce but not eliminate the leakage of information. The remaining leakage needs to be taken into account when calculating the required shortening of the key during privacy amplification.

The following procedure could be employed. Bob follows the procedure in Section 6.1.1 to find the APD's probability of backflash P_b and receiver's reverse transmission efficiency T_b. This T_b includes all optical isolators and filters added to the receiver to limit the information leakage. If Bob does not include a narrow-pass filter, these parameters need to be characterized in a very wide spectral range, because typical free-space optics and air are transparent in a wide spectral band. This wide spectral characterization will be challenging. However, if a band-pass filter is used, it is sufficient to characterize the parameters over its spectral pass-band. From the result in Section 6.1.2, it is reasonable to assume that in the worst case, with ideal equipment, Eve could distinguish the origin of backflash photons with certainty. The information leakage to Eve is then $P_E = P_b T_b$. In other words, a fraction P_E of Bob's detections is tagged by Eve without disturbing the quantum state or inducing error. Then the privacy amplification for QKD with tagged signal [51, 88] can be used to take care of the information leakage.

As an example, let us consider the key rate equation for the Bennett-Brassard 1984 (BB84) protocol in QKD system with single-photon signals. Under the backflash attack, the secret key rate per signal sent by Alice becomes

$$l \geq AP_{det}(1 - h(\frac{e}{A})) - leak_{EC}, \tag{6.1}$$

where P_{det} is the probability of detection per signal, e is the error rate, $h(x) = -x \log x - (1-x)\log(1-x)$ is the binary Shannon entropy, and $leak_{EC}$ is the portion of key disclosed during error correction. The correction term $A = (P_{det} - P_E)/P_{det}$, where P_E is the information leakage calculated in the characterization step above.

The theoretical analysis in this paper considers only the worst-case scenario where Eve has the ability to collect and distinguish all backflash photons and map them to the raw key in Alice and Bob. This analysis also provides only the lower bound on the secret key rate, which could be improved by more careful analysis.

6.1.5 Conclusion

We have quantified the backflash emission of photons from APD-based single-photon detectors, and verified that these photons can be used by an eavesdropper to learn about the key in QKD systems. We have found that, for a system without spectral filter, at least 0.065 of

the clicks in actively-quenched Si detector module result in backflash. This probability is reduced by a factor of 14 when a narrowband spectral filter is added, suggesting the latter is an efficient countermeasure. For PMT the backflash emission is negligible within the sensitivity of our measurement. Our experiment with a real polarization-encoding QKD receiver shows that Eve can distinguish polarization of backflash photons with near certainty. The proof-of-principle attack shows that Eve could learn 2.0×10^{-3} fraction of raw key using our today's imperfect setup. The information leakage may be higher for an ideal Eve. To close this loophole, we discuss a procedure to characterize the system and quantify Eve's information, then modify the key rate equation to take care of the information leakage due to backflash emission. We hope that our study will contribute to the development of certification and standardization of practical QKD against side-channels.

6.2 Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence

This section is cited from our study "Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence" published in [22].

Author contributions
Vadim Makarov and Thomas Jennewein provided advise on experimental setup. Katanya B. Kuntz wrote program to generate phase hologram for the SLM. I wrote a programs to control and synchronize the experiment setup. I performed experiment with assistance of Anqi Huang, Jean Philippe Bourgoin, and Shihan Sajeed. With Katanya B. Kuntz, we process the experiment result and analyze practical limit of the attack. Yanbao Zhang and Norbert Lütkenhaus provided the theoretical limit of the attack under turbulence.

A widely studied implementation of QKD utilizes free-space communication between two parties (Alice and Bob) through the atmosphere [159, 37, 119, 111, 81, 124, 172], which allows for long distance point-to-point links on the order of a hundred kilometers. This communication distance can be extended even further to the global scale by introducing satellite-based QKD systems [158, 15, 173, 124, 81, 172, 161, 21]. However, free-space communication can be vulnerable to an eavesdropper attack, such as when Eve precisely controls the incidence angle of an attack laser directed at Bob's QKD receiver. Directing a laser in this way can induce a change in the measurement efficiencies of one (or more) detection channels, which enables Eve to do an intercept-resend (IR) attack that may compromise the system's security [135, 127].

The success of this spatial mode attack depends on the eavesdropper's ability to precisely maintain specific beam angles to a free-space QKD receiver, which attacks different detection channels. Atmospheric turbulence could compromise or even prevent such an attack as turbulence causes a beam to randomly wander along its trajectory, as well as inducing various optical aberrations such as astigmatism, defocus, coma, etc. Stronger turbulence conditions result in a larger variance in the amount of beam wander [157]. Consideration of these physical limitations on Eve is not usually included in the theoretical security analysis of a system, but can be useful to verify whether an attack is feasible under more realistic conditions.

In this study, we experimentally determine the minimum strength of atmospheric turbulence that could prevent a successful attack on our free-space polarization-based QKD receiver by emulating atmospheric turbulence using a phase-only spatial-light modulator (SLM). Since there are limitations on how well adaptive optics can correct for turbulence, our work explores to what level Eve must correct her attack beam to still be successful [80, 78]. We assume that the sender (Alice) and the receiver (Bob) only monitor the total count rates (as opposed to the rates of individual channels), and that they use a non-decoy state BB84 protocol [13]. We also assume that Eve has access to a weak coherent pulse source and state of the art photo-detectors, and does not have a quantum repeater. Furthermore, we assume that Eve cannot replace the quantum channel with a lossless channel. We find that an attack on our free-space receiver could still succeed if Eve can correct the tip-tilt mode for turbulence as strong as $r_0 = 1.53\ cm$ (assuming an initial beam diameter of 20 cm), where r_0 is the atmospheric coherence length. This result defines an "unsafe radius" of 543 m around Bob's receiver in typical sea-level turbulence conditions where Eve's attack could be successful if done within this radius.

First we discuss our SLM setup used to emulate atmospheric turbulence, and how we verified its accuracy and reproducibility in Section 6.2.1. Then we describe the components and operation of our free-space polarization-based QKD receiver under test in Section 6.2.2. In Sections 6.2.3 and 6.2.4, we discuss the results from spatial mode attacks performed in various turbulence strengths, following a similar procedure to Sajeed *et al.* in Ref. [135]. Finally, in Section 6.2.5 we discuss an entanglement breaking scheme proposed by Zhang *et al.* in Ref. [174], to theoretically verify if there exists an attack strategy for Eve, even if Alice and Bob know about their detection efficiency mismatch, and monitor the statistics of all possible detection outcomes. We conclude in Section 6.4.4.

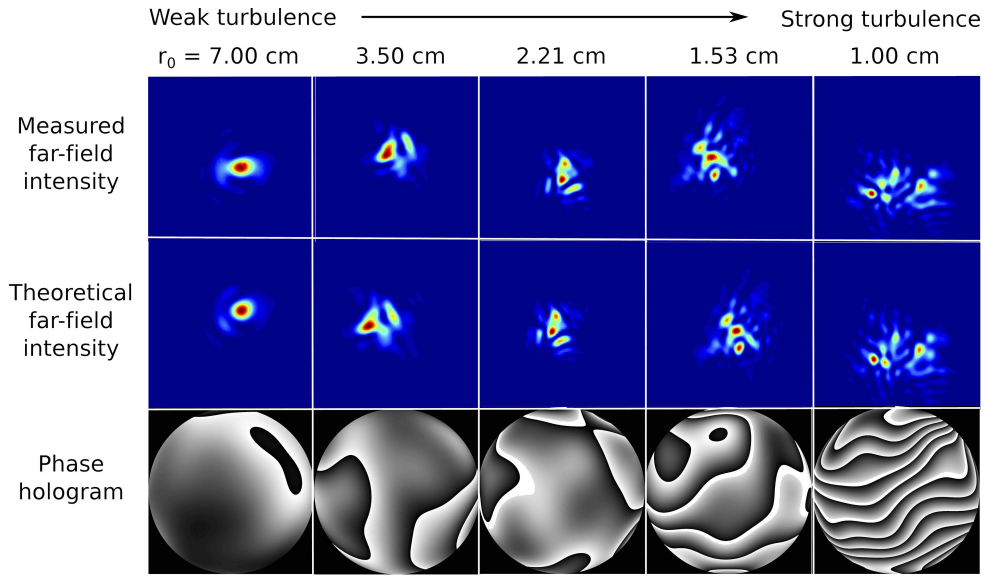

Figure 6.8: Comparison between measured and theoretical far-field intensity distributions of a laser beam corresponding to one of 29 SLM phase holograms per turbulence strength (r_0) for a beam with $D = 20\ cm$ and $\lambda = 532\ nm$. The greyscale in the holograms represents a 0 to 2π phase range. The results show our SLM setup accurately emulates a range of turbulence strengths.

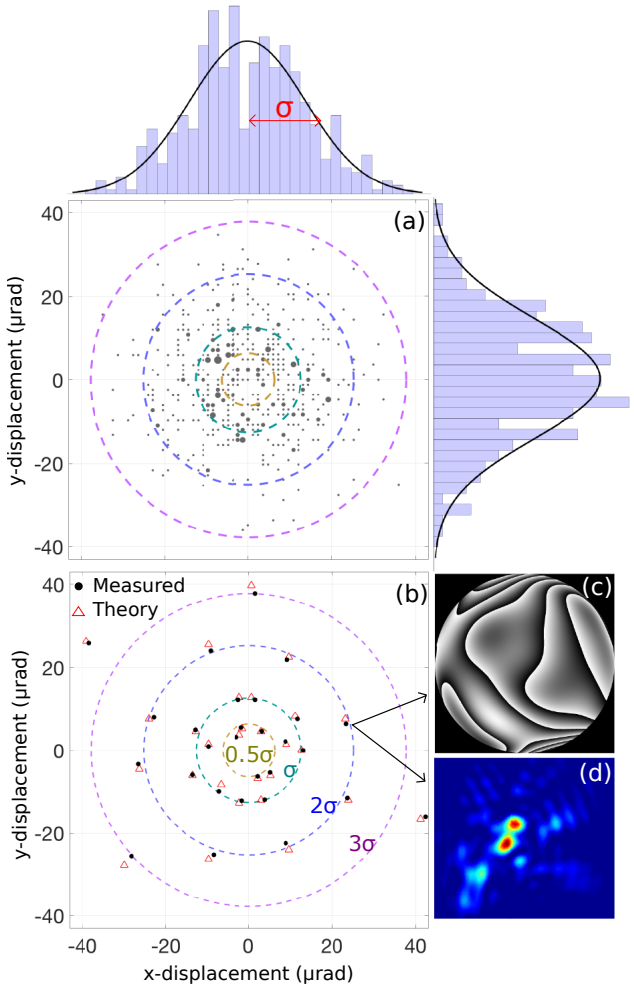

Figure 6.9: Turbulence emulator characterization for $r_0 = 1.00\ cm$, $D = 20\ cm$, and $\lambda = 532\ nm$. (a) Simulated centroid displacements corresponding to 500 phase holograms (σ is the 2-axis standard deviation). The diameter of each data point is proportional to the count frequency. The centroid displacement distribution is normally distributed along both axes in agreement with Eq. (6.3). (b) Comparison between measured and simulated centroid displacements for a subset of 29 holograms. This subset was chosen to represent the normal statistical distribution of the 500-hologram set. The measured values are within error of most theoretical predictions (error bars for measured data are represented by diameter of data points). (c) Phase hologram and (d) far-field intensity distribution corresponding to one centroid data point.

6.2.1 Turbulence emulator

We use a phase-only spatial light modulator (SLM) to emulate a turbulent QKD channel in the lab. One advantage of using a SLM as opposed to performing the experiment outdoors is the ability to generate a range of turbulence strengths, from weak upper atmosphere to stronger sea-level conditions. In addition, by performing our experiment in a laboratory, we are immune to the unpredictability of an outdoor environment, allowing us to repeat the same attack angles on our free-space QKD receiver under reproducible turbulence conditions.

Our model uses the 'thin phase screen approximation' which emulates turbulence using a single random phase screen in the aperture of the receiver, as opposed to requiring two holograms to model multiple parameters that incorporate both phase and amplitude variations [133]. We assume that Eve's laser can mimic the intensity variations caused by turbulence (scintillation) [38]. Note that the absence of these fluctuations could arouse Alice and Bob's suspicion of an eavesdropper in the channel, although fluctuations on the time scale of scintillation at a second or less are rarely monitored in practice.

In order to reproduce the random statistics of turbulence, we load a series of 29 phase maps per turbulence strength on the SLM to distort the optical wavefront. The strength of the turbulence is completely characterized by the ratio of the initial beam diameter, D, to the atmospheric coherence length, r_0; turbulence dominates over diffractive effects when $D/r_0 \gg 1$.

We generate our phase holograms based on the well-known Kolmogorov model [12] that uses a weighted superposition of Zernike polynomials for the basis-set [114]. There are several advantages to using Zernike polynomials to generate the holograms as their weights can be analytically calculated based on the turbulence strength [17]. Furthermore, Zernike polynomials directly relate to known optical aberrations, such as tip-tilt, defocus, astigmatism, coma, etc. Therefore, it is straightforward to characterize the SLM's ability to reliably and precisely emulate atmospheric turbulence by comparing calculated Zernike polynomial coefficients to those reconstructed by a measurement device, such as a wavefront sensor.

The radial phase function $\phi(\rho, \theta)$ that describes each hologram is given by a weighted sum of several Zernike polynomials as $\phi(\rho, \theta) = \sum_i c_i Z_i$, where Z_i and c_i are the Zernike polynomial and corresponding coefficient for the ith polynomial, respectively, following the Noll labelling convention and normalization constants [114]. We use 44 Zernike polynomials to ensure a complex spatial structure that can accurately emulate a range of atmospheric turbulence strengths.

Based on the Kolmogorov model [12, 17], if we assume that the Zernike coefficients are normally distributed with mean zero, then c_i are random drawings from distributions with variance σ_{nm}^2 defined as

$$\begin{aligned} \sigma_{nm}^2 &= I_{nm}(D/r_0)^{5/3}, \\ r_0 &= 1.68(C_n^2 L k^2)^{-3/5}, \\ I_{nm} &= \frac{0.15337(-1)^{n-m}(n+1)\Gamma(14/3)\Gamma(n-5/6)}{\Gamma(17/6)^2\Gamma(n+23/6)}, \end{aligned} \tag{6.2}$$

where C_n^2 is the refractive-index structure constant of the atmosphere, L is the path length through the turbulent atmosphere that has a constant C_n^2, $k = 2\pi/\lambda$, λ is the laser wavelength, and Γ is the Gamma function. The indices n and m are related to the Zernike polynomial order following the Noll labelling convention, where $n \geq |m|$ and $n - m$ is even [114]. We note that the subscript "n" of C_n^2 is not related to the index "n" used in the Zernike polynomials, but instead to the refractive index of the atmosphere. A single value of C_n^2 is used when calculating σ_{nm}^2 over each n and m indices for each atmospheric strength modelled. A large C_n^2 (small r_0) value corresponds to stronger atmospheric turbulence. An example of stronger turbulent conditions that could be found at sea level corresponds to $r_0 = 1.00\ cm$ over $L = 1\ km$ for $D = 20\ cm$ at $\lambda = 532\ nm$, whereas weaker conditions at high altitude corresponds to $r_0 = 7.00\ cm$ [12].

Since Zernike polynomials directly relate to known optical aberrations, we can use simple equations and measurement devices (CCD camera and wavefront sensor), to independently verify and characterize our turbulence emulator. Figure 6.8 shows both the simulated and measured far-field intensity distributions of a beam after its wavefront has been distorted by the SLM hologram. Each hologram shown is one example from a set of 29 holograms per r_0 value used to emulate how different strengths of turbulence would affect a 20 cm beam at 532 nm. We experimentally image the far-field by placing a camera in the focal plane of a lens that is located one focal length from the SLM. This arrangement maps the phase wavefront imprinted on the beam by the hologram into an intensity distribution at the camera plane. Note that we include an additional x-grating in the hologram (not shown for clarity) to spatially separate the first-order diffracted beam from the zeroth-order, as only the first-order beam contains the pure phase wavefront. The zeroth-order (and higher-order) diffracted beams were carefully blocked shortly after the SLM.

We also verify our turbulence emulator by examining the centroid deviations caused by each hologram. This is an important characterization as beam displacements due to turbulence could dominate Eve's ability to repeatedly send a beam at precise angles to the receiver. Beam wander is the strongest effect on average as the tip-tilt coefficients ($n = 1$,

$m = \pm 1$) have the largest weights overall [$I_{11} = 0.45$ from Eq. (6.2)], whereas defocus ($I_{20} = 0.02$) and astigmatism ($I_{22} = 0.02$) have a smaller contribution on average. Higher order aberrations can also cause centroid displacement, especially in the case of stronger turbulence.

