Detection Efficiency Mismatch and Finite-Key-Size Attacks on Practical Quantum Cryptography Systems

by

Poompong Chaiwongkhot

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics

Waterloo, Ontario, Canada, 2015

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

Security verification for the physical implementation of a cryptography system is an important step to ensure the security level promised by theory. As has been shown many times, any physical device has characteristics and behavior that deviate from theoretical expectations. Frequently, those lead to new security loopholes.

This thesis presents three experimental studies of attacks on quantum key distribution (QKD) systems. The first is the detection efficiency mismatch on free-space systems, which takes advantage of alignment imperfections in Bob's detector to control detection efficiencies. The experiment was done on a polarization-encoding free-space receiver to find the detection efficiencies of each detector for different spatial modes of an incoming photon. Those results were put into an optimization program, which modeled an intercept-and-resend attack on a non-decoy Bennett-Brassard 1984 (BB84) protocol. The result shows that an adversary is able to gain information about the key without being detected by Alice and Bob. The second study is an experimental test of reliability of a spatial filter (a pinhole), which is proposed as a countermeasure for the previous attack. The result shows that, by sending a high-power laser beam focused on the pinhole, the pinhole can be widened without affecting other components in the receiver. Thus, the ability to perform a spatial mode detection efficiency-mismatch attack is recovered. The last experiment is a demonstration of Eve's ability to force a commercial system to distill a key from a raw key of a short length, where the asymptotic assumption of security claimed by the manufacturer might not hold. It was shown that this could be done by inducing transmission loss in the channel at an appropriate time.

Acknowledgements

I would like to thank Vadim Makarov and Norbert Lütkenhaus for their helpful advice and their patience in introducing me to both theoretical and practical aspect of QKD. I would like to thank all present and past members of the quantum hacking lab, especially Shihan Sajeed and Anqi Huang for all constructive debates, discussions, and assistance in my research. Thanks to Thomas Jennewein and Jean-Philippe Bourgoin for their assistance, advice and suggestions on experimental setup.

Thanks to my parents and 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 University of Waterloo Thai Student Assosiation (UW-TSA) members who provided friendly and supportive environment which made my life here be much more than studies and research.

I would like to thanks Vadim Makarov, Norbert Lütkenhaus, and Thomas Jennewein for reading and comments on this final version of thesis writing.

Dedication

For life and my dream..

Table of contents

List of Tables

List of Figures

Related publications and presentations

Journal papers and preprints

- S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Ltkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A 91, 062301 (2015). [1]

- V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagn, T. Jennewein, S. Kaiser, R. Kashyap, M. Legr, C. Minshull, and S. Sajeed, Laser damage creates backdoors in quantum communications, arXiv:1510.03148 [quant-ph] [2]

Conference presentations

- P. Chaiwongkhot, S. Sajeed, J.-P. Bourgoin, T. Jennewein, N. Ltkenhaus, and V. Makarov, Spatial-mode detector efficiency mismatch security loophole in free-space QKD (contributed talk), presented at QCrypt 2015, Tokyo, Japan, September 28 October 2, 2015(manuscript preparation and presentation).

- Lecture "Limits on physical security of quantum communications" given by V. Makarov and A. Huang at several seminars in South Korea and China, October 15 November 2, 2015.

- Talk "The future is quantum" given by V. Makarov at the Norwegian cryptographic seminar in Trondheim, Norway, September 8, 2015

- Talk "Progress and challenges in quantum cryptography" given by V. Makarov at Telecom ParisTech, Paris, France, July 10, 2015

- Talk "Testing quantum crypto" given by V. Makarov at ETSI 2nd quantum-safe crypto workshop, Ottawa, Canada, October 67, 2014

Chapter 1

Introduction

This thesis has been written for two main purposes. First is to be a record of my research over my master degree study. Second purpose is to provide an overview of this field of study and be a guideline for new students who are interested but are not familiar with quantum cryptography especially in practical Quantum Key Distribution (QKD).

The goal of this introduction section is to give an overview on cryptography. We will start by emphasizing the importance and advantages of using encryption in secure communication. Then, we will discuss about the necessity of QKD system. Lastly, we will discuss about the importance of the verification of implementation of QKD.

Chapter 2 will be a review of security analysis of the QKD protocol. The chapter will start with a formal security definition of QKD. Next, we will look at Bennett-Brassard 1984 (BB84) as an example of QKD protocols. The last part will be a discussion on how to justify the security of QKD protocol in practice.

Chapter 3 is about the implementation of QKD. In this chapter, we will discuss about various observations about the behavior of the real-life apparatus that affect the security of the QKD system and how to overcome them.

Chapter 4 contains the experimental process and the results of the verification of practical implementation of QKD both on a free-space system and on a fiber based system.

1.1 Secure communication in everyday life

At first glance secure communication might sound like a topic for specialists that has no direct effect on everyday life. In contrast, there are a lot of our activities that rely

on secure communication: e-mail, ATM machine, online banking, software download and update, etc. To guarantee the security of these activities, there are many considerations to take into account [3]. For example, in software update, the software needs to make sure that the client's PC is getting data from the legitimate server, not a malicious entity or virus distributor [4]. This so called 'authentication' process can be done by exchange and verifying a code called 'signature', prior to the authentication. This signature has a property that it is hard to forge by third party and the user can verify its legitimacy using the algorithm, usually, embedded in the program they want to update. Another example is e-mail or online private messaging [3, 5]. Both sender and receiver need to make sure that no third party can read the message without their permission. The method that widely used nowadays is public key encryption which rely on an assumption that factorization of a large number is hard for those who has limited computational power [6]. A method to avoid that assumption is using another scheme called one-time-pad [7]. In this scheme two parties secretly shared a set of pre-exchanged string or 'secret key' and use that key to encrypt the message. We will see later in this chapter that the encrypted message is secure so long as the third party does not know about the key. The trade-off of this scheme is that the key has to be as long as the message itself and the key cannot be reused.

Though, those keys can be exchanged in secret and store before the encryption, some other communications need to encrypt large amount of data, happen at long distance, or require a higher security level that cannot rely on the 'key storage'. Thus, the requirement of generation and exchange of secret key on demand has emerged. This generation and exchange of secret key between two distant parties is called 'key distribution'. The following sections will be a formal statement of 'security' in the communication, and why security of a secret key is a factor to determine the security of the communication.

1.2 Cryptography and security of cryptosystem

Thinking about cryptography, one might believe that perfect secrecy can be achieved only by keeping the methods and the scheme hidden from the outside world. In contrast, modern cryptography assumes that an adversary –often called eavesdropper or Eve– is familiar with all the device used in the cryptosystem and has full knowledge of the protocol – the processes used to generate and distribute the key. This assumption also known as Kerckhoffs's principle [8]. Eve also knows all the possible messages that might be used. With that in mind, the security of a cryptosystem is defined as follows [1]

[1]The following contents in this section are summarized from [9, 10, 11].

Definition 1.2.1. *Let $\mathcal{M}$ be a set of all possible messages, $\mathcal{C}$ is a set of all possible cryptogram or encrypted messages which might transmitted through the public channel. A cryptosystem is perfectly secure if*

$$p(M) = p(M|C) \quad \forall M \in \mathcal{M} \quad and \quad \forall C \in \mathcal{C} \tag{1.1}$$

where $p(M)$ is a priori probability distribution of message and $p(M|C)$ is a posterio 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 can be achieved with an encryption scheme called one-time pad. [7]

One-time pad is a scheme in which two parties – often called Alice and Bob – encrypt and decrypt the message using a share 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 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 perform bit-wise XOR between message M and key K,

$$C = M \oplus K. \tag{1.2}$$

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

$$M_{Bob} = K \oplus C = K \oplus K \oplus M = M. \tag{1.3}$$

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 the other words, the security of the cryptosystem is as high as the security of the key itself.

An advantage of using key distribution and sending the encrypted message via a public channel over other secret communication methods is that 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 many time as necessary until they are

certain that they got a secure key. The next challenge is, since modern cryptography needs to support long communication, how can Alice and Bob exchange their secret key without meeting each other in person? For that, many schemes and protocols for 'Key Distribution' have been developed.

1.3 Why QKD?

To fulfill the need of key distribution, many schemes have been introduced, many theories and claims have been put to test, many trial-and-error processes have been done. Eventually, criteria of security that are widely accepted have emerged. Classical cryptography assumed that any adversary has limited computation power, the key is secure if the adversary takes longer time, on average, on their calculation to decrypt the key than the lifetime of the cryptogram. An example of key distribution protocol that relies on this assumption is RSA introduced in 1978 [5]. RSA is a key distribution method based on the problem of factorization of a large number. This problem is considered to be a hard problem to solve in mathematics since the calculation steps of the most effective known factorization protocol in classical computer is an exponential function of a number of bits of that large number [6]. This algorithm is widely being used until today.

During the last century, our understanding of quantum phenomena has been rapidly developed. Many applications of this knowledge have also been developed. An application of the knowledge of the quantum world is Quantum Computing, a new paradigm of computing that uses quantum states as register bits (widely called quantum bits or qubits) and quantum operations and measurements to manipulate and read those states in order to simulate the classical computing. A quantum algorithm that challenged and shook the foundation of classical security was introduced in 1994: Peter Shor has introduced an algorithm using qubits and quantum operations to solve the factorization problem [12]. This algorithm can factorize a number with polynomial steps of calculation as compare to the exponential steps achieved by the best classical algorithm. This, when implemented, has a potential to break any RSA code with significantly shorter time than expected.

One of the solutions to the mathematical assumption above is to find a mathematical problem and encryption scheme that is also hard-to-solve with any quantum algorithm. For that the study of post-quantum cryptography was born. Another solution and the main topic of this thesis is, instead of relying on hard-to-solved a mathematical problem; the security criteria should rely on law of physics and mathematical proof, which is almost impossible to defy or break. This is the beginning of Quantum Key Distribution or QKD.

The conceptually motivations, and development of security proof shall be discussed in the next chapter.

1.4 Hacking: verification of practical systems

As we have already seen throughout last decade, many cryptographic schemes experienced many unexpected behaviors of the physical device that cause protocols unable to work as proposed in theory. Worst, some of those behaviors open a loophole or side channel for Eve or hackers to sneak in and take advantage of it. The developers needed to fix their program or developed a new hardware to close those loopholes while hackers continue to seek unknown loopholes in the patched system and so on. This presumably unending loop of attacking and patching, in turn, drove the development of classical communications to the level of security we have today.

Throughout the last decade, the concept and understanding of Quantum phenomena and QKD systems have been rapidly developed. A lot of schemes and protocol have been introduced. Many proof-of-concept experiments have been realized, some developed to be fully functional QKD systems; some evolved even further to the level of being commercialized. As we learned from 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 also tests its resilience against any disturbance of Eve. Some of the systems has already been put to the testing, and patching loop[13, 14, 15, 16, 17, 18, 19, 20]. 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.

We will discuss about these verifications of practical systems–later on they will be called 'Quantum Hacking'– in Chapter 3 and 4. Chapter 3 will be a general discussion about the implementation of QKD and how the behaviors of physical devices affect the security of the system. Chapter 4 is about three experimental security verifications and countermeasures on two QKD systems.

Chapter 2

Review of theoretical aspect of QKD

Advantages of quantum key distribution (QKD) over its classical counterpart are the provable security in mathematics and no-cloning theorem in quantum mechanics that make the information carrier, photon, unable to be duplicated without inducing error. This chapter contains a discussion of theoretical aspect of Quantum Key Distribution.