There is a direct relationship between the tilt angle variance of centroid displacement for two uncorrelated axes σ^2 and the turbulence strength r_0, which is given by [157]

$$\sigma^2 = 0.364\left(\frac{D}{r_0}\right)^{5/3}\left(\frac{\lambda}{r_0}\right)^{5/3}. \tag{6.3}$$

Since this equation is independent of the method used to emulate turbulence, we can verify whether the 29 chosen phase holograms accurately portray the statistics of atmospheric turbulence both theoretically via computer simulations of far-field intensity distributions, and experimentally through our SLM setup. This independent verification ensures that the holograms are accurate, as well as that the SLM is correctly imprinting the phase mask onto the beam.

The centroid displacement data presented in Fig. 6.9 corresponds to low-altitude sea level turbulence ($r_0 = 1.00$ *cm* for a 20 *cm* beam). The simulated centroid displacements from 500 holograms are shown in Fig. 6.9(a). Each data point corresponds to a unique hologram [Fig. 6.9(c)] and far-field intensity distribution [Fig. 6.9(d)]. The simulated centroids follow a Gaussian distribution with a standard deviation σ that is in agreement with Eq. (6.3). These results confirm that the phase holograms we calculated properly emulate the statistics of low-altitude sea level turbulence, irrespective of the SLM setup. Similar tests were performed to verify the sets of holograms for each r_0 value tested in this experiment.

We compare simulated and measured centroid displacements of 29 holograms per r_0 strength in Fig. 6.9(b). The number of holograms used in the hacking experiment were limited to reduce data acquisition time and stability issues while scanning. Therefore, we chose 29 holograms from a larger distribution of 500 to emulate each r_0 strength. The holograms were chosen based on their centroid displacements being approximately 0.5σ, σ, 2σ and 3σ from the origin [along the dashed circles outlined in Figs. 6.9(a) and 6.9(b)], along with one histogram with no turbulence representing 0σ. The centroid results, along with the qualitative comparison between theoretical and measured far-field intensity distributions (Fig. 6.8), confirmed we had excellent agreement between theory and experiment for turbulence emulated by our SLM setup. The 29th hologram always emulates 0σ displacement with no turbulence. The contribution of each of the 29 holograms to the emulated turbulence in subsequent experiments is weighted by its probability of occurrence, which

follows a Gaussian distribution. This probability of occurrence is a definite integral of normalized Gaussian distribution over the annulus formed by the adjacent radii shown in Fig. 6.9(b). We refer to each annulus by the name of its inner radius, near which its holograms are located. The 0σ annulus, extending from 0 (where its hologram is located) to 0.5σ radius, has the weight of 0.1175. The 0.5σ annulus has the weight of 0.2760, 1σ of 0.4712, 2σ of 0.1242, and 3σ (extending to infinity) has the weight of 0.0111.

6.2.2 Test setup for QKD system

We use our turbulence emulator to study the effect of turbulence on free-space detection efficiency mismatch. Eve's experimental setup consists of two parts: the turbulence emulator (SLM) and the beam scanning unit, as shown in Fig. 6.16. Our source is a 532 nm continuous-wave laser that is first sent through a polarization beam splitter $\mathrm{PBS_E}$ (Thorlabs CCM1-PBS251) to transmit only horizontally-polarized light to the SLM, which ensures phase-only modulation. The beam's wavefront after the SLM represents propagation through atmospheric turbulence of a particular strength. We use a quarter-wave plate $\mathrm{QWP_E}$ (Thorlabs AQWP10M-600) to rotate horizontal light to circularly polarized to equalize the QKD receiver detector signals on the four polarization channels. Eve's scanning lens $\mathrm{L_E}$ is mounted on a two-axis motorized translation stage (Thorlabs MAX343/M), which scans the attack beam's angle. A half-wave plate $\mathrm{HWP_E}$ (Thorlabs AHWP10M-600) and neutral density filter $\mathrm{ND_E}$ (Thorlabs ND30A) are used to control Eve's intensity. Finally, the receiver is placed 13 m away from $\mathrm{L_E}$.

The QKD receiver under test is a prototype for a quantum communication satellite [15], which uses a passive basis choice to detect polarization-encoded light. Its telescope consists of a focusing lens L1 (diameter of 50 mm with a focal length $f = 250$ mm; Thorlabs AC508-250-A), and a collimating lens L2 (diameter of 5 mm with $f = 11$ mm; Thorlabs A397TM-A). The collimated beam of $\lesssim 2$ mm diameter then passes through a 50:50 beam splitter BS (custom pentaprism [15]), and a pair of polarization beam splitters PBS1 and PBS2 (Thorlabs PBS121). The purpose of PBS2 is to increase the polarization extinction ratio in the reflected path from PBS1. The four lenses L3 (Thorlabs PAF-X-18-PC-A) focus the beams into four multi-mode fibers, each with a core diameter of 105 μ m (Thorlabs M43L01), which are connected to single-photon detectors (Excelitas SPCM-AQRH-12-FC). We use one set of polarization optics and detectors to measure diagonal **D** and anti-diagonal **A** polarizations by rotating them 45 degree relative to the horizontal **H** and vertical **V** polarization detectors. We note that this receiver under test does not contain any active pointing system or adaptive optics.

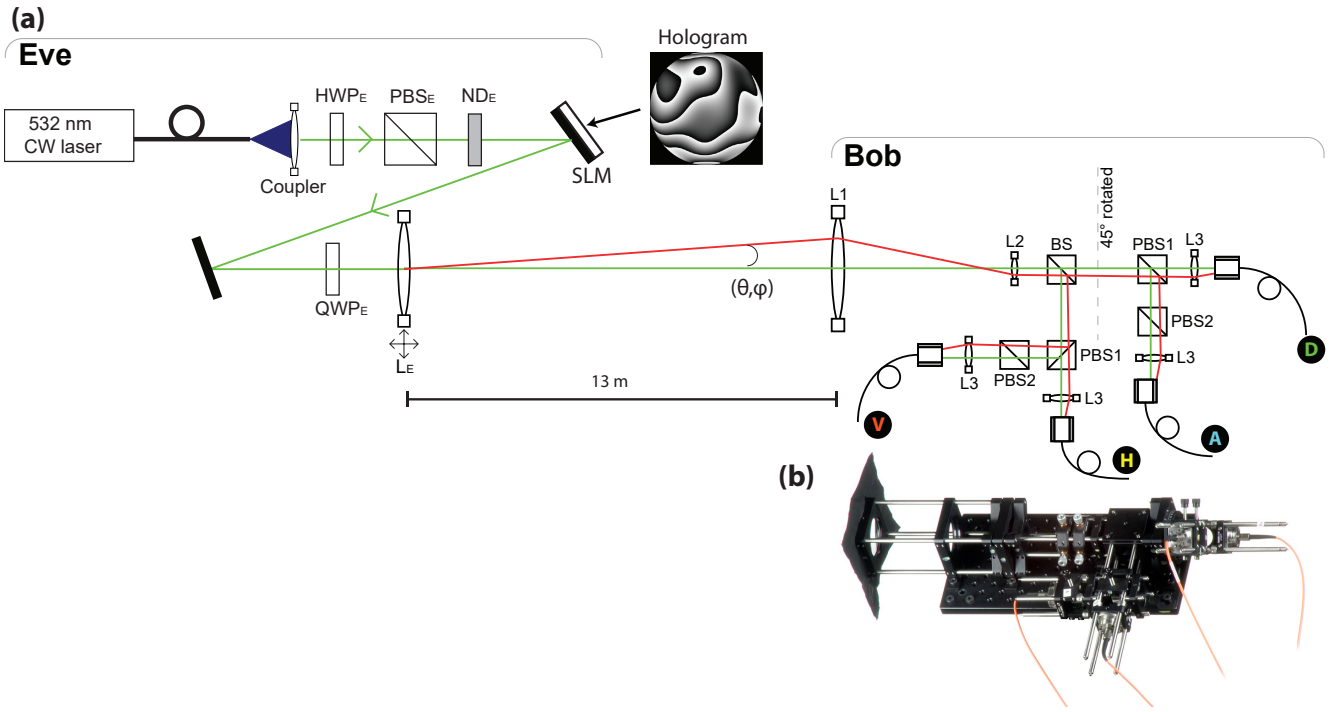

Figure 6.10: Scanning setup. (a) Experimental setup of our spatial mode attack in a turbulent channel, top view (drawing not to scale). The green central ray that is parallel to the optical axis denotes normal alignment of Alice's beam into Bob's receiver. The red rays show the optical path of Eve's scanning beam when tilted at an angle (θ, ϕ) via lens L_E. CW: continuous-wave; HWP: half-wave plate; QWP: quarter-wave plate; BS: beam splitter; PBS: polarization beam splitter; ND: neutral density filter; SLM: spatial light modulator; L: lens. (b) Photograph of the actual free-space QKD receiver for detecting polarization-encoded light.

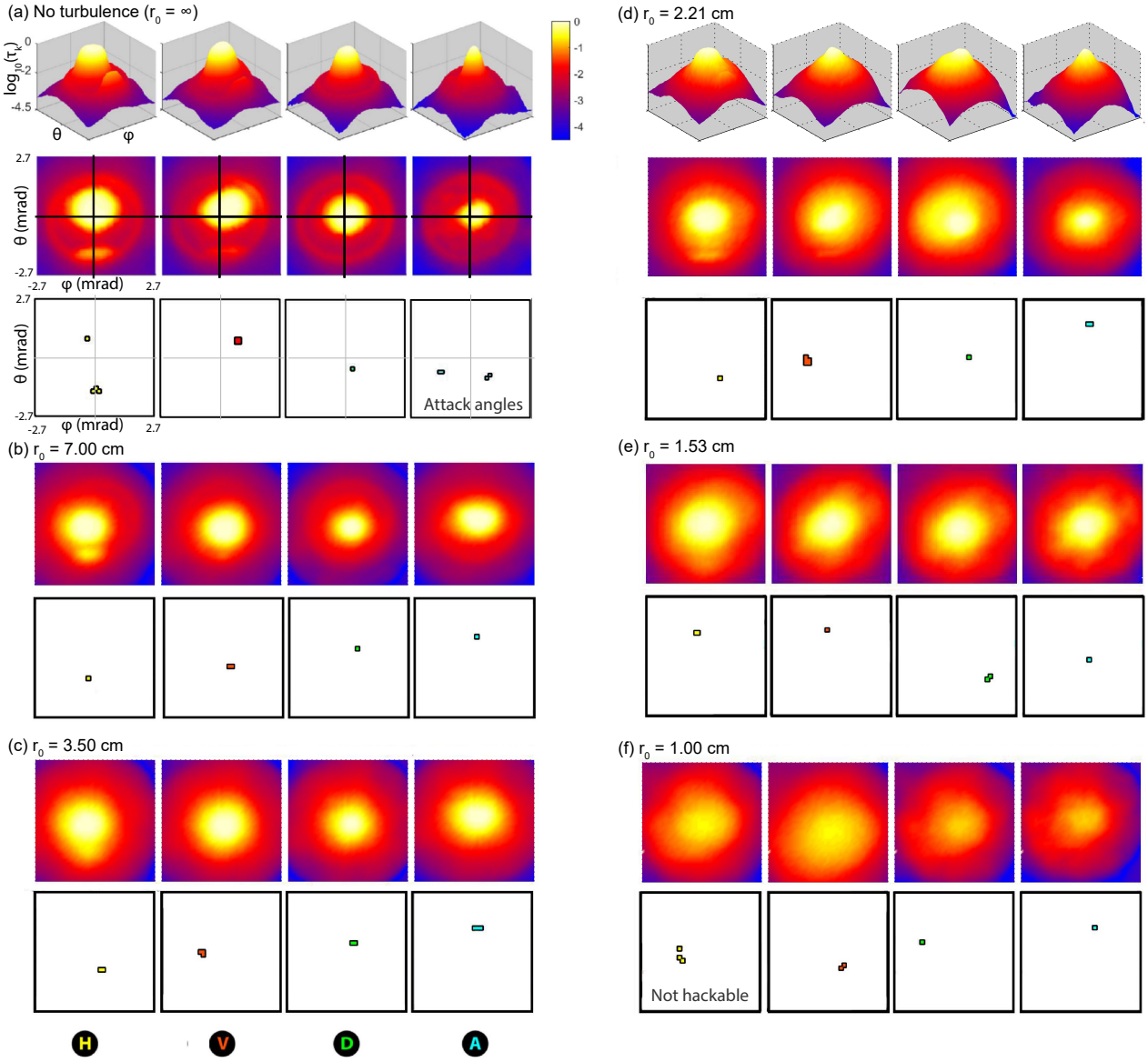

Figure 6.11: Normalized count rates τ_k for each detector $k = \mathbf{H}, \mathbf{V}, \mathbf{D}$, or $\mathbf{A}$ at different incoming beam angles (θ, ϕ), and the corresponding attack angles for different turbulence strengths r_0. The attack angles for the four polarization detectors are shown left to right as horizontal $\mathbf{H}$ (yellow), vertical $\mathbf{V}$ (red), diagonal $\mathbf{D}$ (green), and anti-diagonal $\mathbf{A}$ (light blue). The emulated turbulence corresponds to different r_0 values for an initial beam diameter $D = 20\ cm$ and $\lambda = 532\ nm$. A smaller r_0 value corresponds to stronger atmospheric turbulence.

6.2.3 Attack using Spatial mode detection efficiency mismatch

This study assumes that Alice and Bob generate a secret key using a non-decoy state Bennett-Brassard 1984 (BB84) protocol [13]. We also make the weaker assumption presented in Ref. [135] that they only monitor the total detection rate for evidence of Eve's attack rather than the counts of each channel. Additionally, we assume Alice and Bob also monitor only the average error rate over the four channels, and terminate the protocol if the average quantum bit error rate (QBER) over the four channels is higher than a 8% threshold [138].

The attack model we consider is an intercept-resend attack called the faked-state attack [97, 98]. In this attack, Eve attempts to deterministically control Bob's basis choice and detection outcomes without terminating the protocol. To achieve this, Eve needs to maintain the expected detection rate between Alice and Bob, and keep the QBER below the termination threshold during her attack. In our practical attack model, we assume that Eve knows the attack angles for each polarization state, as well as the detection efficiency ratios between the detectors. Eve intercepts signals sent by Alice using an active basis choice receiver and superconducting nanowire detectors with an overall detection efficiency of 85%. This interception could be done right in front of Alice's setup, to negate the turbulence effect on Eve's measurement. She then generates a signal with the same polarization state as her measurement result, and sends it to Bob at the ideal attack angle. These fake signals may suffer from atmospheric turbulence in transmission to Bob.

We assume that Eve is restricted to today's technology, and uses a weak coherent state for her resend signal. Thus, Eve can control the mean photon number μ of her pulses, as well as mimic scintillation caused by turbulence in the free-space channel to avoid arousing suspicion. Several free-space QKD systems employ pointing and tracking systems that use a bright beacon source and wave front sensor [16, 124, 172] which could be adapted by Bob to monitor and correct beam wander. However, this pointing system uses a separate beacon laser at a different wavelength. This beacon laser does not need to be tampered with by Eve, and the pointing is unaffected by her attack. In the worst case, Eve could perform an intercept-and-resend attack on the beacon beam such that Bob's receiver is pointed according to her designated direction. Thus, this pointing and correction system cannot prevent the attack in our model.

To verify the possibility of a successful attack, we use an optimization program to find the mean photon number that Eve should use for each attack angle to match Bob's expected total detection probability while minimizing the QBER. Our detailed attack model and the optimization process are explained in Ref. [135].

We first characterize a spatial mode attack for a channel without turbulence ($r_0 = \infty$)

before considering a turbulent channel. The optical alignment between the sender (Alice) and the receiver (Bob) is optimized by equalizing the detection count rates of the four polarization channels for a beam propagating through the center of the scanning lens L_E [i.e., along the green center ray shown in Fig. 6.16(a)]. This initial alignment represents normal operation which has a scanning angle $\phi = \theta = 0$. We then move the two-axis translation stage to adjust the position of lens L_E, and record the four detection efficiencies (**H**, **V**, **D**, and **A**) for different angles (θ, ϕ). In principle, the tip-tilt angles induced on the beam by the scanning lens are equivalent to including additional Zernike polynomial terms in the SLM hologram. Furthermore, the order in which the different Zernike polynomials are applied to the beam is interchangeable. As a result, our configuration of having the scanning lens follow the SLM is equivalent to Eve first steering the beam before it propagates through atmospheric turbulence. The scan is performed in $135\,\mu\ rad$ steps, covering a range of $\pm 2.7\ mrad$, which corresponds to a lateral displacement of $\pm 35\ mm$ along the front lens L1 of the QKD receiver.

In order for an angle to be a valid attack angle for channel k ($k = \mathbf{H}, \mathbf{V}, \mathbf{D}$, or $\mathbf{A}$), it must satisfy the condition that the probability of detection in channel k is δ_k times greater than the detection probabilities of the two channels in the other basis. For example, if $k = \mathbf{H}$, then $\min\{\tau_H/\tau_D, \tau_H/\tau_A\} > \delta_H$, where τ_k is the normalized detection probability defined as the ratio between the detection rate at the attack angle over the expected detection probability of Bob. We continuously increase the threshold δ_k until only a few attack angles satisfy these conditions. From the attacker's point of view, it is desirable to have δ_k as large as possible because a large value means an increased chance that detector k will click while minimizing the detection probabilities of the two other channels, which improves Eve's knowledge of Alice's state.

The scan results without turbulence ($r_0 = \infty$) for the four polarization channels are shown in Fig. 6.15(a), and the corresponding detection efficiency mismatch parameters are listed in Table 6.2. There are noticeable features that cause efficiency mismatch, such as the side peak visible below the center peak in **H** detector's map, and the outer ring in all four detector maps. The valid attack angles for the **H** detector correspond to when the click probability is 22 times higher than **D** and **A** detectors (i.e., $\delta_H = 22$), and the normalized detection probability $\tau_H = 0.1$. Although the mismatch ratios on **D** ($\delta_D = 5$) and **A** ($\delta_A = 1.2$) channels are small, the mismatch in **H** and **V** ($\delta_V = 30$) channels are sufficient for a successful attack under our assumption that Alice and Bob only monitor the total count rate (not individual channels).

The optimized QBER as a function of transmission loss between Alice and Bob for a channel without turbulence is shown in Fig. 6.12. In a practical scenario, Alice and Bob might experience transmission efficiency fluctuations in their quantum channel. As a

Table 6.2: Detection efficiency mismatch parameters for attack data shown in Figs. 6.12 and 6.15. τ_k is the relative detection efficiency at an attack angle compared to the normal incidence case, and varies for different turbulence strengths due to changes in the scanning features that lead to valid attack angles. The value of the threshold of detection efficiency ratio δ_k decreases under stronger turbulence. If the δ_k are too low, it is impossible for Eve to find an optimal mean photon number for her resend signal that matches Bob's expected detection rate and does not induce error above the termination threshold. * denotes the turbulence strengths where an attack is not feasible.

r_0 (cm)	δ_k				τ_k			
	H	V	D	A	H	V	D	A
∞	22	30	5.0	1.2	0.1	0.03	0.3	0.001
7.00	20	5.0	1.03	3.5	0.3	0.4	0.8	0.7
3.50	8.0	2.5	1.08	2.3	0.5	0.15	0.85	0.5
2.21	4.5	1.8	1.15	2.21	0.4	0.2	0.85	0.2
1.53	3.0	2.0	1.7	1.25	0.45	0.3	0.85	0.02
1.00*	1.2	1.7	1.02	1.01	0.25	0.4	0.3	0.15

result, they need to tolerate some deviation in their key rate from their estimated value. The results shown in Fig. 6.12 is the QBER during Eve's attack as a function of the lowest transmission loss acceptable to Alice and Bob. In the next section, we examine the success of Eve's attack in the presence of turbulence.

6.2.4 Practical attack under turbulence

To simulate our attack in the presence of atmospheric turbulence, we use a set of 29 holograms per turbulence strength, as described in Sec. II. We have performed scans of our QKD receiver for five different turbulence strengths: $r_0 = 7.00$, 3.50, 2.21, 1.53, and 1.00 cm. Our preliminary experiments that included tip-tilt wander caused by turbulence (i.e., the second and third terms of Zernike polynomials) showed that if Eve does not correct for beam wander caused by turbulence, her attack is not feasible even under very weak turbulence ($r_0 = 7.00$ cm) corresponding to typical high-altitude atmospheric conditions. The beam wander from tip-tilt alone was a strong enough disturbance to significantly hinder her attack. We then repeated the attack under the assumption that Eve can correct

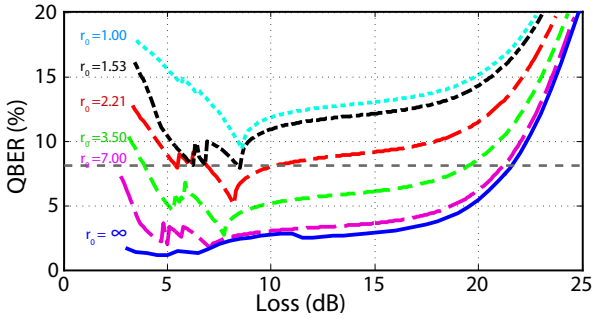

Figure 6.12: Modeled attack performance. Quantum bit error rate (QBER) as a function of transmission loss for no turbulence (blue solid line) and different turbulence strengths corresponding to $r_0 = 7.00\ cm$ (pink dashed line), $3.50\ cm$ (green dotted line), $2.21\ cm$ (red dot-dash line), $1.53\ cm$ (black dashed line), $1.00\ cm$ (cyan dashed line). The horizontal grey dashed line denotes the 8% threshold where Eve's attack is successful when QBER is below this value in our attack model. The maximum transmission loss where Eve's attack is successful decreases as turbulence strength increases. The mismatch ratios are too small in the case of $1.00\ cm$ ($\delta_k \leq 2$ for all channels), and the optimization program could not find a solution with a QBER below 8% threshold given any transmission loss. The higher QBER at low loss (i.e., 3.5–7 dB) is because Eve has to send higher mean photon number states for channels with lower δ_k in order to match expected detection rate of Bob.

for tip-tilt beam wander using adaptive optics, such as with a deformable mirror or SLM. These corrections are implemented in our scans by setting the weight of the second and third terms of Zernike polynomials to zero.

In order to maintain accuracy and stability in our scans, we have chosen to cycle through all 29 holograms at one lens position before moving the translation stage to the next position. This method ensures each hologram is applied to the same scanning angle. We then repeat this scanning process for a total of 1681 angle positions, and record 29 separate detection rates per attack angle for each of the four polarization channels. To represent the Gaussian distribution of centroid displacements discussed in Section 6.2.1, the final normalized detection efficiency of each detector τ_k is given by a weighted average of the detection rates from each hologram per scanning angle (θ, ϕ),

$$\tau_k(\theta, \phi) = \sum_{i=1}^{N} \Phi_i \tau_{k,i}(\theta, \phi), \tag{6.4}$$

where $\tau_{k,i}$ is average detection efficiency of k detector under the holograms selected from ith radius. Φ_i is probability of occurrence of ith partition discussed in Section 6.2.1. $N = 5$

is the number of partitions. We select 1 sample hologram for no turbulence, 8 samples each for 0.5σ, 1σ, 2σ partition, and 4 samples from 3σ partition. The samples are given the weight factor corresponding to the radius from the sample used to the next larger sample, thus representing the best case hologram from this range. This weight factor ensures that the samples form an optimistic (easier to hack) representation of the turbulence effect, and therefore ensure any turbulence found to not be vulnerable to attacks is indeed safe under the parameter monitoring assumptions. The total detection rate τ_k is used to find valid attack angles under turbulent conditions using the same method as without turbulence. We then repeat this process for different turbulence strengths from very weak ($r_0 = 7.00\ cm$) to stronger turbulence emulating low-altitude sea level conditions ($r_0 = 1.00\ cm$). A map of successful attack angles and the corresponding detection efficiency mismatch parameters are shown in Fig. 6.15(b)–(f) and Table 6.2.

Our scanning results in Table 6.2 show that as the turbulence strength increases, the mismatch ratios δ_k are significantly reduced. We can see in Fig. 6.15 that the features that are responsible for efficiency mismatch become blurry and eventually disappear as turbulence increases in strength, and it becomes harder for Eve to maintain a precise attack angle when $r_0 \leq 1.53\ cm$. For stronger turbulence ($r_0 = 1.00\ cm$), the only remaining hackable feature is the displacement of the center peaks due to a slight misalignment between the fiber couplers in each arm of the receiver. As a result, most of the attack angles at stronger turbulence are found closer to the center peak. However, they do not result in a successful attack for $r_0 < 1.53\ cm$ because the induced QBER is above the 8% termination threshold.

In order to perform a quantitative verification of an attack, we use an optimization program to find the minimal QBER as a function of transmission loss. The results in Fig. 6.12 show the optimized QBER for an attack in stronger turbulence ($r_0 = 2.21\ cm$) is higher than that of weaker turbulence ($r_0 = 7.00\ cm$). If we assume that the QBER threshold for Alice and Bob to terminate the protocol is 8 %, then the attack without turbulence is successful as long as the transmission loss between Alice and Bob is less than 21 dB. Whereas in the presence of turbulence, Eve can successfully attack this receiver for $r_0 \geq 2.21\ cm$ when the transmission loss is less than 10 dB but higher than 7 dB. Using Eq. (6.2), $r_0 = 2.21\ cm$ is equivalent to Eve having her resend setup approximately 0.5 km away from Bob's receiver in typical sea-level turbulence conditions ($C_n^2 = 1.8{\times}10^{-14}\ m^{-2/3}$). Eve is unable to match Bob's count rate for transmission loss below 3.5 dB even if she uses all four channels due to Eve's non-perfect detection efficiency. Therefore, the optimization program could not find a solution matching Bob's total detection rates for transmission losses below 3.5 dB.

The result for $r_0 = 1.53\ cm$ shows there is only a small loss window (around 8.5 dB)

where Eve can attack without inducing a QBER higher than the threshold. Using Eq. (6.2) and the value of C_n^2 given above, this r_0 corresponds to a distance of 1 km. At lower transmission loss (i.e., 3.5–7 dB), the expected detection rate at Bob is too high for Eve to match using a single channel, and therefore she must also use the other channels that have a lower δ_k. This causes the QBER to increase and results in the irregularities seen for loss below 7 dB when the number of channels being used is changed. The QBER curves become smoother at higher loss once Eve can fully replicate Bob's detection rates while only sending signals to a single polarization channel, which takes advantage of the greatest efficiency mismatch for an optimized attack. The mismatch ratios in the case of 1.00 cm ($\delta_k \leq 2$ for all channels) are too small for the optimization program to find a solution for a QBER below the threshold given any transmission loss.

Implementations of QKD can and should monitor counts at each detector to ensure they remain relatively balanced. The higher QBER obtained when Eve is forced to send states to channels with lower mismatch ratios illustrates how monitoring each channel would increase the difficulty of a successful attack. However, it is uncommon in practice to monitor individual count rates, and there are no current standards or established guidelines for allowable variation in detection rates. The added constraint to maintain precise detection rates would make hacking more difficult for an eavesdropper, but does not in itself prevent an attack. It also does not invalidate the current work of determining if bounds exist on the turbulence strength where QKD systems can be hacked.

6.2.5 Theoretical limit of attack under turbulence

The attack described in Section 6.4.3 is only one particular example of an intercept-resend attack. Other attacks in this class may exist which shows that a QKD system with detection efficiency mismatch could be insecure if the security analysis does not take the mismatch into account. Whenever the observed and monitored data are compatible with an IR attack, no secret key can be obtained [27, 26].

For this reason, it is useful to ask the question whether the data we observe is consistent with an IR attack or not. Along the way we can also answer the question whether a fine-grained analysis of the observations could exclude IR attacks, and thus potentially give a secure key where the coarse-grained analysis (which uses only average error rate and average detection rate) fails.

The handle to determine whether given data are compatible with an IR attack or not is the fact that IR attacks make the channel between Alice and Bob entanglement breaking. That is, this channel acting as one system of a bipartite entangled state will

transform it into a separable bipartite state. So by verifying that the channel is not entanglement breaking, we can exclude the IR attacks. To do so, we do not require actual entanglement: we can probe the channel with non-orthogonal signal states, just as in any prepare-and-measure QKD set-up, and use the formalism of the source-replacement scheme (see for example [39]) to formulate an equivalent thought set-up that virtually uses an entangled state. The probabilities $p(ab|xy)$ between Alice's signal choice a and Bob's measurement result b for respective basis choices x and y can then be thought of as coming from measurements on this entangled state with both Alice and Bob performing measurements with POVM elements $M_A^{x,a}$ and $M_B^{y,b}$, respectively. If these observations serve as an entanglement witness, we have shown that the channel is not entanglement breaking.

We can formulate the entanglement verification problem as the optimization problem

$$\begin{array}{ll} \text{find} & \rho_{AB} \\ \text{subject to} & \rho_{AB} \geq 0 \text{ and } \rho_{AB}^{\Gamma_A} \geq 0 \\ & \text{Tr}(\rho_{AB} M_A^{x,a} \otimes M_B^{y,b}) = p(ab|xy), \forall a, b, xy. \end{array} \tag{6.5}$$

Here Γ_A is the partial transpose operation on Alice's system. If the above optimization problem is not feasible, then the state ρ_{AB} is entangled [120]. In our previous work [174], we developed a method to solve the above optimization problem when detectors' efficiencies are mismatched and the dimension of the optical signal is unbounded.

In this work, we did not measure the joint distribution $p(ab|xy)$ of Alice and Bob directly in the experiment. However, given the characterization of detection efficiency mismatch from our experiment, we can deduce the joint distribution of Alice and Bob from the case without efficiency mismatch according to our simulation model. Using the method developed in Ref. [174], we found that when there is no turbulence or very weak turbulence $r_0 = 7.00\ cm$, we cannot verify entanglement. Thus, the channel is vulnerable. This result is in agreement with the results in Ref. [174].

However, when turbulence is stronger ($r_0 \leq 3.50\ cm$), our calculation shows that entanglement can be verified. This means that there is no intercept-resend strategy for Eve that can match all of Alice and Bob's expected observations. This result is based on a strong condition where Eve needs to match all expected measurable parameters of Alice and Bob. Whereas, the results presented in Section 6.4.3 were under the practical assumptions that Alice and Bob monitor only coarse-grained information, namely the total detection rate and error rate.

6.2.6 Conclusion

We experimentally study how atmospheric turbulence in a free-space channel can affect an eavesdropper's ability to perform a spatial mode attack on a QKD receiver. We use a phase-only spatial light modulator to emulate atmospheric turbulence in the lab, whose accuracy is verified by comparing measured far-field intensity distributions and centroid displacements to theoretical predictions. We then study a spatial mode detection efficiency mismatch attack under a range of atmospheric turbulence strengths to determine the maximum unsafe radius around the free-space QKD receiver. Our attack model is based on an intercept-resend attack under the practical assumptions that only the total detection rate and QBER are monitored by Alice and Bob. We find that for this particular receiver, an eavesdropper could attack a non-decoy state BB84 system from up to about 1 km away in typical sea-level turbulence conditions ($r_0 = 1.53$ cm for a 20 cm beam at 532 nm). This result is assuming Eve can correct for basic tip-tilt beam wander using conventional adaptive optics. Eve's chances of success will be further reduced if Alice and Bob choose to monitor individual detection channel statistics. In this case, we theoretically find that an IR attack is still possible for weaker turbulence ($r_0 \geq 7.0$ cm). The assumption that an eavesdropper has physical limitations is not usually included in the security analysis of a QKD system. If there is a chance that Eve is inside this secure zone around Bob's receiver, or has advanced adaptive optics capacities to correct for beam aberrations, then extra care regarding these types of attacks may be required.

6.3 Spatial-mode response characterization in a free-space QKD system with Zernike polynomials

Author contributions
Vadim Makarov, Norbert Lütkenhaus, and Thomas Jennewein provided advice on the experimental setup. Katanya B. Kuntz wrote a program to generate phase hologram for the SLM. I wrote programs to control and synchronize the experiment setup. With Katanya B. Kuntz and Jean Philippe Bourgoin, we performed an experiment and verified the countermeasures. With Katanya B. Kuntz, we process the experiment result and analyze the practical limit of the attack.

Unlike eavesdropper Eve, whose ability is limited only by laws of physics, the legitimate parties in the QKD scheme are limited by both available knowledges as well as equipment and technology. As the understanding of the subject and better tools being developed, it is

equally important to revisit and verify the effectiveness of countermeasure implementation against the attack it is designed to counter, as well as other variants.

Our previous study [135] shows that by altering the angle of the signal sent to Bob, Eve could bias the detection probability in a free-space QKD receiver, enabling intercept and resend attack. A spatial filter (pinhole) was proposed as a countermeasure. In this study, we propose a more general method of characterizing the spatial-mode detection efficiency mismatch in a free-space QKD system using a phase-only spatial light modulator (SLM). Our experiments are divided into two parts: first in Section 6.3.1, we characterize the detection efficiency mismatch apparatus with SLM and explore the effect of higher-order Zernike polynomials on detection efficiency mismatch. In Section 6.3.2, we verify the effectiveness of the spatial filter against both original tip-tilt as well as using more complex wavefront intensity distributions generated by the SLM.

6.3.1 Zernike poynomials and SLM characterization

In this study, we use a phase-only Spatial Light Modulator (SLM) to manipulate the phase wavefront of the attack beam. The wavefront consists of a combination of Zernike polynomials [12, 17]. Each Zernike polynomial represents a different optical aberration, such as defocusing, tip-tilt, astigmatism, coma, etc. In principle, phase hologram generated from linear combinations of these polynomials,

$$\phi(\rho, \theta) = \sum_i c_i z_i \tag{6.6}$$

where Z_i is the ith Zernike polynomial and c_i are weighing, could produce arbitrary wavefront intensity distribution out of a characterized incidence beam reflected from the SLM.