2.1 Practical BB84

Before we dive into the formal statements and security analysis, let us look at a QKD protocol as an example: Bennett-Brassard 1984 or BB84 protocol. Named after C. Bennett and G. Brassard [21] who introduced this protocol in 1984. This protocol is the first successfully implemented QKD protocol and still being studied and developed until today [21, 22, 23, 24].This protocol use the state of photon as an information carrier. The protocol assumed that Alice and Bob have an authenticated classical channel which is read-only for Eve(i.e. Eve can only read the information transmitted via this channel but cannot interfere or modify the information). They also have a quantum channel which is fully controlled by Eve. Eve has infinite resources and computational power and can do everything that is allowed by laws of physics. The definition of the protocol can be seen in Fig. 2.1.

The security of this protocol rely on the fact that the state of the photon cannot be duplicated with certainty so that Eve cannot have a perfect copy of the states transmitted

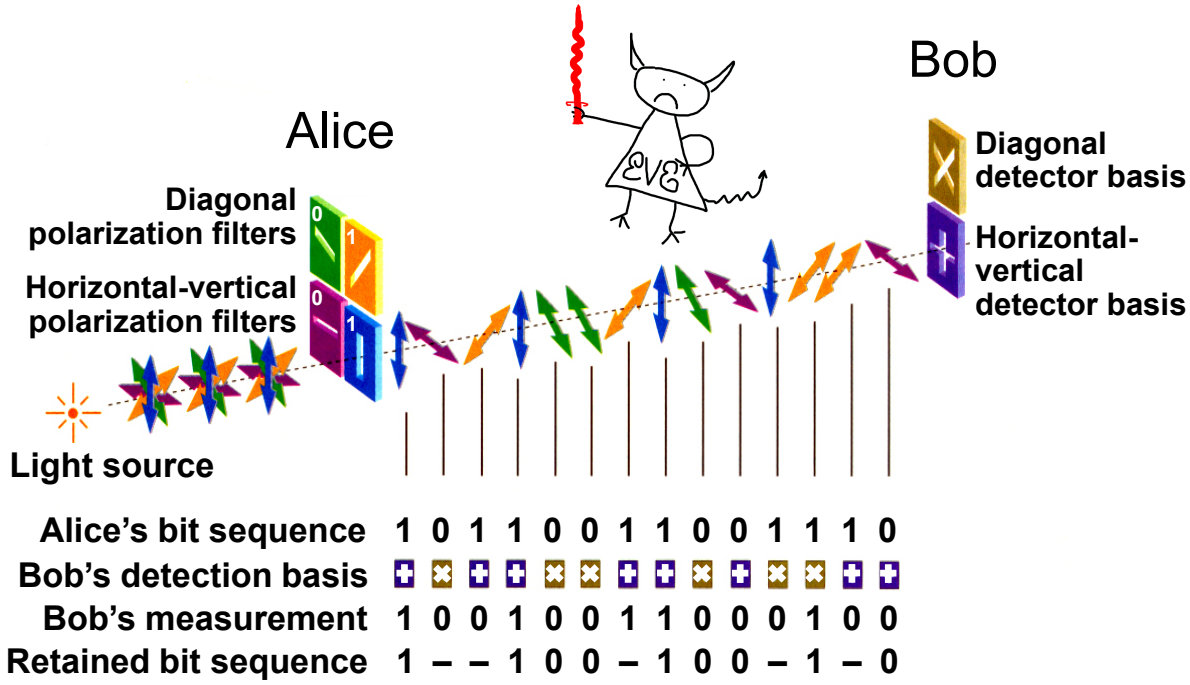

Figure 2.1: BB84 protocol with polarization encoding.(modified from [25])

Step	Process
(Quantum phase) Raw key exchange	Alice prepare series of qubit state $\|0\rangle, \|1\rangle, \|+\rangle = \|0\rangle+\|1\rangle$, or $\|-\rangle = \|0\rangle - \|1\rangle$ where $\|0\rangle, \|1\rangle$ are orthogonal. She records the bit value and sends the state to Bob. For each time slot, Bob locally picks, at random, one of the two basis of measurement, $(0, 1)$ or $(+, -)$, he performs the measurement, record the measurement result and the basis he chose in each bit.
(Classical phase) Sifting	Via a classical authenticated channel, Bob send the index of slots that he detected signal and their corresponding basis of measurement. Alice keeps only the slots in which the basis of measurement match her preparation, and discard the rest. Then, he send the index of those keeping slot to Bob. Bob discard all other slot. After that, both map each remaining slots in to respective binary bit. For example, $\|0\rangle$ and $\|+\rangle$ to bit 0 and $\|1\rangle$ and $\|-\rangle$ to bit 1
Error correction	Alice and Bob execute an error correction algorithm to correct any error in their raw key. If the error rate exceed a certain threshold Q, terminate the protocol. The value of Q can be estimated from the background count rate and extinction ratio of Bob's receiver.
Privacy amplification	Alice and Bob apply a hash function to the bit string. They disclose and compare a portion of the result. They discard the key if the results are difference, otherwise keep the rest of the key string as a secret key [26, 27].

Table 2.1: BB84 protocol

in the quantum channel. In addition, since Eve has no information about the basis of the states that Alice send, if she try to measure the signal, there is a probability that she picks the difference basis of measurement compare and induce error on Bob's detection which can be detected after sifting step. Another feature of this protocol is that if Eve did not gain information about the transmission in the quantum channel while the protocol is running, it is not possible for her to gain information about the key later no matter how much computational power or technology she has, or will have. This 'forward security'[28] is another advantage of QKD protocol over its classical counterpart. That is the scheme and high-level idea of obtaining a secure key via a QKD system of a QKD protocol[1]. In next section, we will discuss about the security statement and mathematical proof of security.

2.2 Security definition of QKD protocol

In general, the success of any key distribution protocol requires three things, correctness, secrecy, and resilience. Correctness requires that the final keys shared by Alice and Bob after the protocol execution are identical. This means that all errors in the key sequence need to be corrected or to be discarded. Secrecy, in information theory, requires that the keys are equally likely and that the knowledge of Eve about the key is the same before and after Alice and Bob execute the protocol. Resilience means that the protocol need to take account of possible interference and tamper from a third party (Eve) and prevent it. In most cases, this means that the protocol has a monitoring mechanism and post-processing to decouple Eve's information from the final key, or allow the process to abort if any disturbance detected.

As can be seen from the example above, quantum key distribution protocols consist of two parts namely, Quantum phase and Classical phase. In the Quantum phase, Alice and Bob produce, transmit, and measure quantum signals via a quantum channel. Classical phase is where Alice and Bob perform the classical post processing (calculation or communication via classical channel) on the result from the Quantum phase in order to generate a secret key. One of the features of any QKD scheme is a process called 'privacy amplification'[22, 31] where Alice and Bob are able to generate a secret key out of a string of partially-secret raw key using a family of functions called 'U_2 hash function' to map the raw key of size n to the new key of size l. These functions have a colliding probability (i.e.the probability to get the same output string out of two different input strings) less than $\frac{1}{l}$. This ability to provably estimate Eve's knowledge is an advantage of QKD system over its classical counterpart.

[1]For more detail, see[29, 30]

In the security analysis of QKD, we assume that Eve takes control of the quantum channel and is able to do everything allowed by the laws of physics in an attempt to gain information on the state shared by Alice and Bob[21, 24, 32, 11]. Furthermore, Eve is familiar with protocol and devices Alice and Bob used. We also assume that Eve has full knowledge about the information communicated via the classical channel.

Now that we get an overview of the goals and the capabilities of QKD, let us begin the security analysis. The following model considers classical-quantum approach where Alice and Bob hold classical bits at the end of the protocol (after privacy amplification), while Eve holds quantum state that might contain information about the final key [9, 32, 11]. Let $|K\rangle$ 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, the state of the overall system as viewed by Eve can be written as,

$$\rho_{ABE} = \sum_{k} \sum_{k'} p(k,k') \left|K\right\rangle \left\langle K\right| \otimes \left|K'\right\rangle \left\langle K'\right| \otimes \rho_E^{(K,K')} \tag{2.1}$$

where $\rho_E^{(K,K')}$ is the quantum state hold by Eve which might contain information about keys. As seen in the previous section, the security of the key require that the key satisfied the i.i.d.criteria and the keys shared by Alice and Bob are identical, so that the joint probability, $p(k,k') = \frac{1}{\mathcal{K}}\delta_{K,K'}$ where δ is the Kronecker delta function. Furthermore, no information about the key should have leaked to Eve. In other words, Eve is factored off or her state is independent of K and K'. So, the ideal overall state at the end of an ideal protocol should satisfy,

$$\rho_{ABE}^{ideal} = \sum_{k} p(k,k') \frac{1}{\mathcal{K}} \left|K\right\rangle \left\langle K\right| \otimes \rho_E \tag{2.2}$$

According to quantum mechanics, this can be accomplished if there exist a system with a channel that can reliably share pairs of maximally entangled qubits, for example, $|00\rangle \pm |11\rangle$. Then the problem turned to be: from their observation, how can Alice and Bob make sure that their channel can send those states untampered? To answer that question, let consider a system that generates a pair of signal encoded in one of four states, $0, 1, +$, and $-$ and sends them to Alice and Bob. This system has a property that the joint probability of Alice and Bob's measurement satisfies table 2.2.

[2] More detail about Dirac notations and density matrix can be seen in [33, 9].

$p(xy)$	0	1	+	-
0	p_{00}	0	p_{0+}	p_{0-}
1	0	p_{11}	p_{1+}	p_{1-}
+	p_{+0}	p_{+1}	p_{++}	0
−	p_{-0}	p_{-1}	0	p_{--}

Table 2.2: Joint probability of detection for an ideal QKD system.p_{ij} represent the probability that Alice detect state i, while Bob detect state j.

From the table, the state $|\psi\rangle$ sharing in this system has to be orthogonal to vectors $|01\rangle, |10\rangle, |+-\rangle$, and,$|-+\rangle$. The only solution for $|\psi\rangle$ is $\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$ which means that this system is able to share an entangle state. In addition, Alice and Bob can monitor the reliability of the system by observing the cross-over detection probability when they measure in the same basis (i.e. detection error).

In practice, the verification of those states is based on measurements and statistics, which might deviate from what was predicted. A more practical security definition is given by R.Renner in [32],

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 inequality*

$$\frac{1}{2} \left\| \rho_{ABE} - \rho_{ABE}^{ideal} \right\| < \epsilon \tag{2.3}$$

holds.

Those density matrices are as defined in equations 2.1 and 2.2. This ϵ is the bound of the probability that the protocol is not aborted but Eve still holds information about the key.

2.3 Key-rate equation

From the security definition, R.Renner[32] also derived that the value of ϵ is bounded by

$$\frac{1}{2} \left\| \rho_{ABE} - \rho_{ABE}^{ideal} \right\| < 2^{-\frac{1}{2}(H_{min}(A|E)-l)} \tag{2.4}$$

where $H_{min}(A|E)$ is the minimal entropy of state A for the states known by E. l is length of the key after privacy amplification. If the two states on the right were infinitely-close, the exponent terms on the left is approach zero. Hence, we have

$$\frac{l}{N} = fracH_{min}(A|E)N \geq S(A|E) - leak_{EC} \tag{2.5}$$

where $S(A|E)$ is the conditional Holevo entropy of each quantum signal share by Alice and Bob as seen by Eve. Note that this therm approaches Shannon entropy, $H(A|E)$, as the signal size $N \to \infty$. $leak_{EC}$ is the information leakage during error correction process. This term is bounded by Shannon entropy between Alice and Bob, $H(A|B)$. As a result a key rate equation for the raw key of size(signal) $N \to \infty$

$$\frac{l}{N} = H(A|E) - H(A|B) \tag{2.6}$$

This is a general structure to calculate the key rate in any QKD protocol.

Now, let us consider BB84 protocol stated in section 2.1. If the channel is not tampered with, the joint probability of Alice and Bob state should satisfy table 2.2, which means that the key they generate from the protocol is secure. To find the key rate for this protocol, let us look at the protocol step-by-step.