The receiver we test is a prototype for a quantum communication satellite [15] with polarization encoding. It is a passive basis choice receiver operating at 532 nm wavelength. In this type of receiver, the input light is split by a 50:50 beamsplitter (BS) and polarizing beamsplitters (PBS) into four multimode fibers leading to four single-photon detectors. The detectors receive photons polarized horizontally H, vertically V, +45 deg D and −45 deg A. The efficiency mismatch ratio (δ_k) means that a detector in channel $k \subset H, V, D, A$ has a probability of clicking at least δ_k times higher than the detectors in the other basis. We replace the mechanical scanning apparatus in Ref. [135] with SLM, as shown in Fig. 6.16. To verify the ability of the SLM to modulate wavefront intensity, we projected the hologram between $z_4 - z_{10}$. The far-field intensity distribution of the reflected beam from SLM is measured at three distances 3m, 10m, and 20m along the beam

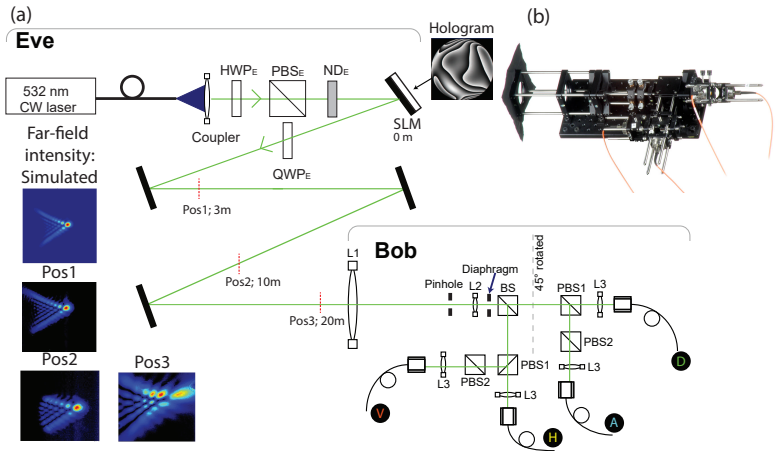

Figure 6.13: (a)Experimental setup, and (b)Picture of receiver under test.

propagation path. The measurement results in all distance closely resemble the theoretical simulation, as shown in Fig. 6.14.

6.3.2 Generalized spatial-mode detection efficiency mismatch characterization

In addition to flexibility, the SLM also provides better precision and stability over the mechanical scanning setup. It also eliminates distortion caused by tilting the scanning lens. This new setup could reveal some exploitable features obscured in the mechanical scanning setup.

The experiment is done by sending circularly polarized light from the source with the wavefront controlled by weight terms z_i of the hologram on the SLM. The goal here is to find a combination of z_i that causes the highest δ_k for each k channel. Limited by the stability of the setup, it is impossible to measure all combinations of Zernike polynomial terms and weigh values. Our first task is to narrow down this parameter space. For that, we need to look for specific polynomial z_i that contributes to the detection efficiency mismatch. We generated 1000 holograms with a random weight value of $z_4 - z_20$ (tip-tilt modes are excluded). The range of weight value c_i in this study is bounded by the SLM pixelate to ± 20 for Z2 and Z3 (tip-tilt), and ± 8 for higher-order Z_i.

We project these randomly generated histograms one-by-one on the SLM and record detection efficiency mismatch ratio δ_k. The result shows that, of all the holograms that

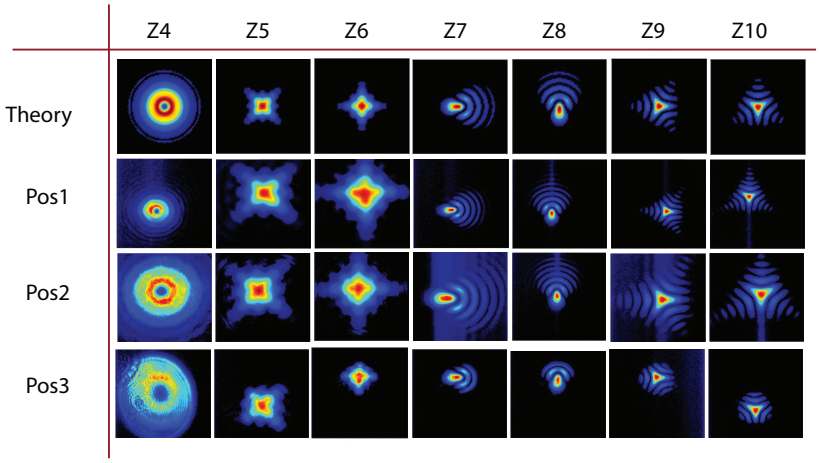

Figure 6.14: Far-field characterization of wavefront intensity generated by Zernike polynomials in the setup. The measurement result agreed with the simulation throughout beam propagation path.

cause mismatch ratio higher than 5 (the minimum ratio that Eve could exploit [135]), only z_4 to z_7 have a noticeable higher impact. Thus, in the following experiments, we will consider only the effect of $z_2 - z_7$.

Our test of tip-tilt (z_2, z_3) scanning shows similar result to [135] (see Fig. 6.15 (a)). This tip-tilt-only case gave δ_k varying between 1.5–17.7 as shown in Table 6.3. We also perform another scan without tip-tilt modes, the higher-order scan of $Z_4 - Z_7$ showed values of δ_k varying between 1.3–4.7, which is not high enough for Eve to exploit.

However, when we fixed the weight of z_2 and z_3 to the value that causes highest efficiency mismatch in the tip-tilt-only case, then scan the weight value of $z_4 - z_7$ and record the combinations that cause the highest mismatch, the results show that Eve can significantly increase the highest mismatch ratio from 17.7 to 52.3 (See the last column of Table 6.3). The results in this section show the significance of including higher spatial-mode in the characterization of free-space QKD systems. Furthermore, if one were to use SLM and Zernike polynomials to actively correct spatial mode distortion either by Eve or environment such as atmospheric turbulence, and if the detection efficiency mismatch is concerned, one can narrow-down their calculation to $z_2 - z_7$. This would significantly improve calculation speed.

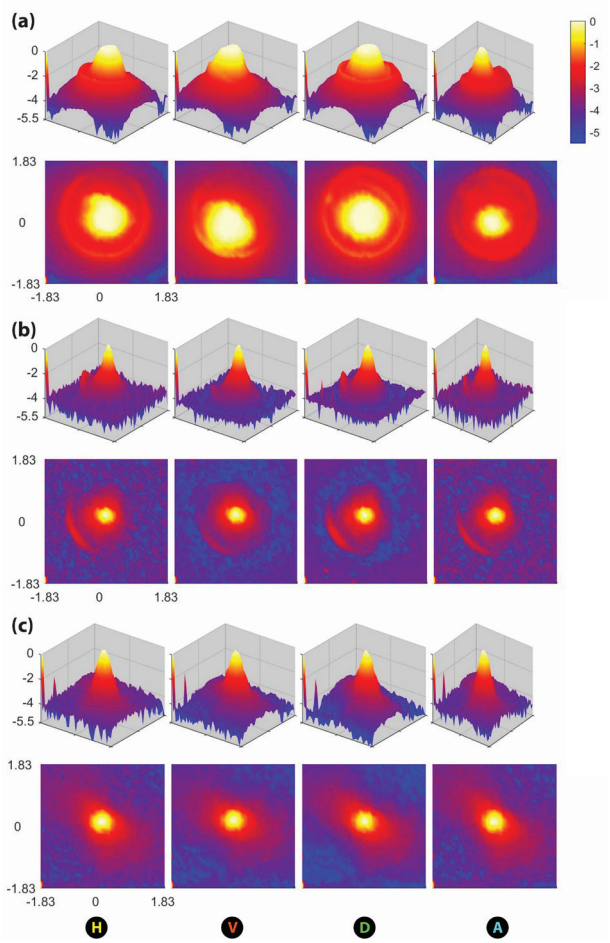

Figure 6.15: Tip-tilt scanning result shows normalized detection probability of each detector at different incoming beam angle in mrad on three different scenarios; (a) without pinhole, (b) with pinhole, and (c) with pinhole and diaphragm.

Table 6.3: Maximaum detection efficiency mismatch in each receiver channel. The result shows that, with the help of higher order Zernike polynomials, the detection efficiency mismatch ratio can be increased significantly.

Channel	Optimal polynomial weighing						Mismatch ratio	
	z_2	z_3	z_4	z_5	z_6	z_7	Tip-tilt only	With higher order polynomials
H	-4	8	4	6	4	-4	1.5	2.2
V	-8	3	0	0	0	0	17.7	17.7
D	12	8	-6	8	-4	0	7.7	52.3
A	10	11	-2	-2	2	6	1.4	1.7

6.3.3 Countermeasure verification

In this section, we use the setup to verify the effectiveness of the spatial filter (25 µm pinhole) as a countermeasure to spatial mode attack. The result in Fig. 6.15 (b) shows that the pinhole can only block the translational modes and small-angle reflection from beamsplitters. However, it could not reliably block high-angle trajectory (i.e. lens edge scattering). Furthermore, it opens a new attack for different combinations of Zernike polynomials weights, which increases the mismatch ratio in this case to 15.0. This ratio is exploitable by Eve(See Table 6.4). This feature could not be seen in the mechanical scan experiment. To counter high-angle scattering, we add a diaphragm behind the collimating lens (L2) in the receiver. This diaphragm alone helps block the higher-angle scattering features, as shown in Fig. 6.15 (d). The result in Fig. 6.15 (d) shows that diaphragm and pinhole together help prevent most of the efficiency mismatch from the tip-tilt mode. The only feature left is the translational shift of fiber coupler, which causes a mismatch angle close to the original beam path in channel H ($\delta_H = 4.5$) and channel V ($\delta_V = 15.9$), worsen the situation. However, when the diaphragm's diameter is reduced to 4mm, all exploitable features are blocked, and no combination of weight values within our scanning range cause detection efficiency mismatch.

These series of experiments provides two valuable insight. First, any system characterization methods and countermeasures need to be revisited as new techniques and equipment developed. In our case, the tip-tilt only characterization is not sufficient to guarantee the countermeasure's effectiveness, and the SLM helps reveals new preventable vulnerabilities. Second, new countermeasures which parameter is not set properly, diaphragm diameter in this case, could change the outcome from successfully preventing the attack from opening

Table 6.4: Efficiency mismatch ratio and corresponding weight value of Zernike polynomial weights of V channel under different countermeasures.

Cases	Optimal weight combination				Mismatch ratio (δ)
	Z4	Z5	Z6	Z7	
No pinhole	-8	2	4	4	4.7
Pinhole	8	0	8	4	15.0
Pinhole+diaphragm (7mm)	-2	6	6	0	15.9
Pinhole+diaphragm (4mm)	-	-	-	-	1.0 ± 0.1

a new attack angle.

6.3.4 Conclusion

In this study, we present a new method to characterize the spatial-mode detection efficiency mismatch using SLM. Characterization of spatial-mode detection efficiency mismatch using an SLM helps reveal some exploitable features previously obscured. We show that by including higher-order Zernike polynomials, Eve can increase detection efficiency mismatch. We also show that diaphragm with a proper set diameter, in addition to a sufficiently small pinhole proposed in previous studies, could prevent the efficiency mismatch due to wavefront manipulation. These results are valid only within our experimental parameter range

The exploitable features shown in this study demonstrates the importance of including a tip-tilt scan while adjusting the alignment between Alice and Bob, as these features could not be seen in the normal alignment procedure. Further study on characterization and finding a better countermeasure against spatial-mode detection efficiency mismatch is highly encouraged.

6.4 Faking photon number on transition-edge sensor

Author contributions
With Vadim Makarov, Anqi Huang, Hao Qin, we designed the experiment process. Jiaqiang Zhong and Sheng-cai Shi provided the TES for the study. I performed an experiment with Jiaqiang Zhong, Anqi Huang, and Hao Qin. With Vadim Makarov and Jiaqiang Zhong, we post-process the data and design an attack model exploiting the vulnerability.

Photon detectors are indispensable in quantum communication applications. To ensure the reliability of the detection results, it is important to characterization of detectors being used both within the intended working parameters and possible unintended conditions. This characterization could help in revealing possible flaws and imperfections. These flaws could lead to misguided detection results or worse exploitable vulnerabilities in the case of quantum communication and cryptography applications. These characterizations of photon detectors provide guides to improve the robustness of quantum systems. Over the years, many studies have been reported with attacks on various types of photon detectors[97, 175, 135, 93, 91, 94, 92, 90, 44, 79].

TES is a photon detector capable of providing full photon-number-resolving (PNR) capability [14, 35]. It also achieved the highest detection efficiency among PNR detectors up to 95% for 1556-nm detection efficiency [82, 41, 107]. This type of detector is used in various applications that require high detection probability, such as device-independent quantum key distribution (DI-QKD) [47]. As one of the potential detectors in quantum communication where the reliability of detection result affects overall security, the TES photon detector should be investigated for its robustness and possible flaws. In this study, we experimentally demonstrate two vulnerabilities of TES, namely, a wavelength attack here the photon number result could be controlled by changing signal's wavelength and a faked-state attack where the adversary take control the temperature of TES with appropriate bright CW-laser and force an arbitrary photon number detection result using a bright pulsed laser. We also model an attack on a QKD system with TES as detectors based on these characteristics.

The structure of this section is as follows. In Section 6.4.1, we present the device under study and experimental setup. We then experimentally show the two methods of faking photon number states in Section 6.4.2. To emphasize the threat of this attack, we use our measurement results to model an attack on a QKD system in Section 6.4.3. We conclude in Section 6.4.4.

6.4.1 Experimental setup

The operational description of TES has been discussed in chapter 3. Extremely sensitive TES for photon detection operate below 1 K. The commercial SQUID amplifier chips also work at low temperature, generally below 4 K. In our case, the TES and SQUID are integrated onto a mounting copper block which is attached to the cold plate of an adiabatic demagnetization refrigerator (ADR). Under the normal operational condition, both the TES devices and SQUIDs operate at 100 mK. 6.16 a) shows the circuit diagram

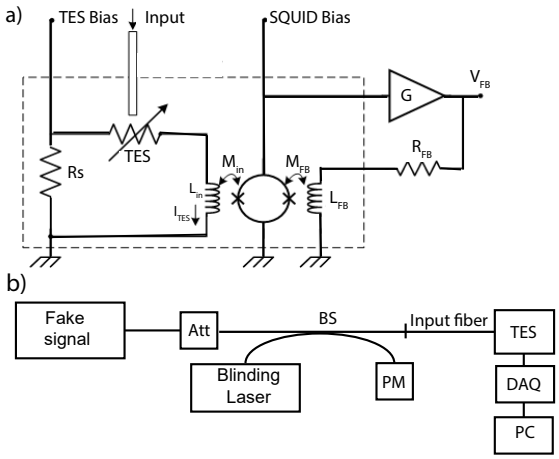

Figure 6.16: a) Internal circuit diagram of TES and DC-SQUID readout. b) Experimental setup. Blinding and fake signal power is controlled by attenuator (Att). The input power is measured by an optical power meter (PM).

of the TES. The TES bias is obtained by applying a constant current through a shunt resistor (R_s). The changes of current resulted from the absorption of incident photons are read by inducting coil coupling to the DC-SQUID. The magnetic field $M_F B$ produced by the DC-SQUID inducing the output current I_{FB}, which is further amplified by a current amplifier G. The changing of output voltage V_{FB} is proportional to the TES current change.

To test the response of the TES to various optical signals, we use the setup shown in Fig. 6.16 b). The TES is fiber-coupled and designed for 1550 nm wavelength. [41, 42] The photon coupling efficiency in the TES understudy is $\approx 1\%$ owing to a misaligned fiber end to the TES effective area. However, this does not affect our study. The faking signal is coupled through the same path as the input signal. The blinding laser is added by a beam splitter (BS). A power meter is used for monitoring the laser input power. A function generator is used to product trigger pulses to synchronize the laser source and signal recordings. Details of the operation will be explained in the respective sections. The signal from TES is digitized by a data acquisition module (DAQ) and analyzed on a computer(PC).

6.4.2 Fake detection on TES

In this section, we investigate two of the exploitable vulnerabilities of the TES detector against two types of attack; wavelength attack and faked-state attack.

Wavelength attack

TES's output voltage is inherently proportional to the energy of photons absorbed. In principle, N photons with a wavelength $N\lambda$ arriving simultaneously has the same photon energy as one photon with a wavelength of λ. Thus TES would give the same output between the detection of these two cases. With this fact, we show in the first experiment that an attacker Eve could fake a single-photon detection result by sending multiple photons with proportionally lower photon energy. To confirm this effect, weak-coherent signals from several pulsed lasers of different wavelengths are sent through the input fiber of the TES. We then record the voltage response $V_F B$ from the TES.

The histogram in Fig. 6.17 shows that the response signal of single-photon detection from a 450 nm photon is overlapped with two-photons detection from 780 nm and three-photons detection from 1550 nm photons. This result shows that a TES's expected photon number readout could be faked by multiple photons with a proportionally longer wavelength. It shows that the photon number measurement results from a TES alone cannot be used to characterize the photon number distribution of photon signal through an untrusted channel, e.g. QKD channel, where an adversary could intercept and replace the signal with photons of arbitrary wavelength. A narrow-band wavelength filter could prevent this attack. However, the characterization of the filter's performance against exploitable wavelengths for each specific filter is needed.

Faked-state attack

In the ideal condition, a TES operates at the transition edge between superconductor and a normal resistor of a material. In this region, a small change of energy, such as single-photon absorption, could induce a measurable change in output voltage proportional to the energy absorbed. By setting a voltage threshold level for each input photon energy, one could discriminate the number of absorbed photons. From the characteristic of TES [61], a TES at a slightly higher temperature than the operational regime could produce the same voltage output level when absorbing photons with much higher energy (bright laser pulse). In this section, we experimentally demonstrate such behavior.

We first investigate the behavior of TES when its temperature is increased beyond the designed transition-edge region. We set the TES to the operational temperature. We then record the I-V characteristic curve of the system at different temperatures, which are a plot of current across a superconducting material and the voltage readout from the DC-SQUID. This characteristic curve will be used as a reference for the following experiments. At low temperature ($100 - 150$ mK), the output voltage of the DC-SQUID is reduced drastically

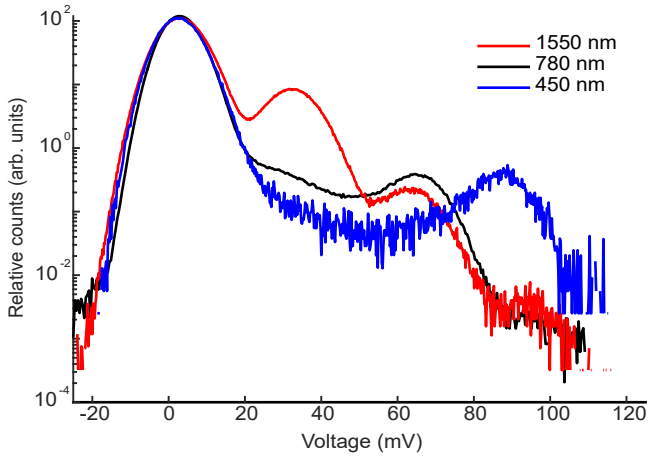

Figure 6.17: Histogram of TES output voltage of weak-coherent laser pulses at 1550nm (blue), 780nm (red), and 450nm (green). The leftmost peak represents zero-photon detection. Subsequent peaks to the right represent higher photon number detection. These peaks appear at the voltage level proportional to the energy of the photons.

as its input current increased. As the temperature of TES increasing, the I-V response rate is decreased. Up to a certain threshold ($\approx$ 180 mK), the voltage response turned to be directly proportional to the current as the system becomes a normal resistor. This I-V characteristics is shown in Fig. 6.18(a).

We now demonstrate the ability of an adversary to control the temperature using a bright light. A tunable CW-laser at 1550nm is coupled through the input port of TES. Fig. 6.18(b) shows that the I-V characteristics at different temperatures of the device under test can be replicated. This result shows that an adversary could arbitrarily control the temperature of TES using a bright CW-laser.

For the faked-state attack, the appropriate blinding laser power is one that puts the response at the threshold between the transition-edge regime and the normal resistor regime. In this region, the TES is 'blinded' from single-photon input as the change of voltage produce from single-photon absorption is minimal. At the same time, the system in this condition could produce the same voltage level as the system at normal operating temperature when absorbing a bright laser pulse. In this experiment, the blinding CW laser is 0.25 nW. The fake photon-number response can then be forced by sending additional bright pulsed laser with appropriate peak power. The histogram of faked-state results with different peak power is shown in Fig. 6.19. Here, the fake signals are laser pulses with 16 ns width and 100 kHz repetition rate. The result shows that an arbitrary 'photon number'

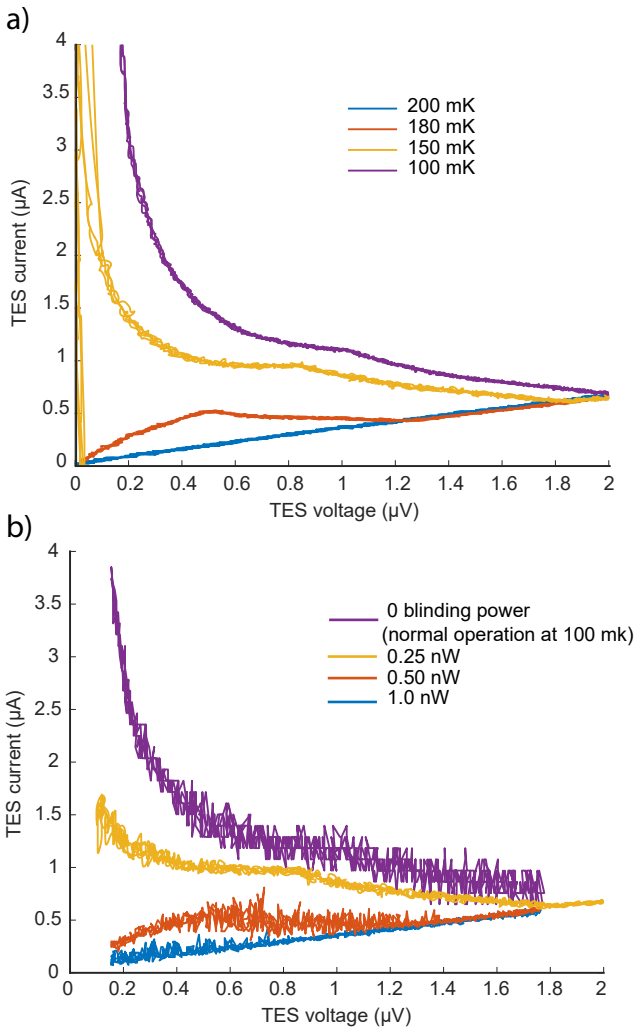

Figure 6.18: I-V curves of the system. The characteristics of the system at 100 mK under bright laser illumination (b) closely resemble the characteristics at different heat-bath temperatures (a). This presents the ability of Eve to control TES's temperature using bright light through the input port.

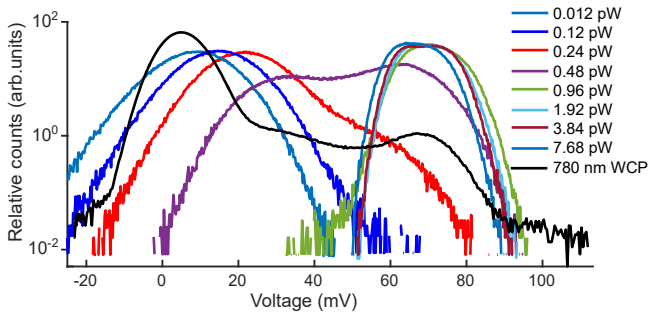

Figure 6.19: Fake detection histogram at different faked-state power.

response could be controlled by an outside adversary who has access to the input channel. This vulnerability poses an immense threat to any communication system employing TES as a detector.

6.4.3 Attack model

To emphasis the threat of vulnerabilities found in the previous section, we model a faked-state attack [93] on a Bennett-Brassard 1984 (BB84) [13] QKD system, assuming it uses the TES under test as its detectors. In this attack model, the adversary Eve intercepts each signal from Alice and measures it on a random basis. She then reproduces a fake signal identical to her detection result and sends it to Bob. Here, she also sends a CW blinding laser power set to 0.25 nW and set her fake pulsed signal peak power to 0.48 pW. In case of Bob's measurement basis choice being different to that of Eve, the power of the fake signal would be split equally between Bob's detectors. As shown in Fig. 6.20, most of the response signal from TES would fall below the single-photon detection threshold, thus remain unregistered. Otherwise, if their basis choices matched, some of the signals could be registered. It can be seen from the histogram in 6.20 that this attack condition causes detection loss in Bob. In practice, Eve could hide this loss from Alice and Bob by controlling her quantum channel loss. Thus, if the original quantum channel loss between Alice and Bob is lower than the detection loss induced by Eve's attack, this attack could be done unnoticed. Our calculation shows that this attack on a QKD system with the TES under test as detectors would induce 7.4% error rate. This error rate is lower than the abort threshold of the BB84 protocol; thus, the security of the key could be compromised. Similar attacks on other QKD protocols such as coherent-one-way (COW) [92] should also be considered.

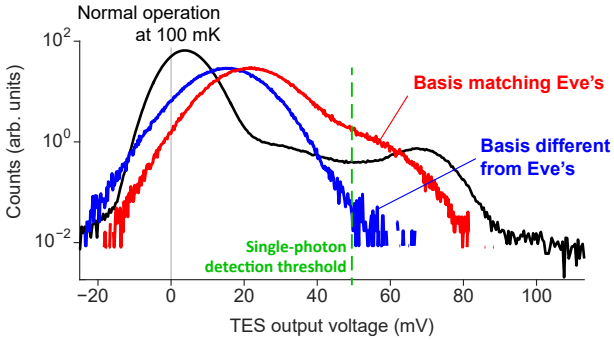

Figure 6.20: An attack model on a BB84 QKD system with TES as a detector. The response under normal condition (black) contains a zero-photon response (left peak) and a single-photon response (right peak). The threshold (green vertical dashed line) marks the minimum TES voltage output that the system in our model would register as a detection. The fake response is shown for two cases where Bob and Eve pick the same (red) and different (blue) measurement bases.

6.4.4 Conclusion

We experimentally demonstrated two vulnerabilities of TES as a photon detector. In this study, we showed an ability of Eve to fake photon-number results in TES using different wavelengths. We also showed that the characteristics of TES could be altered by CW laser, and photon-number detection results could be faked using laser pulses with appropriate peak power. From the result, we showed an attack model on a BB84-QKD system with TES as a detector and showed that Eve could perform intercept and resent attack while inducing as low as 7.4 % error rate. Since the TES under test has a misalignment of its input coupling, which limits its detection efficiency, we speculate that an attack on a TES with a higher-efficiency detector with better energy resolution could yield a better result for Eve. This, to our knowledge, is the first demonstration of potential vulnerabilities of TES to hacking attacks. Countermeasures to such attacks will need to be considered in the future when TES begins getting employed in secure quantum communication schemes.

Chapter 7

Conclusion

In this thesis, I have shown six experiments that are examples of the method to improve the performance and security of practical QKD implementations. In the first experiment on the quantum dot as a single-photon source for QKD, we have seen that the development of near-ideal single-photon source allows us to perform key exchange at a higher rate longer distance, close to the theoretical limit. It also shows that QKD with a single-photon source can be a candidate for long-distance QKD. The results also imply that other QKD protocols with single-photon security analysis could benefit from employing a quantum dot. In general, this study shows the necessity of exploring and evaluating all available tools both in theory and practical implementation during the design stage of the QKD system.

The second study on a generalization of device characterization against Trojan horse attack. The result that the method being considered as a standard for QKD implementation could be improved to cover more powerful attacks allowed by the law of physics. It is an example of the necessity to revisit and analyze the method and solution at hand from a broader perspective, especially for the practices that would be included in the standardization and certification criteria. To achieve the level of security promised in theory, we should analyze the system design and practical devices based on what Eve could do, not what she would do.

The third experiment on the backflash side-channel shows one of the vulnerabilities in the detection devices. It shows that behavior that has been known for a long time in the development of the device but has yet been analyzed and characterized within the security model could hide a potential threat to the security of the system that employs such a device. It is yet another example of the necessity of exploring and including all

known behavior of the practical devices into the security analysis to guarantee the security of practical QKD.

The next experiment is about the effect of atmospheric turbulence on Eve's spatial mode detection efficiency mismatch attack. The experiment shows two main results. First, the phase-only SLM and holograms generated by Zernike polynomials can be used to emulate the atmospheric turbulence that covered typical strength at sea level up to the upper atmosphere. Using that emulator, we show both the practical and theoretical limits of Eve's attack. The result implies that if Alice and Bob could establish a secure zone a certain radius around their receiver where Eve could not present, although that zone does not cover the whole quantum channel, that would prevent Eve from performing the attack under study. Although the assumption of Eve's limitation is not a common practice, this study provides an insight into Eve's capability and practical assumption on the security claim that should be put on practical QKD. It also shows that a practical QKD can be used today so long as such assumptions are acceptable for the risk.

The fifth experiment is another application of Zernike polynomials and phase-only SLM to characterize a free-space QKD receiver. We first use the apparatus to narrow down the number of Zernike polynomials terms that would affect the spatial mode detection efficiency mismatch of the detector. We then use that result to characterize the receiver. With better stability and more degree of freedom of the SLM, the experiment reveals exploitable features that are obscured in the previous experiment. The result shows the necessity of including higher-order Zernike polynomial terms to characterize the system against the spatial mode attack. It also shows the insufficiency of the countermeasure proposed in our previous study, and provide a test bench for an improved version of the countermeasure. This study shows the threat of setting a wrong parameter on a countermeasure. It also shows the necessity of improving the characterization method and employs better characterization apparatus as the tools become available.

The last experiment is the fake-state attack on the transition edge sensor. We show the ability of Eve to deterministically control the output result of a TES using a bright laser. The result implies that the photon number result from TES alone, in contrast to previously believes, cannot be used to characterize the quantum channel faithfully. It also tells us that, before including in the system design, we should thoroughly characterize the device and understand its behaviors both within the operational regime and beyond.

These studies have addressed some of the important issues in developing the QKD standard and provided some possible solutions. I hope that this work will emphasize the necessity of improving the system characterization procedure and the importance of investigating physical side-channels in every implementation of QKD. Furthermore, I also

believe that the iterations of finding vulnerabilities and testing countermeasures should eventually lead us toward the high level of security promised by the theory of QKD.

References

[1] OEspace, https://www.eospace.com/polarization-controller, visited August 2020.

[2] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

[3] Clavis2 specification sheet, http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf, visited 8 July 2016.

[4] OEspace, https://www.eospace.com/phase-modulator, visited August 2020.

[5] BME-Bergmann, https://www.bme-bergmann.de/high-voltage-electronics/pockels-cell-driver-head/, visited August 2020.

[6] Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems, draft ETSI GS QKD 0010 V0.0.1 (2017-12), https://docbox.etsi.org/ISG/QKD/Open/GS_QKD_0010_ISTrojan_Draft_0-0-1.pdf, visited 20 April 2019.

[7] SPCM-AQRH single photon counting module data sheet, http://www.excelitas.com/Downloads/DTS_SPCM-AQRH.pdf, visited 13 March 2018.

[8] Photosensor modules H7422 series, https://www.hamamatsu.com/resources/pdf/etd/m-h7422e.pdf, visited 13 March 2018.

[9] Arash Ahmadi. *Towards On-demand Generation of Entangled Photons with Quantum Dots*. PhD thesis, University of Waterloo, 2019.

[10] N. Akil, S. E. Kerns, D. V. Kerns Jr., A. Hoffmann, and J-P. Charles. Photon generation by silicon diodes in avalanche breakdown. *Appl. Phys. Lett.*, 73:871–872, 1998.

[11] Scott A. Vanstone Alfred J. Menezes, Paul C. van Oorschot. *Handbook of Applied Cryptography*. CRC Press, 5th edition, 2011.

[12] Larry C. Andrews and Ronald L. Phillips. *Laser Beam Propagation through Random Media*. SPIE, 2nd edition, 2005.

[13] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. International Conference on Computers, Systems, and Signal Processing (Bangalore, India)*, pages 175–179, New York, 1984. IEEE Press.

[14] Karl K. Berggren, Eric A. Dauler, Andrew J. Kerman, Sae-Woo Nam, and Danna Rosenberg. Detectors based on superconductors. In *Experimental Methods in the Physical Sciences*, volume 45, pages 185–216. Elsevier, 2013.

[15] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New J. Phys.*, 15:023006, 2013.

[16] Jean-Philippe Bourgoin, Nikolay Gigov, Brendon L. Higgins, Zhizhong Yan, Evan Meyer-Scott, Amir K. Khandani, Norbert Lütkenhaus, and Thomas Jennewein. Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. *Phys. Rev. A*, 92:052339, 2015.

[17] Liesl Burger, Igor A. Litvin, and Andrewll Forbes. Simulating atmospheric turbulence using a phase-only spatial light modulator. *S. Afr. J. Sci.*, 104:129–134, 2008.

[18] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Daylight quantum key sistribution over 1.6 km. *Phys. Rev. Lett.*, 84:5652–5655, 2000.

[19] R. Y. Q. Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.*, 11:045024, 2009.

[20] Joe C. Campbell. Recent advances in avalanche photodiodes. *J. Lightwave Technol.*, 34(2):278–285, Jan 2016.

[21] Alberto Carrasco-Casado, Hideki Takenaka, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, and Morio Toyoshima. QKD from a microsatellite: the SOTA experience. In *SPIE 10660, Quantum Information Science, Sensing, and Computation X*, page 106600B, 2018.