- For every raw key exchange, there is a probability $p^{keep} = \frac{1}{2}$ that the key bit is in the same basis of measurement and that it passes the sifting.
- In the error correction step, Alice and Bob need to disclose some of their bits via a classical channel. They need to assume that Eve gains full information about those bits. Let E be the probability of error in the remaining bit. The lower limit of the disclosed bits in this process is the Shannon entropy $h(e)$[7].
- Privacy amplification step: from equation 2.6, by reconstruct the state shared by Alice and Bob out of the joint probability table, [24] derived that the term $H(A|E)$ is bounded by $(1 - h(e))$.

With all bullets above together, we can write a key rate equation for an ideal BB84 protocol, with raw key size $n \to \infty$, as a function of observed error rate.

$$\frac{l}{n} = \frac{1}{2}(1 - 2h(e)) \tag{2.7}$$

This example was set for the reader to get an overview of the security analysis of QKD system. In order to get a practical key rate, there are many factors that have to be included in the analysis and this key rate equation will be modified as a result. We will discuss about these factors and their effect as we look at the implementation of QKD in the next chapter.

Chapter 3

Implementation of QKD

As one looks back through the history of cryptography, one might find that one of the most challenging parts of any cryptosystem is its implementation. Some requirements of the criteria might be convenient for analysis and calculation but might be hard or impossible to achieve with the technology at that time. Some unexpected phenomena or unpredictable behavior of the devices might hinder the communication, or worst, leak the information to the third party.

This chapter is an overview of the implementation of QKD. This chapter will begin with an example of physical QKD system that was designed for the BB84 protocol shown in the previous chapter. These systems will be use as study subject in security verification of QKD in the next chapter. Second half of this chapter is about the difficulties in building a QKD system with current technology. This will be an overview about un-predicted phenomena in the physical system that affect the QKD security and how we adapt the scheme or include them into the theoretical analysis to overcome those effects.

3.1 Practical QKD systems

This section is about a physical scheme of practical QKD system. Different scheme has different way of encode and transmit the photon in the quantum phase and different way of perform post-processing in classical phase. The following is two examples of QKD systems that designed for BB84 protocol. Each has its own advantages and limitations. These two systems will be mentioned again when we discuss the security of the system in the next chapter.

3.1.1 Polarization encoding free-space QKD system

Free-space QKD is a type of systems that transmits information carriers, photons, through free space or air. The advantage of this channel is that air, in a clear weather, has low loss per km, which means that information can be exchanged over a long distance. The example is the experiment in 2012 [34] which demonstrated quantum teleportation over 143km Furthermore, free-space QKD is the only type, with current technology, that enables a satellite-based system, which allows the global-scale QKD network. In contrast, a drawback of this system is the fluctuation of the atmosphere, which is a result of clouds, dust particle or air pollution, and can hinder or prevent the communication. Another drawback is the fact that front-end of the receiver has to be exposed to free space. As a result, this system suffers from higher noise from the environment. The following is a model of a free-space system using polarization encoding. This is also a model for satellite QKD project [35].

Alice's device consists of a laser as a photon source. In each time slot, a light pulse passes through a polarization modulator(PM) which randomly encodes the polarization of the photon into horizontal(H), vertical(V), $+45°$ (D), and $-45°$ (A) [36, 37, 37, 38, 39, 40, 41, 42]. Then, the beam passes through an attenuator(VOA) which decreases the mean photon number of each pulse below one before sending it to Bob. The intensity modulator(IM) is used to compensate the fluctuation of the laser source. It also used to generate decoy signals in decoy-stare QKD scheme. The polarization controller is used to compensate polarization shift in the fiber and optics components.

At Bob's side, the receiver consists of a beamsplitter(BS) which acts as a passive basis selection. In each arm of BS is a polarizing beamsplitter(PBS) which, in one arm, is aligned to match the HV basis on Alice and in the other arm is aligned to match DA basis. Finally, a detector is attached to each arm of the PBS to detect the photon. Alice and Bob can use this system for the BB84 protocol mention in previous section by mapping the HV basis onto 0 and 1 and DA basis to $+$ and $-$ (See fig.3.1).

3.1.2 Phase encoding fiber-based QKD system

As the name suggested, fiber-based system is a system that transmits signal via fiber optics. That makes this type of system relatively easier for alignment and maintenance in comparison to the free-space counterpart. The drawback of this system is the loss in fiber optics, which limits the distance of communication. Nevertheless, fiber optics is a choice for many commercial systems. The following is the scheme for a phase encoding system called plug-and-play QKD system by IDQuantique.[43, 44]

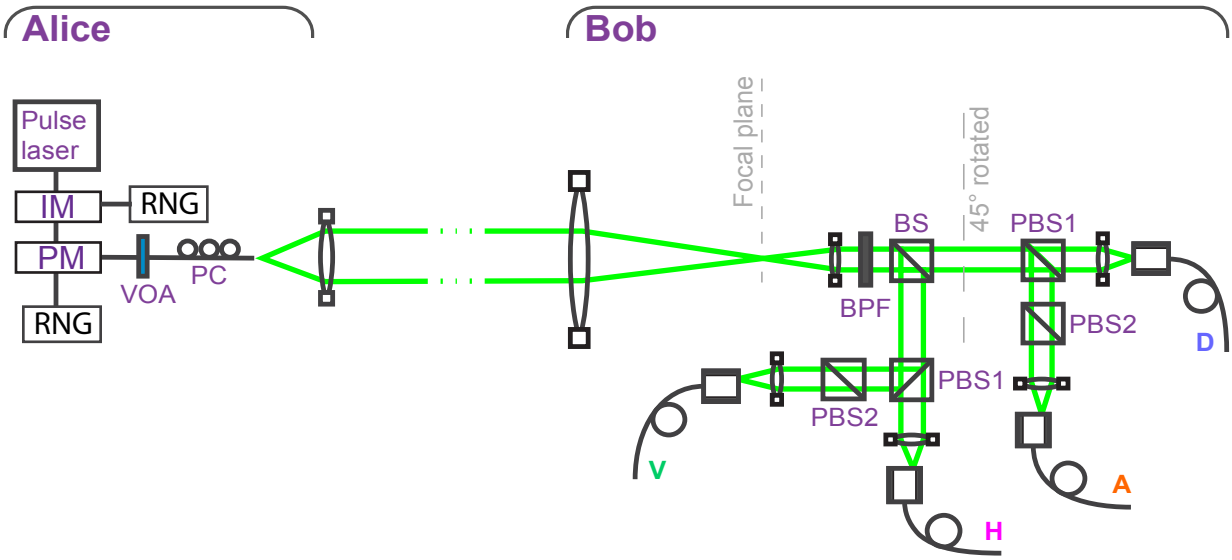

Figure 3.1: Polarization encoding free-space BB84 system (reprinted from [1]).

The scheme of the system is in 3.2. The following description is collected from [43, 44, 13] Pulses originate in Bob's laser at a fixed rate. They pass through an unbalanced Mach-Zehnder interferometer (MZI) where one arm is intentionally made longer than the other arm. The longer arm has a polarization rotator to rotate the polarization by 90 °. It also has a phase modulator that acts as a measurement basis for Bob. The phase modulator is off during the first pass when the light is travelling from Bob to Alice. The two pulses from two arms gets combined by the polarization beam splitter and goes out into the quantum channel. For each pulse generated by Bob's laser, there are two orthogonally polarized pulses in the optical link going towards Alice with a fixed delay between them corresponding to the difference in the arm length of the MZI. The first pulse is called the reference pulse while the second pulse is called the signal pulse. The signal pulse has lower energy than the reference pulse because it goes through the longer arm consisting of the phase modulator and suffers additional loss.

Alice's attenuator VOA1 attenuates the signal, her phase modulator (PM) applies a random phase ϕ_A $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$, and the Faraday mirror (FM) reflects and rotates the polarization orthogonally for both pulses. The two pulses arrive at Bob and take the opposite arms of the MZI than the ones they took before. The PM in the long arm is now 'on' and

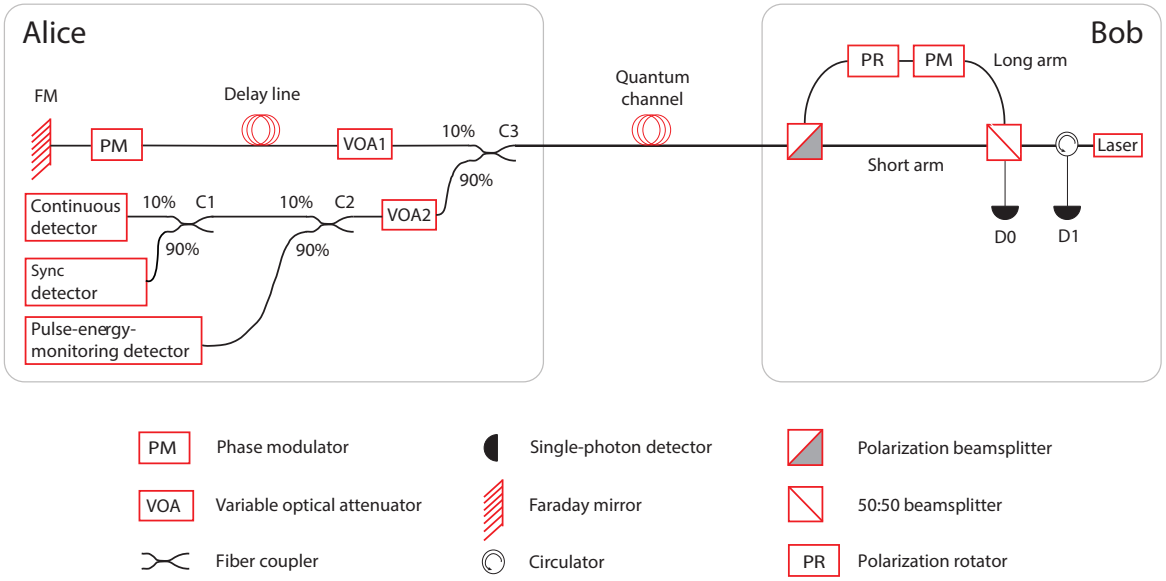

Figure 3.2: Plug-and-play system. Reprinted from [13]

applies a random phase ϕ_B (either 0 *or* $\frac{\pi}{2}$). As a result of the combination of the FM and the unbalanced MZI, the two pulses have the same polarization and path difference, and arrive at Bob's 50:50 beamsplitter (BS) at the same time. Hence, the choice of the output BS path depends only on their relative phase difference ($\phi = \phi_A - \phi_B$). Two detectors D_0, D_1 and a circulator are used in the configuration shown in the Fig. 3.2 to collect the light after the BS. If $\phi = 0$ ($\phi = \pi$), the pulses emerge at the same (different) path from which they came, and are collected by D_1 (D_0). This is a measurement in the compatible basis. However, if Alice and Bob choose different bases (such that $\phi = \frac{\pi}{2}$ or $\frac{3\pi}{2}$), then the photons are split with equal probability between D_0 and D_1.

3.2 Difficulties in implementation of QKD and possible solutions

This section is about difficulties of taking the idea and concept in the paper and implement it in reality. Those difficulties might be because of lack of technology, or an unexpected behavior of the devices which was not included in security analysis. In this section, we will look at the problems and its effects, then discuss about the possible solution for that problem.

	Mean photon number			
photon number	0.1	0.3	0.5	1
0	0.904	0.740	0.606	0.367
1	0.090	0.222	0.303	0.367
2	0.004	0.033	0.075	0.183
3	0.0001	0.003	0.012	0.061

Table 3.1: Probability distribution of photon-per-pulse for different mean photon number.