[22] Poompong Chaiwongkhot, Katanya B. Kuntz, Yanbao Zhang, Anqi Huang, Jean-Philippe Bourgoin, Shihan Sajeed, Norbert Lütkenhaus, Thomas Jennewein, and Vadim Makarov. Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence. *Phys. Rev. A*, 99:062315, Jun 2019.

[23] P. A. Childs and W. Eccleston. Impact ionization induced minority carrier injection by avalanching p-n junctions. *J. Appl. Phys.*, 55:4304–4308, 1984.

[24] A. G. Chynoweth and K. G. McKay. Photon emission from avalanche breakdown in silicon. *Phys. Rev.*, 102(2):369–376, Apr 1956.

[25] Federal Financial Institutions Examination Council. Authentication in an internet banking environment. 2008.

[26] Marcos Curty, Otfried Gühne, Maciej Lewenstein, and Norbert Lütkenhaus. Detecting two-party quantum correlations in quantum-key-distribution protocols. *Phys. Rev. A*, 71:022306, 2005.

[27] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004.

[28] Marcos Curty, Xiongfeng Ma, Bing Qi, and Tobias Moroder. Passive decoy-state quantum key distribution with practical light sources. *Phys. Rev. A*, 81:022310, 2010.

[29] D. Dalacu, K. Mnaymneh, J. Lapointe, X. Wu, P. J. Poole, G. Bulgarini, V. Zwiller, and M. E. Reimer. Ultraclean emission from inasp quantum dots in defect-free wurtzite inp nanowires. *NanoLett*, 11:5919–5923, 2012.

[30] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto. 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors. *Opt. Express*, 14(26):13073–13082, 2006.

[31] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *NPJ Quantum Inf.*, 2, 2016.

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

[33] M. Dušek, M. Jahma, and N. Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A*, 62(2):022306, Jul 2000.

[34] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited review article: Single-photon sources and detectors. *Rev. Sci. Instrum*, 82:071101–25, 06 2011.

[35] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Single-photon sources and detectors. *Rev. Sci. Instrum.*, 82:071101, 2011.

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

[37] C. Erven, C. Couteau, R. Laflamme, and G.Weihs. Entangled quantum key distribution over two free-space optical links. *Opt. Express*, 16:16840–16853, 2008.

[38] C Erven, B Heim, E Meyer-Scott, J P Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, 2012.

[39] Agnes Ferenczi, Varun Narasimhachar, and Norbert Lütkenhaus. Security proof of the unbalanced phase-encoded bennett-brassard 1984 protocol. *Phys. Rev. A*, 86:042327, 2012.

[40] A. Fognini, A. Ahmadi, M. Zeeshan, J. T. Fokkens, S. J. Gibson, N. Sherlekar, S. J. Daley, D. Dalacu, P. J. Poole, K. D. Jöns, V. Zwiller, and M. E. Reimer. Dephasing free photon entanglement with a quantum dot. *ACS Photonics*, 6:1656, 2019.

[41] D Fukuda, G Fujii, T Numata, A Yoshizawa, H Tsuchida, H Fujino, H Ishii, T Itatani, S Inoue, and T Zama. Photon number resolving detection with high speed and high quantum efficiency. *Metrologia*, 46(4):S288–S292, 2009.

[42] Daiji Fukuda, Go Fujii, Takayuki Numata, Kuniaki Amemiya, Akio Yoshizawa, Hidemi Tsuchida, Hidetoshi Fujino, Hiroyuki Ishii, Taro Itatani, Shuichiro Inoue, and Tatsuya Zama. Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. *Opt. Express*, 19(2):870–875, 2011.

[43] D. K. Gautam, W. S. Khokle, and K. B. Garg. Photon emission from reverse-biased silicon P-N junctions. *Solid-State Electron.*, 31:219–222, 1988.

[44] 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. *Nat. Commun.*, 2:349, 2011.

[45] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[46] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73(2):022320, 2006.

[47] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, 2015.

[48] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller. A short wavelength gigahertz clocked fiber-optic quantum key distribution system. *IEEE J. Quantum Electron.*, 40(7):900–908, 2004.

[49] Karen Gordon, Veronica Marmol, Gerald Buller, Ivan Rech, Sergio Cova, and Paul Townsend. Quantum key distribution system clocked at 2 ghz. *Optics express*, 13:3015–20, 05 2005.

[50] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory*, 49(2):457–475, 2003.

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

[52] R. H. Hadfield. Single-photon detectors for optical quantum information applications. *Nat. Photonics*, 3:696–705, 2009.

[53] E. Hecht. *Optics*. Addison-Wesley world student series. Addison-Wesley, 1998.

[54] Tobias Heindel and et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New Journal of Physics*, 14:083001, 08 2012.

[55] Anqi Huang, Shihan Sajeed, Poompong Chaiwongkhot, Mathilde Soucarros, Matthieu Legré, and Vadim Makarov. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption. *IEEE J. Quantum Electron.*, 52(11):8000211, 2016.

[56] T. Huang, J. Shao, X. Wang, L. Xiao, and S. Jia. Photon emission characteristics of avalanche photodiodes. *Opt. Engineering*, 44:074001, 2005.

[57] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.*, 4:43, 2002.

[58] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, 2003.

[59] H. Iams and B. Salzberg. The secondary emission phototube. *Proceedings of the Institute of Radio Engineers*, 23(1):55–64, 1935.

[60] P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, and A. J. Shields. Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm. *Appl. Phys. Lett.*, 91:161103, 2007.

[61] Kent D Irwin and Gene Charles Hilton. Transition-edge sensors. In *Topics Appl. Phys.*, volume 99, pages 63–150. Springer, 2005.

[62] Jim J. Napolitano J. J. Sakurai. *Modern Quantum Mechanics*. Pearson, 2nd edition, 1994.

[63] Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.*, 16:123030, 2014.

[64] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron.*, 21:6600710, 2015.

[65] Mu-Sheng Jiang, Shi-Hai Sun, Chun-Yan Li, and Lin-Mei Liang. Frequency shift attack on 'plug-and-play' quantum key distribution systems. *J. Mod. Opt.*, 61:147–153, 2014.

[66] Jeongwan Jin, Jean-Philippe Bourgoin, Ramy Tannous, Sascha Agne, Christopher J. Pugh, Katanya B. Kuntz, Brendon L. Higgins, and Thomas Jennewein. Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel. 2019.

[67] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A*, 87:062313, 2013.

[68] A. Kerckhoffs. La cryptographie militaire. *J. des Sciences Militaires*, IX:5–38, January 1883.

[69] A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Gol'tsman, and B. Voronov. Kinetic-inductance-limited reset time of superconducting nanowire photon counters. *Appl. Phys. Lett.*, 88:111116, 2006.

[70] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, 98(14):140502, 2007.

[71] A. Kress, F. Hofbauer, N. Reinelt, M. Kaniber, H. J. Krenner, R. Meyer, G. Böhm, and J. J. Finley. Manipulation of the spontaneous emission dynamics of quantum dots in two-dimensional photonic crystals. *Phys. Rev. B*, 71:241304, Jun 2005.

[72] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter. Long distance free space quantum cryptography. *Proc. SPIE*, 4917:25–31, 2002.

[73] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419(6906):450–450, 2002.

[74] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. The breakdown flash of silicon avalanche photodiodes—back door for eavesdropper attacks? *J. Mod. Opt.*, 48:2039–2047, 2001.

[75] A. Lacaita, S. Cova, A. Spinelli, and F. Zappa. Photon-assisted avalanche spreading in reach-throught photodiodes. *Appl. Phys. Lett.*, 62(6):606–608, 1993.

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

[77] Wang Le, Zhao Sheng-Mei, Gong Long-Yan, and Cheng Wei-Wen. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chinese Physics B*, 24(12):120307, 2015.

[78] Lawton H. Lee, Gary J. Baker, and Robert S. Benson. Correctability limitations imposed by plane-wave scintillation in multiconjugate adaptive optics. *J. Opt. Soc. Am. A*, 23:2602–2612, 2006.

[79] Hong-Wei Li, Shuang Wang, Jing-Zheng Huang, Wei Chen, Zhen-Qiang Yin, Fang-Yi Li, Zheng Zhou, Dong Liu, Yang Zhang, Guang-Can Guo, Wan-Su Bao, and Zheng-Fu Han. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A*, 84:062308, 2011.

[80] Youkuan Li, Dongquan Chen, and Xiangwan Du. Atmospheric scintillation effect on adaptive optics correction. *Proc. SPIE*, 5237:271–280, 2004.

[81] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549:43, 2017.

[82] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Express*, 16(5):3032–3040, 2008.

[83] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express*, 18(8):8587–8594, 2010.

[84] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111:130502, 2013.

[85] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012.

[86] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005.

[87] Marco Lucamarini, Iris Choi, Martin B Ward, James F Dynes, ZL Yuan, and Andrew J Shields. Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X*, 5:031030, 2015.

[88] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61(5):052304, 2000.

[89] N. Lütkenhaus. Quantum key distribution. *Quantum Information and Coherence*, pages 107–146, 2014.

[90] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys.*, 13:113042, 2011.

[91] L. Lydersen and J. Skaar. Security of quantum key distribution with bit and basis dependent detector flaws. *Quantum Inf. Comput.*, 10:60–76, 2010.

[92] L. Lydersen, J. Skaar, and V. Makarov. Tailored bright illumination attack on distributed-phase-reference protocols. *J. Mod. Opt.*, 58(8):680–685, 2011.

[93] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics*, 4:686–689, 2010.

[94] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Thermal blinding of gated detectors in quantum cryptography. *Opt. Express*, 18:27938–27954, 2010.

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

[96] V. Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003, 2009.

[97] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74(2):022313, 2006. erratum ibid. **78**, 019905 (2008).

[98] V. Makarov and D. R. Hjelme. Faked states attack on quantum cryptosystems. *J. Mod. Opt.*, 52:691–705, 2005.

[99] Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed. Creation of backdoors in quantum communications via laser damage. *Phys. Rev. A*, 94:030302, 2016.

[100] Leonard Mandel and Emil Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[101] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.*, 93:180502, Oct 2004.

[102] F Marsili, D Bitauld, A Gaggero, S Jahanmirinejad, R Leoni, F Mattioli, and A Fiore. Physics and application of photon number resolving detectors based on superconducting parallel nanowires. *New Journal of Physics*, 11(4):045022, apr 2009.

[103] Alice Meda, Ivo P. Degiovanni, Alberto Tosi, Zhiliang Yuan, Giogio Brida, and Marco Genovese. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light Sci. Appl.*, 6:e16261, 2016.

[104] Alice Meda, Ivo Pietro Degiovanni, Alberto Tosi, Zhiliang Yuan, Giorgio Brida, and Marco Genovese. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light Sci. Appl.*, 6:e16261, 2017.

[105] Isaac L. Chuang. Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge, 1st edition, 2000.

[106] P Michler, Alper Kiraz, Christoph Becher, Winston Schoenfeld, Pierre Petroff, LD Zhang, Ella Hu, and A Imamoglu. A quantum dot single-photon turnstile device. *Science (New York, N.Y.)*, 290:2282–5, 12 2000.

[107] Aaron J. Miller, Adriana E. Lita, Brice Calkins, Igor Vayshenker, Steven M. Gruber, and Sae Woo Nam. Compact cryogenic self-aligning fiber-to-detector coupling with losses below one percent. *Opt. Express*, 19(10):9102–9110, 2011.

[108] E Moreau, I Robert, J. M. Gérard, I Abram, L Manin, and V Thierry-Mieg. Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities. *Appl. Phys. Lett*, 79:2865, 10 2001.

[109] M. Muller, S. Bounouar, K. D. Jöns, M. Glass, and P. Michler. On-demand generation of indistinguishable polarization-entangled photon pairs. *Nature Photon*, 8:224–228, 2014.

[110] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.*, 11(6):065001, 2009.

[111] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nat. Photonics*, 7:382, 2013.

[112] Roger Newman. Visible light from a silicon p–n junction. *Phys. Rev.*, 100:700–703, 1955.

[113] J. Noda, K. Okamoto, and Y. Sasaki. Polarization-maintaining fibers and their applications. *Journal of Lightwave Technology*, 4(8):1071–1089, 1986.

[114] Robert J. Noll. Zernike polynomials and atmospheric turbulence. *J. Opt. Soc. Am.*, 66(3):207–211, 1976.

[115] National Institute of Standards and Technology. NIST cryptographic standards and guidelines development process (second draft). 2015.

[116] A. Pacelli, A. S. Spinelli, and A. L. Lacaita. Impact ionization in silicon: A microscopic view. *J. Appl. Phys.*, 83(9):4760–4764, 1998.

[117] James L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1970.

[118] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. The SECOQC quantum key distribution network in Vienna. *New J. Phys.*, 11(7):075001, 2009.

[119] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer. Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.*, 11(4):045007, 2009.

[120] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[121] P.Grünwald. Effective second-order correlation function and single-photon detection. *New J.Phys.*, 21:093003, 2019.

[122] Paulo Vinicius Pereira Pinheiro, Poompong Chaiwongkhot, Shihan Sajeed, Rolf T. Horn, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. *Opt. Express*, 26(16):21020–21032, Aug 2018.

[123] Mateusz Polnik, Luca Mazzarella, Marilena Di Carlo, Daniel KL Oi, Annalisa Riccardi, and Ashwin Arulselvan. Scheduling of space to ground quantum key distribution. *EPJ. Quant. Tech.*, 7(3), 01 2020.

[124] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Sci. Technol.*, 2:024009, 2017.

[125] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.*, 7(1-2):73–82, 2007.

[126] Bing Qi. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Phys. Rev. A*, 91:020303, 2015.

[127] Markus Rau, Tobias Vogl, Giacomo Corrielli, Gwenaelle Vest, Lukas Fuchs, Sebastian Nauerth, and Harald Weinfurter. Spatial mode side channels in free-space qkd implementations. *IEEE J. Quantum. Electron.*, 21:6600905, 2015.

[128] M. E. Reimer, G. Bulgarini, N. Akopian, M. Hocevar, M. B. Bavinck, M. A. Verheijen, E. P. A. M. Bakkers, L. P. Kouwenhoven, and V. Zwiller. Bright single-photon sources in bottom-up tailored nanowires. *Nat Commun*, 3:737, 2012.

[129] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332, 2005.

[130] R. Renner and R. Koenig. Universally composable privacy amplification against quantum adversaries. In J. Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005*, volume 3378 of *LNCS*, pages 407–425. Springer Verlag, Berlin, February 2005.

[131] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.

[132] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, 1978.

[133] Brandon Rodenburg, Mohammad Mirhossein, Mehul Malik, Omar S Magana-Loaiza, Michael Yanakas, Laura Maher, Nicholas K Steinhoff, Glenn A Tyler, and Robert W Boyd. Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication. *New J. Phys.*, 16:033020, 2014.

[134] K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Opt. Express*, 14(2):527–534, 2006.

[135] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A*, 91:062301, 2015.

[136] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty. Insecurity of detector-device-independent quantum key distribution. *Phys. Rev. Lett.*, 117:250505, 2016.

[137] S. Sajeed, C. Minshull, N. Jain, and V. Makarov. Invisible trojan-horse attack. *Sci. Rep.*, 7:8403, 2017.

[138] Shihan Sajeed, Igor Radchenko, Sarah Kaiser, Jean-Philippe Bourgoin, Anna Pappa, Laurent Monat, Matthieu Legré, and Vadim Makarov. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A*, 91:032326, 2015.

[139] Yousuke Sano, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Secure key rate of the BB84 protocol using finite sample bits. *Journal of Physics A: Mathematical and Theoretical*, 43(49):495302, nov 2010.

[140] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19:23590–23600, 2011.

[141] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301–1350, 2009.

[142] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, 2008.

[143] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98(1):010504, 2007.

[144] P. Senellart, G. Solomon, and A. White. High-performance semiconductor quantum-dot single-photon sources. *Nature Nanotech*, 12:1026–1039, 2017.

[145] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715, 1949.

[146] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[147] Birgit Stiller, Imran Khan, Nitin Jain, Paul Jouguet, Sebastien Kunz-Jacques, Eleni Diamanti, Christoph Marquardt, and Gerd Leuchs. Quantum hacking of continuous-variable quantum key distribution systems: realtime Trojan-horse attacks. In *Proc. CLEO 2015*, page FF1A.7. Optical Society of America, 2015.

[148] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden. High speed coherent one-way quantum key distribution prototype.

[149] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4:41, 2002.

[150] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):075003, 2009.

[151] S.-H. Sun, M.-S. Jiang, and L.-M. Liang. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. *Phys. Rev. A*, 83(6):062331, 2011.

[152] K. Takemoto, Y. Nambu, and T. Miyazawa. Quantum key distribution over 120km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci Rep*, 5:14383, 2015.

[153] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto. Differential phase shift quantum key distribution experiment over 105 km fibre. *New J. Phys.*, 7(1):232, 2005.

[154] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics*, 1(6):343–348, 2007.