3.2.1 Single photon source versus weak coherent source

One of the major problem in the implementation of QKD is the reliably single photon source is still under developed. A photon source that behave closest to the single photon source is the attenuated pulse laser or weak coherence source.

By the fact that the distribution of photon number, $p(N, \mu)$, in each laser pulse is governed by Poisson distribution,

$$p(N, \mu) = \frac{\mu^N \exp^{-\mu}}{N!} \tag{3.1}$$

where μ is mean photon number, N is the number of photon in each pulse. Since the mean photon number of the laser is proportioned to the laser's power, μ can be controlled by the power that drives laser and attenuator or density filter. If the source was set such that $\mu < 1$ majority of the non-empty pulses are single photon. See table 3.2.1.

Though most of the pulses are single photon, Eve, who is limited only by law of physics still be able to take advantage of. She can perform, so call, Photon Number Splitting(PNS) attack [45, 27, 46, 24], see Table 3.2.1.

It can be seen that 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 analysed in the previous chapter.

To handle this attack, Alice and Bob need to look back at their protocol and key rate equation. From the attack scheme, they need to assume the worst case where Eve gains full information about every multi-photon pulse sent by Alice. By characterize the source, they know the probability of getting multi-photon pulse, P_{multi}. Furthermore, they can estimate the detection rate, P_{det} of the signal by characterize Bob's receiver and the channel

Step	Process
(Quantum phase) Raw key exchange	Eve replaces Alice and Bob's channel with a lossless channel. Then, she determines the photon number in each incoming pulse from Alice using quantum non demolition 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 pulse, she takes advantage of her lossless channel by blocking some of the pulse to maintain total detection rate of Bob. If the rate of single photon cannot keep up with original Alice and Bob's line loss, she blocks some multi-photon pulse, in addition.
(Classical phase) Sifting	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.

Table 3.2: Photon number splitting (PNS) attack.

condition without Eve present. From that, Alice and Bob can rule out portion of their key that Eve might know. Further more, Alice and Bob need to assume the worst-case scenario where the bits that Eve gained information of were detected by Bob, passed all post processing, and be part of the final key. As a result, they need to take this into their privacy amplification part in their key rate equation. Let $A = (P_{det} - P_{multi})/P_{det}$ [24, 11] The modified key rate equation is

$$\frac{l}{n} = \frac{A}{2}(1 - H(\frac{E}{A}) - leak_{EC}) \tag{3.2}$$

where $leak_{EC}$ is the portion of information that Alice and Bob disclosed in error correction step. It can be seen from this equation that, by characterizing their devices and find the value of A, Alice and Bob can generate key using a weak coherent source.

3.2.2 Multiple click and squashing model

Many QKD system employ multiple detectors in the receiver to detect signal in each basis or each encoded state. In each time slot these systems have a chance to have multiple detection or 'click' across multiple detector. This might occurred by darkcount in the detector, or detection of a multi-photon pulse in wrong basis, or Eve's interference. While this cause problem in the key mapping process, this double clicks cannot be simply neglected or discarded by the protocol. The reason is that, if the protocol discarded every double click; Eve can perform intercept-and-resend attack as seen in previous chapter with some modification. Instead of sending single photon pulse with the same state as her measurement result, bright pulse can be sent. This pulse will cause single click only when their polarization match Bob's basis. Otherwise, it will course double clicks and is rejected. As seen before that the error causes by intercept and resend attack happened because of basis mismatch between Eve and Bob, this attack of Eve will never cause an error, and such gone undetected.

One of the solutions called 'squashing model' was introduced in [47]. This model stated that double-click in one basis is mapped to a random value in that basis, while multiple clicks in different bases are discarded, see fig3.3.

3.2.3 Statistical deviation and finite key size effect

With limited detection and transmission efficiency, computational power, and most importantly time, only finite amount of raw key can be exchanged during the quantum phase.

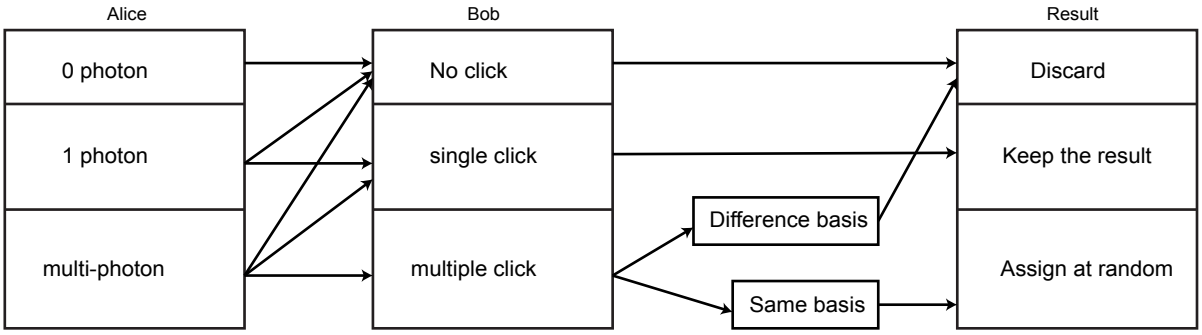

Figure 3.3: Squashing model for BB84 system.(reprinted from [13])

As a result, there are some statistical deviation and failure probability that needed to be considered. For example, the error rate estimated in the parameter estimation process might not represent the error rate of the key. Furthermore, error correction algorithm has a probability that not all the error be detected and corrected. In addition, even though the observed error rate was zero, that does not mean that Eve did not perform an attack. For example, BB84 system with n raw key exchange has a chance of 0.75^n that an intercept-and-resend gone unnoticed. Many literature studied these effects and provided correction terms for the key rate equation to take account on these effects [32, 48, 49]. The key rate equation for finite key size effect can be written as

$$l \leq nA(1 - H(\frac{E}{A}) - leak_{EC}) - \frac{1}{2}\sqrt{(\frac{\ln(1/\epsilon_{PE})\ln(n+1)^2)}{n} - 7\sqrt{\frac{1}{n}log(\frac{2}{\epsilon'})}) - 2log\frac{1}{\epsilon_{PA}} - log\frac{2}{\epsilon_{EC}}} \tag{3.3}$$

where the first correction term is the result of statistical deviation in parameter estimation step where ϵ_{PE} is the probability that the key has more errors than what was estimated in parameter estimation step. The second took account account of statistical approximation in privacy amplification step, where ϵ' is the probability of failure. The third term is for the probability, ϵ_{PA}, that the hatch function transforms two different key sequence into the same final key. The last term takes account of failure probability, ϵ_{EC}, of error correction where there is non-zero error bit left after the correction.[32, 48, 49]

The key generated by a protocol which is not aborted under this analysis satisfies ϵ-security [32] defined in section 2.1. The value of ϵ is a summation of all security parameters, ϵs, in each correction term. It can be seen that all ϵs are free variables. Which means that

ϵ can be set as small as necessary to maintain the level of security Alice and Bob require. The consequence is smaller ϵ lower the secret key rate. [32, 48, 49]

According to R. Renner, the security parameter, ϵ, can be picked to be the same order as major natural disasters such as serious earthquake, volcanic eruption or nuclear power plant meltdown. If such disaster happened, it is most likely that the security of the key would not matter anymore. For example, the probability of a nuclear power plant meltdown is 10^{-4} per year, according to the Nuclear Regulatory Commission. If QKD machine generates two keys every minute or approximately a few million keys a year, one might pick $\epsilon = 10^{-10}$ so that the probability that at least one key leak to Eve is the same order as such disasters. [32]

3.2.4 Real device versus theoretical expectation

One of the most challenges of QKD implementation is to make the device works exactly as stated in the protocol. Otherwise, it might open a side channel for Eve to take advantage of. For example, if the mechanics that produce V-polarization in BB84 system cause time delay on that bit compare to other polarizations, Eve can monitor that time delay and gain some information about the key [50]. This is also true for other variables. Another example is the fake-state attack [19, 51] where Eve takes advantage of Bob detectors' imperfection to control the detection result.

Not only works as the protocol stated, the QKD system also needs to be secured against any tampering by Eve. An example of this is the Trojan horse attack [52] where Eve sends some extra bright pulse and measures the reflection to the system to monitor the state of components inside and learn about the measurement. Another example is blinding attack [17] which Eve sends some bright pulse to cause the avalanche photo diode in the receiver not response to single photon pulse.

Most of these imperfections and vulnerability are not discovered until the system was implemented and put to the test. These vulnerabilities needed to be investigated in scheme-by-scheme basis. Then, countermeasures can be implemented whether by modify the scheme or theoretical analysis. After that, the system with the countermeasure has to be tested again. This is because the countermeasure might not work as expected, or worse, it might open a new loophole for other attacks. This loop of testing and patching shall be seen in the chapter three when we discuss about Quantum Hacking in detail.

Chapter 4

Attacks on QKD systems

The study of its physical implementation reveled a number of vulnerability of QKD [1, 14, 15, 16, 53, 50, 18, 19, 20]. The main reason behind this is the deviation of the actual behavior of the devices from the ideal expected behaviour. Thus, to guarantee the security, it is of utmost importance to scrutinize the practical device behaviors for possible deviations.

4.1 Attack on free-space QKD system

In this section, we will show experimentally that by modifying spatial mode of light can affect Bob's detection efficiency. In first experiment, we investigated an attack called fake state attack [51, 54] on a BB84 system. This attack is a modification of the intercept-and-resend attack where Eve intercept photons from Alice and generate new photons corresponding to her measurement result. These photons are sent to Bob in such a way that they cannot be detected if Bob picks a basis of measurement different from Eve. Hence, Eve gains information about the key without inducing error, see fig. 4.1. Recently, many variants of fake state attack have been studied [51, 54, 55, 56, 18, 50, 57]. This experiment investigated a fake state attack where the beam from Eve is sent at an angle such that the beam focuses only on the intended detector with the same polarization as Eve's measurement result while the beam misses other detectors, see fig. 4.2.

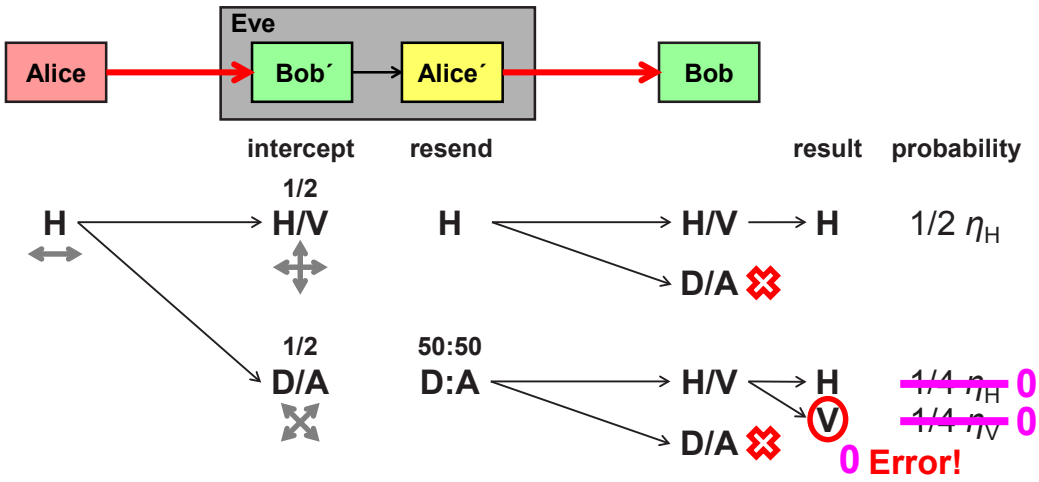

Figure 4.1: Fake state attack on BB84 protocol. The scenario that cause error in an intercept-and-resend attack on a BB84 system is when Alice and Bob pick the same basis of measurement but Eve picks the other. If Eve sends her photon to Bob in such a way that the detection efficiency in the different basis of Bob is zero, she can perform an intercept-and-resend attack without being noticed.

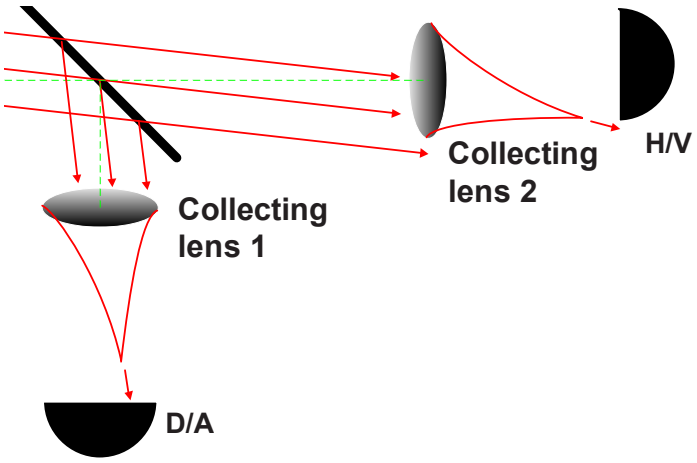

Figure 4.2: An illustration of spatial-mode detection efficiency mismatch. The beam from Eve (red line) is sent to Bob in an angle diverging from the normal setup by Alice and Bob(green line). This angle is picked such that the beam path hit the collecting lens 1 and being detected in the D/A basis, but misses the H/V detector. Thus, this angle can be used to send D/A fake state to Bob without inducing error(modified from [55]).

4.1.1 System under test

We tested a free-space receiver which is a model for a satellite QKD project [35]. This receiver employs a telescope to reduce the size of the collimated beam. It operating at 532 nm wavelength. Its telescope consists of a focusing lens L1 (diameter 50 mm, focal length $f = 250$ mm; Thorlabs AC508-250-A) and a collimating lens L2 ($f = 11$ mm; Thorlabs A397TM-A). The collimated beam of $\lesssim 2$ mm diameter then passes through a 50:50 beamsplitter BS (custom pentaprism [35]) and a pair of polarizing beamsplitters PBS1 and PBS2 (Thorlabs PBS121). PBS2 increases the polarization extinction ratio in the reflected arm of PBS1. Lenses L3 (Thorlabs PAF-X-18-PC-A) focus the four beams into 105 µm core diameter multimode fibers (Thorlabs M43L01) leading to single-photon detectors (Excelitas SPCM-AQRH-12-FC).

4.1.2 Spatial mode detection efficiency mismatch

Motivation

One of the assumptions on the security proof of QKD is the symmetry of detection efficiency among all received quantum states in Bob's detector [19, 56, 18, 50, 57]. If a deviation from this assumption exists, an adversary Eve can send light to Bob in different spatial modes so that one of his detectors has a relatively higher probability of click than the other detector(s) [55]. In this way, she can exploit the mismatch in efficiency and make Bob's measurement outcome dependent on his measurement basis and correlated to Eve, which breaks the assumptions of typical security proofs. In this work, we investigate how crucial this can be to the security of QKD.

My contribution to this experiment is as followeds:
Experiments, data acquisition and post processing
- Programmed scanning and data acquisition, See Appendix A.1
- Find the sources of mismatch in the optical scheme
- Together with Sajeed: finished experiment design for the first experiment, assembled and performed experiments, analyzed data
Attack model
- Independently analyzed and modeled an attack using a photon number state emitter at Eve., See Appendix A.2
Paper publication
- Wrote the first draft of experimental setup and method. - Refined mathematical description in security analysis part. -Scheme and figure drawing

Method

In order to exploit the mismatch in efficiency, Eve needs to know the mismatch for the four detectors as a function of the input angle. Hence, our first step was to scan Bob's receiver for a possible efficiency mismatch. Eve's source [Fig. 4.3(a)] consists of a 532 nm laser coupled into single-mode fiber, attenuator A, polarization controller PC, and a collimating lens L4 (Thorlabs C220TME-A) mounted on a two-axis motorised translation stage (Thorlabs MAX343/M). In Fig. 4.3(a), green (light gray) marginal rays denote the initial alignment from Eve, replicating the alignment from Alice to Bob. This is the initial position of the translation stage $\phi = \theta = 0$. As we moved the stage in the transverse plane, it changed the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously.

This is shown by red (dark gray) marginal rays in Fig. 4.3(a), representing a beam from Eve coming at an angle (ϕ, θ) relative to the initial beam.

Before scanning, the optics in Bob's apparatus was aligned to maximize coupling into all four detectors at the normal incidence, which is the standard alignment procedure for QKD. Note that many free-space QKD systems employ a real-time tracking system to maintain this initial alignment [58, 38, 39, 42]. We then started the scanning procedure that involved first, changing the outgoing beam's angle (ϕ, θ), and then recording the corresponding count rate at all four detectors of Bob. For each data point, we used an integration time of 1 s. Our scan consisted of approximately 100×100 data points in a square matrix covering the whole clear aperture of Bob's front lens L1. Then during post-processing, for each data point for each detector, we subtracted the corresponding detector's background count rate, and then normalized it by dividing by the maximum count rate in that detector.

At first, we did a preliminary scan using optical power meters (Thorlabs PM200 with S130C head) that revealed several features, highlighted in Fig. 4.3(b). Around $\phi = \theta = 0$, maximum light coupling resulted in the central peak ❶. With increasing scanning angle, the focused beam started missing the fiber core, and the detector count dropped off ❷. A region was found when the beam reflected off a polished edge of PBS2 back into the fiber core, causing the peak ❸. Increasing the angle further made the beam hit the anodized aluminum mount of L1 and possibly edges of other lens mounts and round elements in the optical assembly. It was scattered at these edges, producing two ring-like features ❹. Beyond these features, there were no noticeable power reading, as the beam completely missed the receiver aperture.

We then adjusted the receiver setup to minimize the peak ❸, and performed final scans at 26.1 m distance using Bob's single-photon detectors (Excelitas SPCM-AQRH-12-FC). During these scans, the beam at L1 was Gaussian-shaped with 9 mm width (at $1/e^2$ peak intensity). The scans were done in 38.3 μrad steps covering ±1.84 mrad range, corresponding to lateral displacement of ±48 mm at L1.

Experimental result

Figure 4.4 shows the normalized detection efficiency in all four receiver channels as a function of (ϕ, θ). Most of the original features are still visible. However, outside the narrow

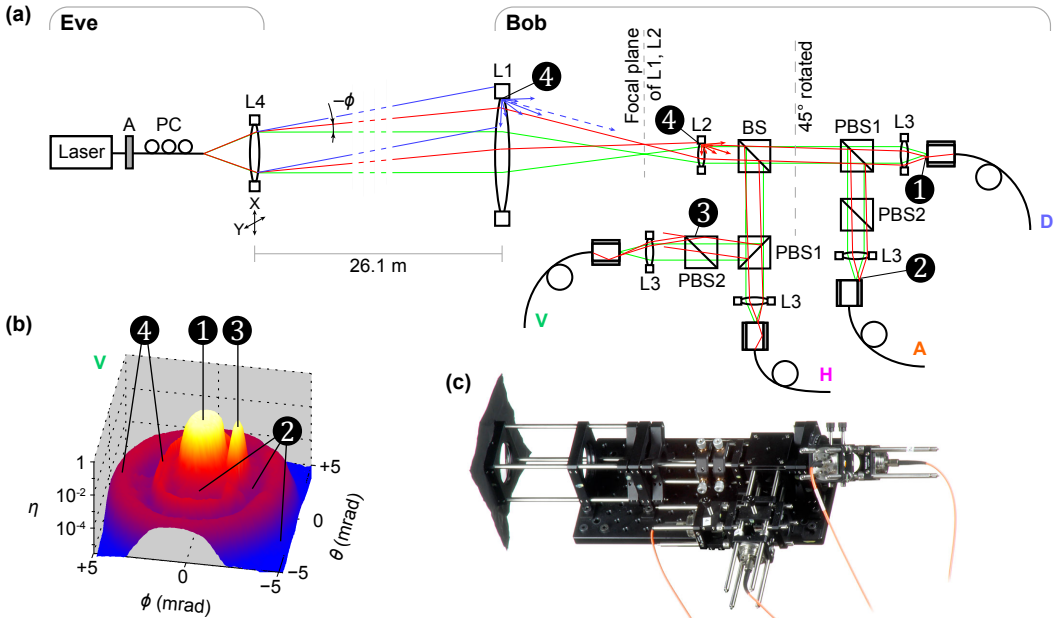

Figure 4.3: Experimental setup. (a) Scheme of the experimental apparatus, top view (drawing not to scale). Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens mounted on a two-axis motorised translation stage. The latter allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. Green (light gray) marginal rays parallel to the optical axis denote the original alignment of Alice's beam to Bob. Red and blue (dark gray) marginal rays show a scanning beam from Eve tilted at an angle (ϕ, θ) relative to the original beam. Features ❶–❹ mark different transmission paths for light inside Bob. (b) Normalized detection efficiency η in channel V versus the illumination angle (ϕ, θ). This scan was taken to show the features clearly by placing Eve at a closer distance. (c) Photograph of Bob's receiver. The actual distance between facing surfaces of L2–BS is 42 mm, BS–PBS1 66 mm, PBS1–L3 31 mm, PBS1–PBS2 45 mm, PBS2–L3 10 mm in channel A and 5 mm in channel V.

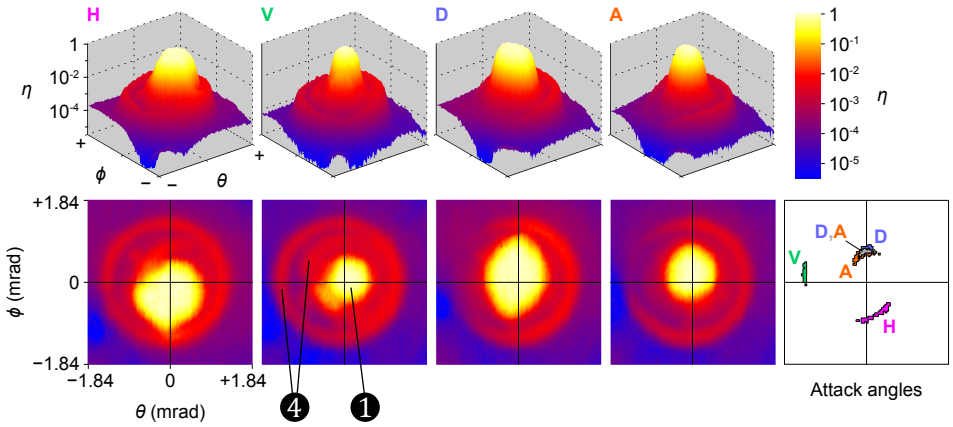

Figure 4.4: Angular efficiency scan of the receiver, and points of interest. Four pair of plots **H, V, D, A** shown in both 3D and 2D represent normalized detection efficiency in the four receiver channels versus illuminating beam angle (ϕ, θ). The angle $\phi = \theta = 0$ is the initial angle of QKD operation. The last plot shows angle ranges with a high mismatch, usable in our attack.

central range of angles close to $\phi = \theta = 0$, individual channel's efficiencies vary independently. Also, the size and shape of the central peak is significantly different between channels. This was impossible to identify during the normal alignment procedure. This effect can be attributed to imprecise focusing, optical path length difference between the arms, off-centered alignment of lenses, mode-dependent bending loss in fibers, and individual variations in components. These may have also caused the efficiency at one side of the outer ring being higher. Because of these reasons, there exist angles such that if photons are sent at those angles, one channel has a much higher click probability than the rest.