[155] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X*, 6:011024, 2016.

[156] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Phys. Rev. A*, 66:062304, Dec 2002.

[157] Robert Tyson. *Principles of Adaptive Optics*. CRC Press, 3rd edition, 2010.

[158] R. Ursin, T. Jennewein, J. Kofler, J.M. Perdigues, L. Cacciapuoti, C.J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R.H. Hadfield, R. Laflamme, N. Lütkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J.P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger. Space-quest, experiments with quantum entanglement in space. *Europhys. News*, 40:26–29, 2009.

[159] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nat. Phys.*, 3(7):481–486, 2007.

[160] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *J. Mod. Opt.*, 48(13):2023–2038, 2001.

[161] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115:040502, 2015.

[162] S. Vinogradov, T. Vinogradova, V. Shubin, D. Shushakov, and C. Sitarsky. Efficiency of solid state photomultipliers in photon number resolution. *IEEE Transactions on Nuclear Science*, 58(1):9–16, 2011.

[163] M. Waldschmidt and S. Wittig. Backscattering and bremsstrahlung of electrons in a silicon detector. *Nucl. Instr. Meth.*, 64:189–191, 1968.

[164] H. Wang, Y. He, T. Chung, and et al. Towards optimal single-photon sources from polarized microcavities. *Nat. Photonics*, 13:770–775, 8 2019.

[165] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2 ghz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.*, 37:1008–1010, 2012.

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

[167] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. After-gate attack on a quantum cryptosystem. *New J. Phys.*, 13:013043, 2011.

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

[169] F. Xu, B. Qi, and H.-K. Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.*, 12:113026, 2010.

[170] Eli Yablonovitch. Inhibited spontaneous emission in solid-state physics and electronics. *Phys. Rev. Lett.*, 58:2059–2062, May 1987.

[171] Zhizhong Yan, Deny R. Hamel, Aimee K. Heinrichs, Xudong Jiang, Mark A. Itzler, and Thomas Jennewein. An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode. *Review of Scientific Instruments*, 83(7):073105, 2012.

[172] Hua-Lei Yin, Wei-Long Wang, Yan-Lin Tang, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Wei-Jun Zhang, Hao Li, Ittoop Vergheese Puthoor, Li-Xing You, Erika Andersson, Zhen Wang, Yang Liu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Marcos Curty, Teng-Yun Chen, and Jian-Wei Pan. Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phys. Rev. A*, 95:042338, 2017.

[173] Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Experimental quasi-single-photon transmission from satellite to earth. *Opt. Express*, 21(17):20032–20040, 2013.

[174] Yanbao Zhang and Norbert Lütkenhaus. Entanglement verification with detection-efficiency mismatch. *Phys. Rev. A*, 95:042319, 2017.

[175] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78(4):042333, 2008.

APPENDICES

Appendix A

Codes for free-space detector scanning

A.1 Matlab Code for Phase hologram generation

Here we show the MATLAB code for hologram phase mask generation. Adapted from original code written by Katanya Kuntz.

```
% Code for hologram phase mask generation.
%Adapted from original code written by Katanya kuntz.

function PhaseAngleAp = HoloGenHigherorder(weight,theta,rho,Aperture)

% This script generates a superposition of Zernike modes, each with a
% random weighting chosen from a certain range


% ************************************
% ************ Parameters ************
% ************************************

% TIP = 0; % Additional Z2 for spatial separation of 0 & 1st orders
TIP = 60;
TILT = 40; % Additional Z2 for spatial separation of 0 & 1st orders
% TILT = 40;  % Additional Z3 for spatial separation of 0 & 1st orders
```

```
% Z2_coeff = 1;  % Keep/remove Z2 from hologram 0=remove, 1=keep
% Z3_coeff = 1;  % Keep/remove Z3 from hologram 0=remove, 1=keep

%% ************************************************************************
%% ********************** Generate phase hologram **********************
%% ************************************************************************
%%only first 7 terms are used in our experiment.
Z2 = 2.*rho.*cos(theta);                                    % Tip n=1,m=1
Z3 = 2.*rho.*sin(theta);                                    % Tilt n=1,m=-1
Z4 = sqrt(3).*(2.*(rho.^2)-1);                              % Defocus n=2,m=0
Z5 = sqrt(6).*rho.^2.*sin(2.*theta);          % Oblique astigmatism n=2,m=-2
Z6 = sqrt(6).*rho.^2.*cos(2.*theta);          % Vertical astigmatism n=2,m=2
Z7 = sqrt(8).*(3.*rho.^3-2.*rho).*sin(theta);       % Vertical coma n=3,m=-1
% Z8 = sqrt(8).*(3.*rho.^3-2.*rho).*cos(theta);  % Horizontal coma n=3,m=1
% Z9 = sqrt(8).*rho.^3.*sin(3.*theta);           % Trefoil n=3,m=-3
% Z10 = sqrt(8).*rho.^3.*cos(3.*theta);          % Trefoil n=3,m=3
% Z11 = sqrt(5).*(6.*rho.^4-6.*rho.^2+1);        % Spherical n=4,m=0
% Z12 = sqrt(10).*(4.*rho.^4-3.*rho.^2).*cos(2.*theta);    % n=4,m=2
% Z13 = sqrt(10).*(4.*rho.^4-3.*rho.^2).*sin(2.*theta);    % n=4,m=-2
% Z14 = sqrt(10).*rho.^4.*cos(4.*theta);                   % n=4,m=4
% Z15 = sqrt(10).*rho.^4.*sin(4.*theta);                   % n=4,m=-4
% Z16 = sqrt(12).*(10.*rho.^5-12.*rho.^3+3.*rho).*cos(theta);
%n=5,m=1
% Z17 = sqrt(12).*(10.*rho.^5-12.*rho.^3+3.*rho).*sin(theta);
%n=5,m=-1
% Z18 = sqrt(12).*(5.*rho.^5-4.*rho.^3).*cos(3.*theta);
%n=5,m=3
% Z19 = sqrt(12).*(5.*rho.^5-4.*rho.^3).*sin(3.*theta);
%n=5,m=-3
% Z20 = sqrt(12).*rho.^5.*cos(5.*theta);
%n=5,m=5
% Z21 = sqrt(12).*rho.^5.*sin(5.*theta);
%n=5,m=-5

PhaseMask = (weight(2)+TIP).*Z2 + (weight(3)+TILT).*Z3 +
weight(4).*Z4 + weight(5).*Z5 + weight(6).*Z6 + weight(7).*Z7 +
weight(14).*Z14 ;
```

```
PhaseAngleAp = (angle(exp(1i.*PhaseMask))+pi).*Aperture;
```

A.2 Matlab Code for free-space detector scanning (tip-tilt modes)

Here we show the MATLAB code for tip-tilt spatial mode scanning with turbulence emulation phase mask.

```
%%%%%%%%tip-tilt spatial mode scanning%%%%%%%%%%%%%%%%%%%%

clear; close all; clc;

nTerms = 15;  % number of Zernike polynomial terms

weight = zeros(nTerms,1);


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Generate 'turbulence-free' phase hologram for alignment
% This hologram generation code is adapted from the original code
%writen by Katanya Kuntz
maxWeight = 25;
steps = 20;
stepSize = maxWeight/steps;

xrange = 2;
r = 1;
DiagHolo = 20e-2;       % Diameter of initial beam [m]
% gridA = 40;           % needs to be an even number;
                        % grid will be 2*gridA X 2*gridA
gridA = 800;            % needs to be an even number;
                        % grid will be 2*gridA X 2*gridA
xa = DiagHolo/(2*gridA);  % spacing between pixels in INPUT grid

aa = -xa*gridA:xa:gridA*xa;    % length of input grid
```

```
[C,D] = meshgrid(aa,aa);          % input grid
l1 = length(C);

xx = -1*xrange:((2*xrange)/(l1-1)):xrange;
[X,Y] = meshgrid(xx,xx);
[theta,rho] = cart2pol(X,Y);  % This makes theta [-pi,pi]

% ************************************************
% ************ Generate a circular aperture ************
% ************************************************
x = length(rho);
for k=1:x
for j=1:x
if rho(k,j) <= r
Aperture(k,j) = 1;
else
Aperture(k,j) = 0;
end
end
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


PhaseAngleAp = HoloGen(weight,theta,rho,Aperture);

pos = [350 800 1243 1200];

figure(1);
%figure(FigNum);
pcolor(PhaseAngleAp), shading interp
colormap gray
set(gca,'visible','off');
set(gcf,'Color','black');
set(0, 'DefaultFigurePosition', pos);
title('Phase hologram')
% saveas(gcf,'TurbCoeffs/20160725/D=20cm, r0=7cm_20160725T.png');
```

```
% weight(2) = 2;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%55

%Begin scanning
% connect to counters
% fclose(instrfind);

h_APD = serial('COM5');
v_APD = serial('COM6');
d_APD = serial('COM4');
a_APD = serial('COM7');

fopen(h_APD);
fopen(v_APD);
fopen(d_APD);
fopen(a_APD);

fprintf(h_APD, 'SRCE0');
fprintf(v_APD, 'SRCE0');
fprintf(d_APD, 'SRCE0');
fprintf(a_APD, 'SRCE0');

fprintf(h_APD, 'AUTM0');
fprintf(h_APD, 'MODE6');
fprintf(h_APD, 'GATE1');
fprintf(h_APD, 'LEVL1,1.4');
fprintf(h_APD, 'TERM1,1');
fprintf(h_APD, 'SIZE1');

fprintf(v_APD, 'AUTM0');
fprintf(v_APD, 'MODE6');
fprintf(v_APD, 'GATE1');
fprintf(v_APD, 'LEVL1,1.4');
fprintf(v_APD, 'TERM1,1');
fprintf(v_APD, 'SIZE1');
```

```
fprintf(d_APD,'AUTM0');
fprintf(d_APD,'MODE6');
fprintf(d_APD,'GATE1');
fprintf(d_APD,'LEVL1,1.4');
fprintf(d_APD,'TERM1,1');
fprintf(d_APD,'SIZE1');

fprintf(a_APD,'AUTM0');
fprintf(a_APD,'MODE6');
fprintf(a_APD,'GATE1');
fprintf(a_APD,'LEVL1,1.4');
fprintf(a_APD,'TERM1,1');
fprintf(a_APD,'SIZE1');


pause(5); % wait for connection and adaptive parts to be
          % stabelized useful for mechanical scanning
p = xlsread('APDcorrection_poly8fit.xlsx');
maxMismatchH = 1;
maxMismatchV = 1;
maxMismatchD = 1;
maxMismatchA = 1;
count = zeros(4,1);
paulo = measure_APD(h_APD,v_APD,d_APD,a_APD);
det10 = paulo(1);
det20 = paulo(2);
det30 = paulo(3);
det40 = paulo(4);
%det4(row,col)

det30 = correction(det30,p(2,:))
det40 = correction(det40,p(4,:))
det10 = correction(det10,p(3,:))
det20 = correction(det20,p(1,:))

row = 1;
col = 1;
for yPos = -maxWeight:stepSize:maxWeight
```

```
weight(2) = yPos;
for zPos = -maxWeight:stepSize:maxWeight
weight(3) = zPos;

PhaseAngleAp = HoloGen(weight,theta,rho,Aperture);

pause(1);

paulo = measure_APD(h_APD,v_APD,d_APD,a_APD);
det1(row,col) = paulo(1);

det2(row,col) = paulo(2);
%det2(row,col)

det3(row,col) = paulo(3);
%det3(row,col)

det4(row,col) = paulo(4);
%det4(row,col)


det3c = correction2order(det3(row,col),p(2,:))/det10;
det4c = correction2order(det4(row,col),p(4,:))/det20;
det1c = correction2order(det1(row,col),p(3,:))/det30;
det2c = correction2order(det2(row,col),p(1,:))/det40;


mismatchH = det1c/max(det3c,det4c);
if mismatchH > maxMismatchH
count(1) = count(1)+1;
maxMismatchH = mismatchH
maxMismatchHtmp(count(1)) = mismatchH;
OptWeightHtmp(count(1),:) = weight;

end

mismatchV = det2c/max(det3c,det4c);
if mismatchV > maxMismatchV
```

```
count(2) = count(2)+1;
maxMismatchV = mismatchV
maxMismatchVtmp(count(2)) = mismatchV;
OptWeightVtmp(count(2),:) = weight;
end


mismatchD = det3c/max(det1c,det2c);
if mismatchD > maxMismatchD
count(3) = count(3)+1;
maxMismatchD = mismatchD
maxMismatchDtmp(count(3)) = mismatchD;
OptWeightDtmp(count(3),:) = weight;
end

mismatchA = det4c/max(det1c,det2c);
if mismatchA > maxMismatchA
count(4) = count(4)+1;
maxMismatchA = mismatchA
maxMismatchAtmp(count(4)) = mismatchA;
OptWeightAtmp(count(4),:) = weight;
end

figure(1);
pcolor(PhaseAngleAp), shading interp
row = row+1;
end
row = 1;
col = col+1
end

disp('Scan finished')
%%save data%%%%%%
p = 0;

path = '2018-05-15-ScanSLM-BG430-620-830-550-fixedSLMsetup';
filename = [path '.xlsx'];
xlswrite(filename,squeeze(det1(:,:)),'Sheet1','A1');
```

```
xlswrite(filename,squeeze(det2(:,:)),'Sheet2','A1');
xlswrite(filename,squeeze(det3(:,:)),'Sheet3','A1');
xlswrite(filename,squeeze(det4(:,:)),'Sheet4','A1');
disp('file saved')
%
```