Effect on the security of the QKD system

To emphasize the security threat, it is useful to model an attack that exploits the discovered side-channel. One possible attack is the faked-state attack [19, 51], which is an intercept-and-resend attack in which Eve attempts to deterministically control Bob's basis choice and detection outcome. We model a practical faked-state attack using the obtained data and the following assumptions: Alice and Bob perform non-decoy-state Bennett-Brassard 1984 (BB84) protocol using polarization encoding. Alice emits weak coherent pulses with mean photon number μ equal to Alice–Bob line transmittance [46]. Whenever Bob registers a multiple click, he performs a squashing operation [47, 59, 60]. Alice and Bob also

monitor total sifted key rate, and quantum bit error ratio (QBER). Eve has information about Bob's receiver characteristics described above, and only uses devices available in today's technology. She intercepts photons at the output of Alice, using an active basis choice and superconducting nanowire detectors, with overall detection efficiency $\eta_e = 0.85$ and dark count probability $< 10^{-9}$ per bit slot [61]. Then, a part of her, situated close to Bob, regenerates the measured signal and sends to Bob. We assume that Alice–Bob and Alice–Eve fidelity $F = 0.9831$ [35], while Eve–Bob experimentally measured $F = 0.9904$. Here fidelity refers to the probability that a polarized photon will emerge from the PBS at the correct path, which is related to visibility by $F = (1 + \text{visibility})/2$. We also confirmed experimentally that Eve–Bob fidelity is preserved at all illumination angles shown in Fig. 4.4.

From Eve's point of view, she wants to maximize the detection probability when Bob measures in compatible (i.e., same as her) basis, to maximize Eve–Bob mutual information. Also, she wants to minimize Bob's detection probability in non-compatible basis, to minimize QBER. Let $\eta_i(j)$ be the efficiency of Bob's i-th channel ($i \in \{h, v, d, a\}$) given that incoming light is $j \in \{H, V, D, A\}$ polarized. Thus to find attack points for the j-th polarization, we choose angles that have higher values of $\eta_j(j)$ and $\delta_j(j) = \min\left\{\frac{\eta_j(j)}{\eta_{nc0}(j)}, \frac{\eta_j(j)}{\eta_{nc1}(j)}\right\}$, where η_{nc0} and η_{nc1} are the normalized efficiencies of the two detectors in the non-compatible basis. Our experimental attack angles are shown in the rightmost plot in Fig. 4.4. For example, the H attack angles were composed of points for which $\eta_h(H) \geq 0.2$ and $\delta_h(H) \geq 75$. Similarly, for the V, D and A attack angles, $\eta_v(V) \geq 0.002$, $\delta_V \geq 8$; $\eta_d(D) \geq 0.4$, $\delta_D \geq 80$; $\eta_a(A) \geq 0.1$, $\delta_A \geq 20$. The thresholds used here to find the attack angles were not optimal, and were picked manually.

To derive the key rate and QBER formula in Eve's presence, we start with a system with only Eve and Bob. Without loss of generality, consider Eve sending an H-polarized pulse to Bob within the attack angles H. Let's consider a pulse of photon number n arrive at Bob. The probability $p_i(j)^n$ that detector i in Bob clicks given Eve has sent j-polarized

light given n-photon arrival is

$$
\begin{aligned}
p_h^n(H) &= c_h + \sum_{r=1}^{n-1} \left(\frac{1}{2}\right)^n \binom{n}{r} (1-(1-\eta_h)^r)(1-\eta_a/2-\eta_d/2)^{n-r}, \\
p_v^n(H) &= c_v + \sum_{r=1}^{n-1} \left(\frac{1}{2}\right)^n \binom{n}{r} (1-\eta_h)^r(1-\eta_a/2-\eta_d/2)^{n-r}, \\
p_{d(a)}^n(H) &= c_{d(a)} + \sum_{r=1}^{n-1} \left(\frac{1}{2}\right)^n \binom{n}{r} (1-\eta_h)^r \sum_{r=1}^{n-1} \binom{r}{m} (1-(1-\eta_d(a))^m) \\
&\quad \left(\left(\frac{1}{2}\right) (1-(1-\eta_a(d))^{r-m}) + (1-\eta_a(d))^{r-m} \right)
\end{aligned}
\tag{4.1}
$$

By symmetry, the detection rate of all other detectors follow the same form. This equation includes the effect of the squashing scheme and absorbes all internal loss inside the receiver into the detection probability in each detector. The total probability of clicking in each one detector for incoming H-polarization given an arbitrary photon number distribution $f(n)$ is

$$
p_h(H) = \sum_{n=1}^{\infty} (f(n)(p_h^n(H) + p_h^n(V) + p_h^n(D) + p_h^n(A))) \tag{4.2}
$$

where c_i is Bob's background click probability per bit slot in i-th channel. Again, the detection rate of all other detectors follow the same form.

To further emphasize the effect of this attack, we consider a realistic Eve who employs only tools available by current technology. In this analysis we assume that Eve's photon source is a weak coherent source that produces pulses with photon number distribution following the Poisson distribution. By the nature of the detection, which registers only 'click' and 'no click', the detection probability in Bob's detection rate in each detector can be simplified as follows. Before squashing, the raw click probability $p_i(j)$ that detector i in Bob clicks given Eve has sent j-polarized light is

$$
\begin{aligned}
p_h(H) &\approx c_h + 1 - \exp\left(-\frac{\mu_H F \eta_h(H)}{2}\right), \\
p_v(H) &\approx c_v + 1 - \exp\left(-\frac{\mu_H (1-F) \eta_v(H)}{2}\right), \\
p_{d(a)}(H) &\approx c_{d(a)} + 1 - \exp\left(-\frac{\mu_H \eta_{d(a)}(H)}{4}\right),
\end{aligned}
\tag{4.3}
$$

where μ_H is Eve's mean photon number. The probability $P_{hv}(H)$ that after squashing Bob measures in HV basis, given Eve has sent an H-polarized pulse, is composed of three events: when only detector H clicks, when only detector V clicks, or when both click. It can be written as

$$\begin{aligned} P_{hv}(H) = &\big[1 - p_d(H)\big]\big[1 - p_a(H)\big] \\ &\times \big[p_h(H) + p_v(H) - p_h(H)p_v(H)\big]. \end{aligned} \tag{4.4}$$

Let's now include Alice into the picture. Consider Alice sends an H-polarized pulse, and Eve intercepts it. Let $P_c^e \approx \frac{1}{2}(1-e^{-\mu F \eta_e})e^{-\mu(1-F)\eta_e}$ and $P_w^e \approx \frac{1}{2}e^{-\mu F\eta_e}(1-e^{-\mu(1-F)\eta_e})$ be the probability that Eve measures in the compatible basis (i.e., the same basis as Alice) and gets a click only in the correct and wrong detector respectively. Let $P_{nc}^e \approx \frac{1}{2}(1-e^{-\frac{\mu\eta_e}{2}})e^{-\frac{\mu\eta_e}{2}}$ be the probability that she measures in the non-compatible basis (different basis than Alice's) and gets a click in a single detector. The sifted key rate given Alice has sent H-polarized light is

$$\begin{aligned} R_e(H) \approx &P_c^e P_{hv}(H) + P_w^e P_{hv}(V) + P_{nc}^e \left[P_{hv}(D) + P_{hv}(A)\right] \\ &+ (1 - P_c^e - P_w^e - 2P_{nc}^e)(c_h + c_v - c_h c_v). \end{aligned} \tag{4.5}$$

An error can occur when Eve measures Alice's signal in non-compatible basis or when Eve measures in compatible basis but Bob measures a wrong value owing to imperfect fidelity or dark count. Hence, the error rate conditioned on Alice sending H-polarized light is

$$\begin{aligned} E_H \approx &P_c^e P_v(H) + P_w^e P_v(V) + P_{nc}^e \left[P_v(D) + P_v(A)\right] \\ &+ (1 - P_c^e - P_w^e - 2P_{nc}^e)(c_v - \frac{c_v c_h}{2}), \end{aligned} \tag{4.6}$$

where $P_i(j)$ is the probability that Bob measures value i after squashing, given Eve has sent j-polarized light. For example,

$$P_v(H) = \big[p_v(H) - \frac{p_h(H)p_v(H)}{2}\big]\big[1 - p_d(H)\big]\big[1 - p_a(H)\big]. \tag{4.7}$$

Sifted key rates and errors in Eve's presence [Eqs. (4.5) and (4.6)] conditioned on V, D, A polarizations sent by Alice can be calculated similarly. The total sifted key rate and QBER in Eve's presence become

$$\begin{aligned} R_e &= \frac{1}{4}\sum_{j=H,V,D,A} R_e(j), \\ \mathrm{QBER}_e &= \frac{1}{4R_e}\sum_{j=H,V,D,A} E_j. \end{aligned} \tag{4.8}$$

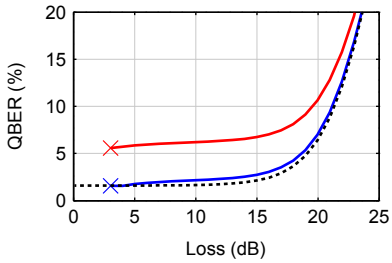

Figure 4.5: Modeled QBER observed by Bob versus line loss. The dotted curve shows QBER without Eve. At lower line loss, the QBER is due to imperfect fidelity, while at higher line loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER_e under our attack when only the total Bob's sifted key rate R_{ab} is matched. The upper solid curve (red) additionally keeps his four channel rates equal.

The only free parameters left for Eve to manipulate are the mean photon numbers of her signal. Knowing the angular scanning data, Eve can use a numerical optimization to find values of μ_H, μ_V, μ_D, μ_A that minimize QBER_e while keeping $R_e = R_{ab}$, where R_{ab} is Bob's sifted key rate without Eve. Our numerical optimization achieves this for Alice–Bob channel loss ≥ 3 dB if they are willing to accept a slight increase of QBER by less than 0.7% (see Fig. 4.5). Here we assumed Bob's detector parameters as measured by us: efficiency at $\phi = \theta = 0$ was 0.4 in all four channels, and individual detector background count probabilities were in the range of 430×10^{-9} to 1560×10^{-9} per 1 ns coincidence window. These optimization results are realistic conditions for a successful attack on most communication channels [36, 37, 62, 63, 39, 40, 42, 35] Note that the distance Eve–Bob can be increased without affecting attack performance, by replacing Eve's illuminator with four collimators oriented at the required attack angles.

We went further and imposed an additional constraint on Eve to make $R_e(H) = R_e(V) = R_e(D) = R_e(A) = R_{ab}$. Our optimization shows that it is still possible for Eve to pick appropriate mean photon numbers and successfully attack the system with resultant QBER $< 6.82\%$ in 3–15 dB line loss range (Fig. 4.5). Similar QBER values are typical for outdoor channels, because of background light. Eve could shield Bob from the latter to hide QBER resulting from her attack.

We would like to point out that the attack angles depend on the way the setup is constructed, the imperfections of each individual sample of component, and each individual alignment procedure. I.e., no two setups are identical, even if they are produced in the same assembly line, and they will generally have different attack angles. However, from a

theoretical point of view, in quantum cryptography it is assumed from Kerckhoffs' principle [8] that except for the keys themselves, Eve has knowledge about all other parameters in the system. It is thus a valid assumption that she knows the attack angles. From a practical point of view, Eve may try techniques proposed in [51]. She may replace a small fraction of the signal states with faked states at different spatial angles, then listen to the classical communication to get an estimate of the efficiency of Bob's detectors at those angles. In this way she may gradually improve her estimate on the mismatch without causing excessive QBER. When she has enough information on the statistics of the mismatch, she can launch her full-fledged attack.

Possible countermeasure

This section is a part of [1] A countermeasures that might be able to prevent this spatial-mode detector-efficiency-mismatch attack is placing a spatial filter or 'pinhole' at the focal plane of lenses L1 and L2. Since the pinhole limits the field of view, any light entering at a higher spatial angle is blocked and Eve no longer has access to the target angles required to have control over Bob. We tested this countermeasure by placing pinhole of various diameters from 100 μm to 25 μm. Then, we perform the scan and find the mismatch area as we did previously. We found that the pinhole smaller than 25 μm in this specific optical setup can prevent the attack. The scan result is shown in Fig.4.6. The trade-off of this countermeasure is that the pinhole limited the field of view of the scanning from approximately 1.5 mrad(outer ring of the scan without pinhole) to 0.4 mrad (width of visible peak in the scan with pinhole). In practice, this might cause some loss due to diffraction in the optics, and angular deviation of the incoming beam under atmospheric turbulence. The limited field of view might also cause difficulties in pointing and tracking between Alice and Bob, and require a more precise and stable pointing system.

4.1.3 Laser damage

In the previous experiment we have already presented the ability of Eve to force a detection efficiency mismatch on a QKD system and presented a possible countermeasure. This study push us further in the loop of hacking and patching where Eve tries to overcome the countermeasure Alice and Bob deployed. We tested the same receiver to find out whether Eve is able to overcome the countermeasure or not.

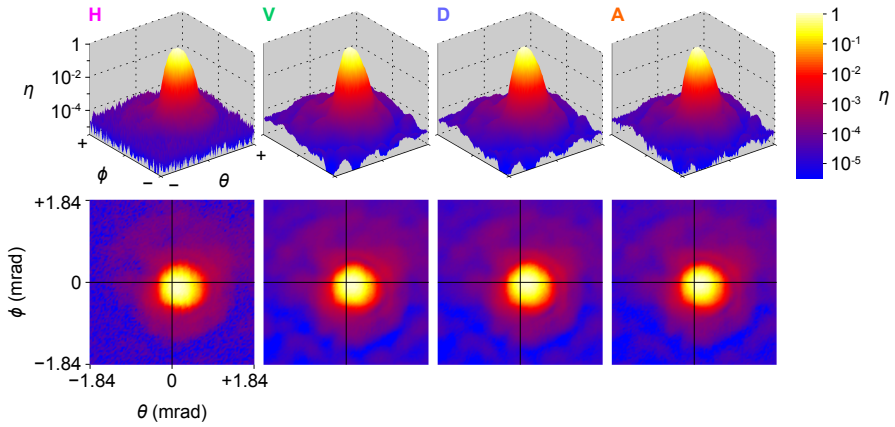

Figure 4.6: Angular efficiency scan of the receiver after a 25 μm diameter pinhole (Thorlabs P25S) is placed in the focal plane of L1, L2 [4.3(a)]. No detectable mismatch between channels was found under tight search conditions $\eta_i(j) \geq 0.001$ and $\delta_i(j) \geq 4$.

Motivation

After looks at a system with a countermeasure to her attack, Eve might tries to get around those countermeasures or exploit other weakness for other attack. This is the first time that Eve attempts to damage or destroy the countermeasure to recover her attack.

The security of the QKD system also assumes that the systems in Alice and Bob control are in an isolated environment where Eve does not have physical access nor can alter the devices inside. However, the front-end of a QKD system is essentially an analog optical system connected to the channel, and easily accessible by an eavesdropper. This section is a study of a new class of attack, laser damage attack, where Eve uses a high-power laser to damage or alter the properties of some components inside the receiver. To prove this idea, this research is a study about effect of a high-power laser on the pinhole's material. After that we investigated the ability of Eve to recover her spatial-mode detection-efficiency mismatch attack. The core idea is simple, try to widen the hole of pinhole using high-power laser without damaging other components in the receiver.

My contribution to this experiment is as followed(together with S.Sajeed):
-Apparatus setup and testing
-Post processing and security verification
-Wrote the first draft of method section
-Scheme and figure drawing

Method

The first experiment was to test whether the high-power laser was able to damage the pinhole (Thorlabs P25S) material, a 13 μm thick stainless steel plate. The latter contained a 810 nm laser diode (Jenoptik JOLD-30-FC-12) pumped by a current-stabilized power supply and was connected to a 200 μm core diameter multimode fiber. It provided a continuously adjustable 0 to 30 W c.w. power into the fiber. The reason for this wavelength was because, in the receiver under test, there were a pair of wavelength-selective filters placed right after lens L2. Those filters effectively work as a 532 nm narrow-band pass filter. The purpose of these filter was to reduce stray light and noise from the environment. By picking the high-power laser wavelength to be 810 nm, most of the laser's energy would be filtered off. With this, we expected that we would be able to damage the pinhole without damaging other components, especially the APD. This filter is a good example of a component that is put into an implementation for a specific purpose but open loophole for another attack.

We began by focusing the laser with a 7.5cm-focal length lens on to a pinhole placed at the focal point of the laser. We gradually increased the laser power until the metal plate around the pinhole began to burnt or vaporized. We found that the sample was burnt within 5 seconds with powers above 2 W.

The second test was whether laser can damage the filters. We replaced the pinhole in the previous test with a replica of filters inside the receiver. We gradually increased the laser power output up to 20 W. At such point, the core of the fiber connected to the laser was burnt but the filter was undamaged. We suspected that the laser reflected from the filter was the cause of the fiber damaged. This test concluded that the power level that damages the pinhole does not affect the filters.

The next test is to prove that Eve is able to damage the pinhole without damaging other components. First, the receiver were set to the normal operation. Next, the APD on the receiver were replaced with the power meters. Then, a collimated high-power laser beam was sent from one meter away through the center of the lenses L1 and L2. We measured the laser power on three points, in front of L1, in front of L3, and at the end of fiber optics in each channel. We found that, even though the laser power was more than 10W measured in front of L1, only the order of μW power was measured at L3 and only nW power was measured at the end of the fiber optics which is the safe level for the APD. Note that the direct measurement of the power at the pinhole's position inside the receiver was not possible since the high-power probe cannot fit inside the receiver.

The final attack test was done at 26.1 m distance. After inserting the pinhole (Thorlabs P25S) at the focal point of lens L1 and L2, we repeated our experiment on the previous

section to confirm that the pinhole was able to prevent the efficiency mismatch attack. Next, the scanning apparatus on Eve's side was replaced by the high power laser and a plano-convex lens L5 (Thorlabs LA1131-B; Fig. 4.7a). A nearly collimated beam was sent to Bob. The beam's intensity was nearly uniformly distributed across Bob's L1 (50 mm diameter achromatic doublet, Thorlabs AC508-250-A), with less than ±10% intensity fluctuation across Bob's input aperture. Transmission of L1 was about 82%, owing to its antireflection coating being designed for a different wavelength band. Note that these transmission percentages were a result from a separate test where 100mW laser of 810nm were sent through each components and measured by a power meter on the other side. As a result, the power delivered at the pinhole plane was 3.6 W, sufficient to reliably produce a hole of ≈ 150 μm diameter in less than 10 s in a standard stainless-steel foil pinhole (Thorlabs P25S).

Result

This section is part of [2]. After the last test, the burning apparatus was removed and another scan process was done. The counts from each channel were put in the analysis as we did in the efficiency mismatch. With this larger pinhole opening, it was again possible to send light at angles that had relatively higher mismatches in efficiency as shown in Fig. 4.8b. This enabled the faked-state attack under realistic conditions of channel loss in the 1–15 dB range with a quantum bit error ratio (QBER) $< 6.6\%$. Thus laser damage completely neutralizes this countermeasure, and makes this free-space QKD system insecure.

4.2 Attack on a fiber-based QKD system

4.2.1 System under test

The subject of this study is a plug-and-play QKD system, Clavis2, produced by IDQuantique(IDQ). The detail of this system was given in the previous section on the example of fiber-based QKD system. More detail and specifications of the system can be seen in [43, 44]. The security of this system implemented in the manufacturer's software is based on the security analysis in [64] which did not considered the finite key-size effect.

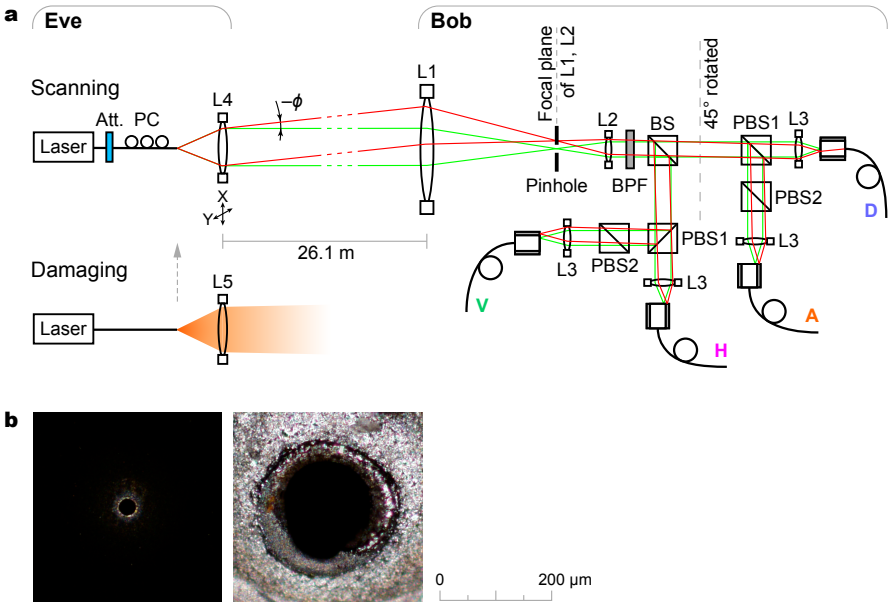

Figure 4.7: Attack on a free-space QKD system. **a**, Experimental setup. QKD receiver Bob consists of two lenses L1, L2 reducing input beam diameter, 50:50 beamsplitter BS, and two arms measuring photons in HV and DA polarizations using polarizing beamsplitters PBS [1, 35]. Photons are focused by lenses L3 into multimode fibers leading to single-photon detectors. Setup drawing is not to scale. Eve's apparatus contains a scanning laser source that tilts the beam angle (ϕ, θ) by laterally shifting lens L4. Green marginal rays denote initial Eve's alignment, replicating the alignment Alice–Bob at $\phi = \theta = 0$. Red marginal rays show a tilted scanning beam missing fiber cores V, H, A, but coupling into D. Eve's damaging laser source can be manually inserted in place of the scanning source. Att., attenuator; PC, polarization controller. **b**, Spatial filter before and after damage. Darkfield microphotographs show front view of the pinhole. See Supplementary Video 1 for real-time recording of laser damage to the pinhole inside Bob.