A.3 Matlab Code for free-space detector scanning (Higher-order)

```
%%%%%%%%Higher ofder scanning%%%%%%%%%%%%%%%%%%
clear; close all; clc;

nTerms = 7;          % number of Zernike polynomial terms

weight = zeros(nTerms,1);
p = xlsread('APDcorrection_poly8fit.xlsx');

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%5
%Generate 'turbulence-free' phase hologram for alignment and reference
% This hologram generation/projection code is adapted from the original
% code writen by Katanya Kuntz

maxWeight = 8; %due to hardware limitation. Higher weight for higher order t
steps = 4;
stepSize = maxWeight/steps;

xrange = 2;
r = 1;
DiagHolo = 20e-2;       % Diameter of initial beam [m]
% gridA = 40;           % needs to be an even number;
                        % grid will be 2*gridA X 2*gridA
gridA = 800;           % needs to be an even number;
                       % grid will be 2*gridA X 2*gridA
xa = DiagHolo/(2*gridA); % spacing between pixels in INPUT grid
```

```
aa = -xa*gridA:xa:gridA*xa;        % length of input grid
[C,D] = meshgrid(aa,aa);           % input grid
l1 = length(C);

xx = -1*xrange:((2*xrange)/(l1-1)):xrange;
[X,Y] = meshgrid(xx,xx);
[theta,rho] = cart2pol(X,Y);  % This makes theta [-pi,pi]

% ***************************************************
% ************ Generate a circular aperture ************
% ***************************************************
x = length(rho);
for k=1:x
for j=1:x
if rho(k,j) <= r
Aperture(k,j) = 1;
else
Aperture(k,j) = 0;
end
end
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
weight(2) = 2.5;
weight(3) = 8.75;

PhaseAngleAp = HoloGenHigherorder(weight,theta,rho,Aperture);

pos = [350 800 1243 1200];

figure(1);
%figure(FigNum);
pcolor(PhaseAngleAp), shading interp
colormap gray
set(gca,'visible','off');
set(gcf,'Color','black');
set(0, 'DefaultFigurePosition', pos);
title('Phase hologram')
```

```
%end hologram generation
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%55

% connect to counters
% fclose(instrfind);

h_APD = serial('COM5');
v_APD = serial('COM6');
d_APD = serial('COM4');
a_APD = serial('COM7');

fopen(h_APD);
fopen(v_APD);
fopen(d_APD);
fopen(a_APD);

fprintf(h_APD, 'SRCE0');
fprintf(v_APD, 'SRCE0');
fprintf(d_APD, 'SRCE0');
fprintf(a_APD, 'SRCE0');

fprintf(h_APD, 'AUTM0');
fprintf(h_APD, 'MODE6');
fprintf(h_APD, 'GATE1');
fprintf(h_APD, 'LEVL1,1.4');
fprintf(h_APD, 'TERM1,1');
fprintf(h_APD, 'SIZE1');

fprintf(v_APD, 'AUTM0');
fprintf(v_APD, 'MODE6');
fprintf(v_APD, 'GATE1');
fprintf(v_APD, 'LEVL1,1.4');
fprintf(v_APD, 'TERM1,1');
fprintf(v_APD, 'SIZE1');

fprintf(d_APD, 'AUTM0');
fprintf(d_APD, 'MODE6');
```

```
fprintf(d_APD,'GATE1');
fprintf(d_APD,'LEVL1,1.4');
fprintf(d_APD,'TERM1,1');
fprintf(d_APD,'SIZE1');

fprintf(a_APD,'AUTM0');
fprintf(a_APD,'MODE6');
fprintf(a_APD,'GATE1');
fprintf(a_APD,'LEVL1,1.4');
fprintf(a_APD,'TERM1,1');
fprintf(a_APD,'SIZE1');

disp('Initiate scanning: Run!!!!!!!')
pause(10);

row = 1;
col = 1;
% weight(2) = 12.5;
% weight(3) = 5;
maxMismatchH = 1;
maxMismatchV = 1;
maxMismatchD = 1;
maxMismatchA = 1;
count = zeros(4,1);
maxMismatchH2 = 1;
maxMismatchV2 = 1;
maxMismatchD2 = 1;
maxMismatchA2 = 1;
count2 = zeros(4,1);
paulo = measure_APD(h_APD,v_APD,d_APD,a_APD);
det10 = paulo(1);
det20 = paulo(2);
det30 = paulo(3);
det40 = paulo(4);

det30 = correction(det30,p(2,:))
det40 = correction(det40,p(4,:))
det10 = correction(det10,p(3,:))
```

```
det20 = correction(det20,p(1,:))

for i7 = -maxWeight-stepSize:stepSize:maxWeight
weight(7) = i7;
i7
for i6 = -maxWeight-stepSize:stepSize:maxWeight
weight(6) = i6;
i6
for i5 = -maxWeight-stepSize:stepSize:maxWeight
weight(5) = i5;
i5
for i4 = -maxWeight:stepSize:maxWeight
weight(4) = i4;

figure(1);
pcolor(PhaseAngleAp), shading interp %display

PhaseAngleAp = HoloGenHigherorder(weight,theta,rho,Aperture);
%Calc, intententionally swap Calc/Display give 'pause'
%time while calcurate next hologram.
pause(3);

paulo = measure_APD(h_APD,v_APD,d_APD,a_APD); %readout
det1 = paulo(1);

det2 = paulo(2);

det3 = paulo(3);

det4 = paulo(4);

%correcting counts
det3c = correction2order(det3,p(2,:))/det10;
det4c = correction2order(det4,p(4,:))/det20;
det1c = correction2order(det1,p(3,:))/det30;
det2c = correction2order(det2,p(1,:))/det40;

%record combinations that cause min and max mismatch
```

```
%=================================Minmismatch=================================
mismatchH = det1c/max(det3c,det4c);
if mismatchH > maxMismatchH
count(1) = count(1)+1;
maxMismatchH = mismatchH
maxMismatchHtmp(count(1)) = mismatchH;
w = weight
w(4) = weight(4)-stepSize;
OptWeightHtmp(count(1),:) = w;

end

mismatchV = det2c/max(det3c,det4c);
if mismatchV > maxMismatchV
count(2) = count(2)+1;
maxMismatchV = mismatchV
maxMismatchVtmp(count(2)) = mismatchV;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightVtmp(count(2),:) = w;
end


mismatchD = det3c/max(det1c,det2c);
if mismatchD > maxMismatchD
count(3) = count(3)+1;
maxMismatchD = mismatchD
maxMismatchDtmp(count(3)) = mismatchD;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightDtmp(count(3),:) = w;
end

mismatchA = det4c/max(det1c,det2c);
if mismatchA > maxMismatchA
count(4) = count(4)+1;
maxMismatchA = mismatchA
maxMismatchAtmp(count(4)) = mismatchA;
```

```
w = weight;
w(4) = weight(4)-stepSize;
OptWeightAtmp(count(4),:) = w;
end

%=============================Maxmismatch=============================
mismatchH2 = det1c/min(det3c,det4c);
if mismatchH2 > maxMismatchH2
count2(1) = count2(1)+1;
maxMismatchH2 = mismatchH2
maxMismatchHtmp2(count(1)) = mismatchH2;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightHtmp2(count(1),:) = w;
end

mismatchV2 = det2c/min(det3c,det4c);
if mismatchV2 > maxMismatchV2
count(2) = count(2)+1;
maxMismatchV2 = mismatchV2
maxMismatchVtmp2(count(2)) = mismatchV2;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightVtmp2(count(2),:) = w;
end

mismatchD2 = det3c/min(det1c,det2c);
if mismatchD2 > maxMismatchD2
count(3) = count(3)+1;
maxMismatchD2 = mismatchD2
maxMismatchDtmp2(count(3)) = mismatchD2;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightDtmp2(count(3),:) = w;
end

mismatchA2 = det4c/min(det1c,det2c);
if mismatchA2 > maxMismatchA2
```

```
count2(4) = count2(4)+1;
maxMismatchA2 = mismatchA2
maxMismatchAtmp2(count(4)) = mismatchA2;
w = weight;
w(4) = weight(4)-stepSize;
OptWeightAtmp2(count(4),:) = w;
end
end
end
end
end

disp('Scan finished')
c = clock;
disp(num2str(c))
```

Appendix B

Codes for Quantum dot QKD experiment

Here we show the Python code for coincidence search and histogram plotting

B.1 Python code for coincidence detection plot

```
# This code is used find the coincidences between two detectors

from scipy.optimize import curve_fit
from pandas import *
import matplotlib.pyplot as plt
import numpy as np
#-------------------------------------------------------------------------
#---Import 'coinciudent' clicks between two detectors
f = open("G280.txt","r")
if f.mode == 'r':
print('file opened')

data = np.genfromtxt(f)
f.close()
# begin coincident finding
```

```
time = []#np.ones((len(data),3))*2e-9
time3 = []
time4 = []
time5 = []
time6 = []
tic = [0]
coinc = []
channel = np.zeros(30)
j = 0
en = len(data)-2600000;
for i in range(1000,en):

# The two timetagger ports used are port 4 and 6.
tic.append(data[i,1])
if int(data[i,0])==4:
time4.append(data[i,:])
for k in range(1,20):
if (data[i+k,0]==6):
coinc.append((data[i+k,1]-data[i,1])*0.000000000078125)
j+=1
if (data[i-k,0]==6):
coinc.append((data[i-k,1]-data[i,1])*0.000000000078125)
j+=1

####end coinc finding----------


#SPlot histogram. The plot is used to find the shift of
#'0'peak (electronic delay). This delay and position of
#side peaks are used in the following g2 fitting and calculation.
fig= plt.figure(figsize=(6,3))
plt.hist(coinc, bins=100, range = (-50e-9,50e-9))
plt.title("coincidences")
plt.savefig('coincidence44.pdf')
plt.show()
```

Here is the Python code for coincidence histogram fitting. The fitting is used for noise subtraction. This code is adapted from the original code written by Arash Ahmadi.

```
#----coincidence finder----comment these after get 'coinc' data
f = open("G280.txt","r")
if f.mode == 'r':
   print('file opened')

data = np.genfromtxt(f)
f.close()

## begin fitting
df1 = []
t0 = 6.4e-9 #time shift to center the plot,
            #estimate from 'coincident plot' above
decimation=1
dt=0.0781e-9 #resolution of the time tagger
HFONT = {'fontname':'Times'}

df1[:] = [x-t0 for x in coinc] #centering the data to t=0

binss = 240
hdf, bin_edges = np.histogram(df1,bins=binss, range
 = (-binss/4*1e-9,binss/4*1e-9))

#choosing the center points of the two side peaks to
#analyze, estimate from the coincident plot
cpp = 0 #center
cp1 = 12.88e-9  #side1
cp2 = 12.88e-9*2 #side2
w= 5e-9 #width of each peak.. +/- w-ns from the center point

plt.plot(bin_edges[:-1],hdf) #plotting the whole data

#Fitting

#SidePeak 1
sp1 = hdf[int(binss/2+(cp1-w)*2e9):int(binss/2+(cp1+w)*2e9)]
edge1 = bin_edges[int(binss/2+(cp1-w)*2e9):int(binss/2+(cp1+w)*2e9)]
```

```
#SidePeak 2
sp2=hdf[int(binss/2+(cp2-w)*2e9):int(binss/2+(cp2+w)*2e9)]
edge2 = bin_edges[int(binss/2+(cp2-w)*2e9):int(binss/2+(cp2+w)*2e9)]

#Center-- or Centre...what ever the locals says...
cp = hdf[int(binss/2+(cpp-w)*2e9):int(binss/2+(cpp+w)*2e9)]
edgecp = bin_edges[int(binss/2+(cpp-w)*2e9):int(binss/2+(cpp+w)*2e9)]

###define hyperbolic distribution function
#https://en.wikipedia.org/wiki/Hyperbolic_distribution
#Only bi-esponential term is needed here
def biexpi(x, *p):
A1, A2, mu, tau1,tau2 = p
return A1*np.exp(-np.abs(x-mu)/tau1)

#plotting the two side peaks
plt.plot(edge1,sp1,'r')
plt.plot(edge2,sp2,'g')

#fitting the two side peaks with bi-exponential function
#...beware of p0 range of parameter
coeff, var_matrix  = curve_fit(biexpi,  edge1, sp1, \
  p0=[1000., 50, cp1, 1e-9,20e-9 ])
coeff2, var_matrix2 = curve_fit(biexpi, edge2, sp2, \
p0=[1000., 50, cp2, 1e-9,20e-9 ])
coeffc, var_matrixc = curve_fit(biexpi, edgecp, cp, \
p0=[100., 10, 0, 1e-9,20e-9 ])

# Get the fitted curve
dt = np.linspace(-binss/4*1e-9,binss/4*1e-9,binss)
pulse_fit = biexpi(dt, *coeff)
pulse_fit2 = biexpi(dt,*coeff2)
pulse_fitcp = biexpi(dt,*coeffc)

plt.plot(dt,pulse_fit)
plt.plot(dt,pulse_fit2)
plt.plot(dt,pulse_fitcp)
plt.plot(dt,pulse_fit+pulse_fit2)
```

```
#plt.plot(dt,pulse_fitcp-(pulse_fit+pulse_fit2),'k')
plt.savefig('g2fit_2.pdf')
#plt.xlim((100,125))
plt.show()
```

The noise level is determined from the fitting. After noise subtraction, the value of g2 can then be calculated from the height of center peak divided by the avarage height of side peaks.

B.2 Matlab code for key rate calculation

Here is the MATLAB code for key length calculation for Quantum dot QKD experiment

```
# Practica key lengtyh calculation for QDot and WCP QKD
clc;
clear all;

RepDec = 80e6;      %repitition rate decoy
rep1 = 2.6*1e6;     %repetition rate QD

flight_time = 100; %key exchange time in second

effd = 1;           %coupling eff decoy
eff = .5;           %coupling efficiency qdot

q=1/2;              %sifting factor

loss_corr = 1;      %loss correction term(lambda mismatch of attenuator)

RepDec = RepDec*flight_time;
rep1 = rep1*flight_time;

N = RepDec;    %%post processing Block size

epsilonf = 1e-9; %epsilon for finite size
theta_Bob = 0.5; %Bob's detecton eff
```

```
fe=1.3; %error correction eff
e0=1/2; %fraction of error from background count
e_detector = 5*10^(-2); %system error
dc = 500;        %dark count per second per detection basis
background_noise = 300;
dc_pd = (dc+background_noise*q*theta_Bob)*5e-9; %darkcount per detection


%%%%%%%%%%%decoy%%%%%%%%%%%%
Len=400;
u=0.5; %mu
v=0.1; %nu

Y0=dc_pd; %background count per detection

l=1:Len;
x=l./10;
t_AB = 10.^(-x./10);
theta= t_AB.*theta_Bob;
Qu1=Y0+1-exp(-theta*u);
Qv1=Y0+1-exp(-theta*v);


Eu=(e0*Y0+e_detector*(1-exp(-theta*u)))./Qu1;
Ev=(e0*Y0+e_detector*(1-exp(-theta*v)))./Qv1;
Y1=u/(u*v-v^2)*(Qv1*exp(v)-Qu1*exp(u)*v^2/u^2-(u^2-v^2)*Y0/(u^2));


A = u./(v.*(u-v)).*Qv1.*(1-2.*Ev).*exp(v)-v./(u.*
(u-v)).*Qu1.*(1-2.*Eu).*exp(u);
B = min((Ev.*Qv1.*exp(v))./v,(Eu.*Qu1.*exp(u)-Ev.*
Qv1.*exp(v))./(u-v));
c1 = u/(v*(u-v))*exp(v);
c2 = v/(u*(u-v))*exp(u);



HE= -Eu.*log2(Eu)-(1-Eu).*log2(1-Eu);
```

```
Q1= u^2*exp(-u)/(u*v-v^2)*(Qv1*exp(v)-Qu1*exp(u)*
v^2/u^2-(u^2-v^2)*Y0/u^2);
%e= (Ev.*Qv1.*exp(v)-e0*Y0)./Y1*v;
%Q1=Y1*u*exp(-u);

e= (Eu.*Qu1.*exp(u))./Y1*v.*x/5;
He=-e.*log2(e)-(1-e).*log2(1-e);
R2 = q*(-Qu1.*fe.*HE+Q1.*(1-He)); %key rate inf

%%finite size correction term for decoy
%%characterization, Curty et.al.%%%

N2=Q1*RepDec*effd;

ua = 10; %ua-Sigma within central estimation
Nu = .9*N2;
Nv = .1*N2;
deltaQu1 = ua*sqrt(Qu1/Nu);
deltaQv1 = ua*sqrt(Qv1/Nv);

Qu1=Qu1+deltaQu1;
Qv1=Qv1+deltaQv1;

Eu=(e0*Y0+e_detector*(1-exp(-theta*u)))./Qu1;
Ev=(e0*Y0+e_detector*(1-exp(-theta*v)))./Qv1;

deltaEuQu = ua.*sqrt(2.*Eu.*Qu1./Nu);
deltaEvQv = ua.*sqrt(2.*Ev.*Qv1./Nv);
deltaA = sqrt((c1.*deltaQv1).^2+4.*(c1.*deltaEvQv).^2+
(c2.*deltaQu1).^2+4.*(c2.*deltaEuQu).^2);
deltaB = zeros(1,size(A,2));
for k = 1:size(A,2)
deltaB(k) = min(exp(u)*deltaEuQu(k)/u,exp(v)*deltaEvQv(k)/v);
deltaB(k) = min(sqrt(((exp(u)*deltaEuQu(k))^2+(exp(v)*
deltaEvQv(k))^2)/(u-v)),deltaB(k));
end

deltaY1 = sqrt((deltaA.*log2((2.*A+2.*B)./(A+2.*B))).^2+(deltaB.*
```

```
((4.*B.*(A+B))./(A+2.*B).^2)).^2)/Nu;

Y1 = Y1-deltaY1;

e= (Eu.*Qu1.*exp(u))./Y1*v;
He=-e.*log2(e)-(1-e).*log2(1-e);

R1 = q*(-Qu1.*fe.*HE+Q1.*((1-He)))-(7*sqrt(N2.*log2(2/epsilonf)).
/N2+2*log2(1/2/(epsilonf)))./N2;
R1 = R1.*N2;
%%%%%%%%%%%%%%

%%%QDot%%%%%%%%%%
p_tag = 0.0001;    %multiphoton probability from Quantum dot
AA = (theta*eff-p_tag)./theta*eff;
N3 = rep1.*theta;
E = (e_detector+e0*(Y0));
Ea = E./AA;
H= -E.*log2(E)-(1-E).*log2(1-E);
Ha = -Ea.*log2(Ea)-(1-Ea).*log2(1-Ea);
Rinf = AA.*q.*(eff*theta.*(1-Ha)-(eff*theta+Y0).*fe*H);
Rsin = Rinf-(7*sqrt(N3.*log2(2/epsilonf))./N3+2*
log2(1/2/(epsilonf)))./N3;
R5 = Rsin.*N3; %secret key length

th = 10000;
%%%%%%plots%%%%%%%%%%
semilogy(x,R1,'r')
hold on;
semilogy(x,R5,'g')
xlabel('Loss(dB)','Interpreter','latex');
ylabel( 'Secret key length per sattellite pass',
'Interpreter','latex');
ylim([1e1,1e8]);
legend('Rdecoy');
end
```

Appendix C

List of publications

C.1 Published papers

-

P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence, Phys. Rev. A 99, 062315 (2019).

P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Eavesdropping and countermeasures for backflash side channel in quantum cryptography, Opt. Express 26, 21020 (2018).

C.2 Papers in preparation

-

P. Chaiwongkhot, A. Huang, J. Zhong, H. Qin, S. Shi, and V. Makarov, Faking photon number on transition-edge sensor

P. Chaiwongkhot, K. B. Kuntz, J.P. Bourgoin, N. Lütkenhaus, V. Makarov, and T. Jennewein1, Generalized spatial-mode detection efficiency mismatch in a free-space QKD system with Zernike polynomials

P. Chaiwongkhot, S. Hosseini, A. Ahmadi, B. Higgins, M. E. Reimer, and T. Jennewein, Quantum dot as a single photon source for satellite-based quantum key distribution

S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, An approach for security evaluation and certification of a complete quantum communication system

C.3 Published papers with minor contribution

-

A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, Phys. Rev. Appl. 12, 064043 (2019).

A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, IEEE J. Quantum Electron. 52, 8000211 (2016).

V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A 94, 030302 (2016).