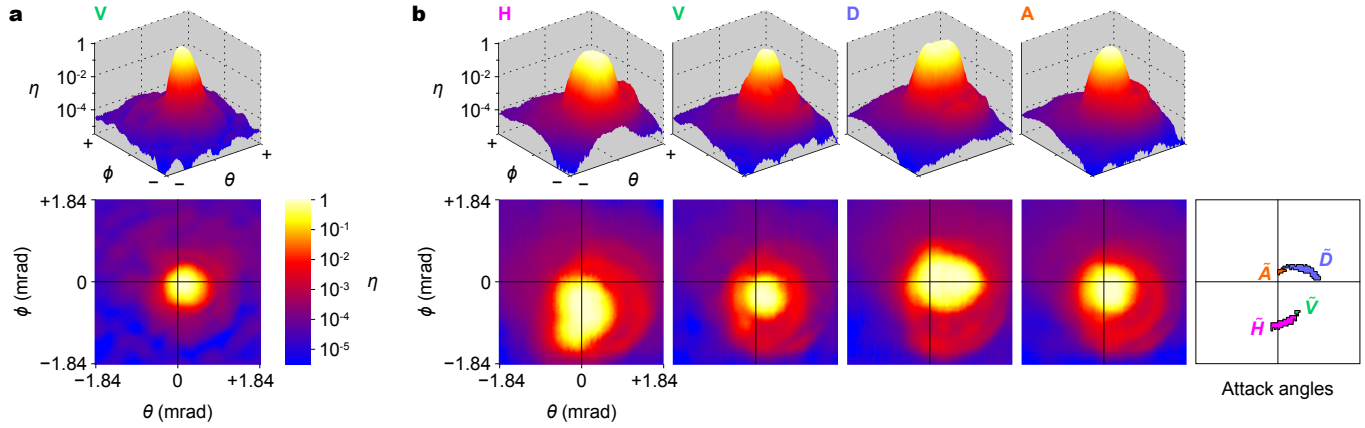

Figure 4.8: Efficiency-mismatch side-channel opened after laser damage in free-space QKD system. Each pair of 3D–2D plots shows normalised photon detection efficiency η in a receiver channel versus illuminating beam angles ϕ and θ. **a**, Before laser damage, the angular dependence is essentially identical between the four channels [1]. Plot for one channel (V) before damage is shown. **b**, After the laser damage, the four receiver channels H, V, D, A exhibit unequal sensitivity to photons outside the middle area around $\phi = \theta = 0$. The last plot shows angular ranges for targeting the four detectors that satisfy conditions for the faked-state attack.

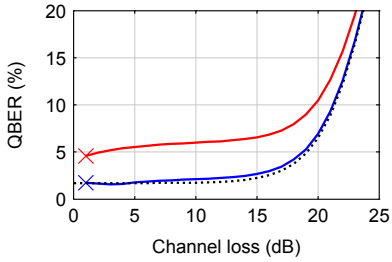

Figure 4.9: Modelled QBER observed by Bob in free-space QKD system. The dotted curve shows QBER without Eve. At lower channel loss, the QBER is due to imperfect fidelity, while at higher channel loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER under our attack when only Bob's sifted key rate is kept the same as before the attack. The upper solid curve (red) additionally keeps the same sifted key rates conditioned on each polarization sent by Alice, which more closely mimics a realistic system operation.

4.2.2 Finite key size attack

Motivation

The finite key size analysis on QKD system has been established and developed for many years [32, 48, 49]. Unfortunately, many QKD schemes, especially the scheme that went commercialized, still neglected this effect and employs only asymptotic key analysis on their systems. Some did it without realizing the effect while some just claim that that their raw key size is large enough to neglect the finite-key-size effect on their security. In the case of Clavis2, IDQ implemented this system when finite-key-size analysis for BB84 protocol was not available.

This study is aimed to emphasize the significance of finite-key-size effects on a practical system. The goal is to demonstrate the ability of Eve to force the system to generate a secret key from a raw key size that is smaller than which was predicted in the system design. As a result, the asymptotic limit employed in the system might no longer hold.

My contribution to this experiment is as follows:
(First measurements on unpatched system were done by Sajeed)
-Studied finite key-size analysis
-Data processing
Second experiment, testing ID Quantique's software update
-Studied the updated software
-Set up and re-run the experiment
-Data processing
-Wrote the manuscript

Method

Under normal operation, the system exchanges the quantum signal and saves the raw key until the memory buffers in Alice and Bob are filled. Then, they perform sifting, error correction and privacy amplification. [45, 43]. One of the features of Clavis2 is that the system will terminate the raw key exchange process when the photon detection efficiency in the quantum channel drops below a certain value, and perform the post-processing from the raw key already exchanged until then. This feature was implemented to compensate the drift of timing alignment of detector gates [44]. Since the security proof of the system did not take account the statistical deviation of non-infinite key length, if Eve can force

the system to generate secret keys from a shorter raw key length, the security proof would no longer apply.

To demonstrate the ability of Eve to force the system to work with a small key length, we began our experiment by setting the system in a normal operation. A variable attenuator was inserted in between the quantum channel. The attenuator was set to 0dB at the beginning. During the raw-key exchange phase, we let the system exchange the raw-key for a set period then change the value of the variable attenuator to induce a 40dB-loss in the fiber. This reduced the detection efficiency in Bob and forced the process to be terminated and began the post-processing. For all non-zero distilled keys, we recorded the length of the sifted key, the number of bits disclosed in the error correction, the error rate, and length of secret key reported by the system. We varied the duration of each raw key exchange to correct the parameter for various lengths of sifted key. We found that the length of distilled key was decreased as the length of sifted key decreased. Next step is to verify if this data falls under the theoretical bound.

Result

We compared the experiment's result with the asymptotic key rate equation 3.2 and finite key rate equation 3.3. After substituting the parameters from the experiment into the equation, we obtained a lower bound of secret key length as shown in Fig.4.10. The blue line was calculated under the asymptotic assumption as used in the system's protocol. The red and black line is the bound of secret key rate under the finite-key size assumption (the area below each line given the secure zone correspond to the security conditions applied to that plot). It can be seen from 4.10 that the experimentally distilled key-size from the system, green $\times$, satisfied the security criteria for the asymptotic assumption. However, the experiment result fall out of bound of finite-key size analysis upto security parameter $\epsilon = 10^{-1}$. As a result, security of the system is not covered by this security proof.

In the middle of our study, IDQ has released a new patch for Clavis2. This patch reduced the QBER and let the system perform post-processing only when the sifted key in the memory exceed a threshold of around 1 million bits. We perform our experiment and recalculated our plot using the new parameters acquired from the system. The result showed that the distilled key is within the secure bound (see Fig 4.11). By the time of submitting this thesis, the manuscript is being reviewed by co-authors. the current version of the manuscript can be seen in Appendix B.3

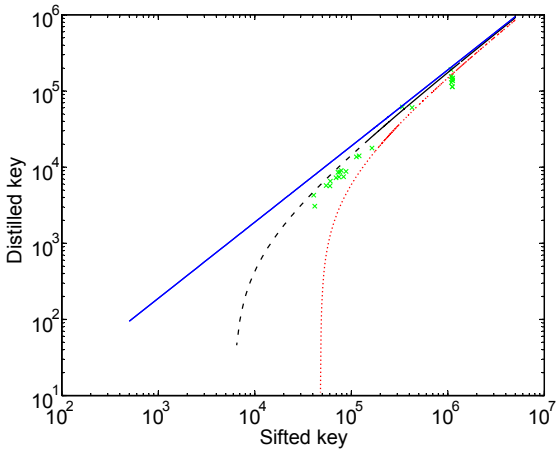

Figure 4.10: Secret key rate vs raw key rate. Blue dashed line is the infinite key bound. Red dotted line is finite-key size bound with $\epsilon = 10^{-10}$. Black-line is finite-key-size bound with $\epsilon = 10^{-1}$. Green dots are experimental results with 3 dB line loss and 5.2% error rate.

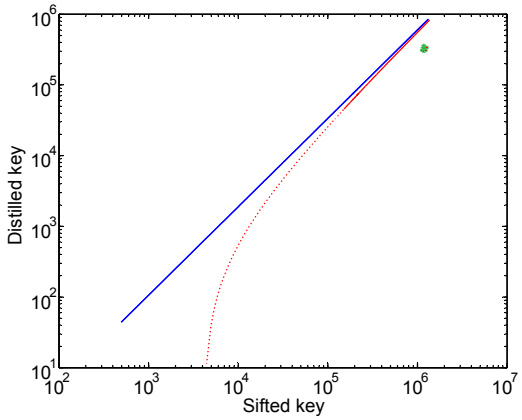

Figure 4.11: Experiment result with the new software. Blue line is the infinite key bound. Red-dotted line is finite-key size bound with $\epsilon = 10^{-10}$. Green $\times$ are experiment results.

Chapter 5

Conclusions

In this thesis I have performed three experiments that showed ability of Eve to manipulate the system so that the she gain more information about the key than what Alice and Bob expected. The first experiment was a spatial-mode detection-efficiency-mismatch where Eve take control the path of the beam and manipulate the probability of detection in each detector, which would allows her to perform intercept-and-resent attack successfully. Second experiment was Laser damage attack, in which Eve employs high-power laser to alter the property of pinhole that was used as a countermeasure for the efficiency mismatch attack. We showed that Eve successfully recover her attack ability without damaging other devices in the receiver. The third experiment was a demonstration of Eve's ability to force QKD a system to generate secret key out of raw key in finite key regime in which the asymptotic security analysis employed by the system might not hold.

I hope that this work will emphasize the necessity 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 guarantee the high level of security promised by the theory of QKD.

5.1 Recommendations and outlook

5.1.1 Detection-efficiency mismatch

- This is a test of a laboratory prototype model of receiver. A test on real devices that are going to be used in long distance QKD or satellite communication is needed.

- Real-life free-space communication suffered from atmospheric turbulence. This subject need to be study on both Alice and Bob key distribution and its effect on Eve's attack.

5.1.2 Laser damage

- This is a test on specific type of pinhole material. The effect of high-power laser on difference spacial filter materials is required.

5.1.3 Finite-key-size attack

- As was shown that the security analysis might no long hold under this attack, an explicit attack that take advantage of this scheme to gain information about the key is left for further study.

Appendix A

Technical details

This section contains technical details of the experiments in Chapter 4. This consists of source codes that I developed to control the devices and post processing.

To acquire the detection efficiency of each channel in the receiver at each specific angle of incoming photon, this experiment require automated control of the translation stage and data acquisition. For this experiment, only computer was used to control both translation stage in the emitter side, and counters which connected to APDs in the receiver side in order to simplify the synchronization processes. All data acquisition and post processing are programmed on Matlab.

A.1 Experiment

The experiment started by established the connection between computer, translation stage, and counters via USB port. Next was a manual setup before the scan. First, we performed a fine alignment between the emitter and receiver to mimic Alice and Bob setup, by send the beam through the center of receiver and maximize the photon count rate on all four APD. The final coordinate of translation stage after this step was used as a reference point for the scan (position $\phi = 0, \theta = 0$). After that, we moved the translation stage along ϕ axis until the beam fail off the objective lens of the receiver, record that distance $\Delta\phi$ from the center. The distance was divided into 50 parts which determined step size of the scan. From here, the 'position' will be defined as a multiplication of this step size. These parameters from this step were put in the program for automated scan. For more detail, please see comments on the code A.1.

Listing A.1: Matlab code for translation stage control and data acquisition in detection efficiency mismatch experiment

```
1
2 clear; close all; clc;
3 global hy hx hz; % make h a global variable so it can be used
     outside the main
4
5 %% Create Matlab Figure Container
6 fpos     = get(0,'DefaultFigurePosition'); % figure default
     position
7 fpos(3) = 650; % figure window size;Width
8 fpos(4) = 450; % Height
9 global ack
10 ack=0;
11 fy = figure('Position', fpos,...
12             'Menu','None',...
13             'Name','APT_GUI');
14 %% Create ActiveX Controller
15 hy = actxcontrol('MGMOTOR.MGMotorCtrl.1',[20 20 600 400], fy);
16
17 fx = figure('Position', fpos,...
18             'Menu','None',...
19             'Name','APT_GUI');
20 %% Create ActiveX Controller
21 hx = actxcontrol('MGMOTOR.MGMotorCtrl.1',[20 20 600 400], fx);
22
23 fz = figure('Position', fpos,...
24             'Menu','None',...
25             'Name','APT_GUI');
26 %% Create ActiveX Controller
27 hz = actxcontrol('MGMOTOR.MGMotorCtrl.1',[20 20 600 400], fz);
28
29 %% Initialize
30 % Start Control
31 hx.StartCtrl;
32 hy.StartCtrl;
33 hz.StartCtrl;
```

```
34 % Set the Serial Port Number
35 SNx = 90847260;
36 SNy = 90847261;
37 SNz = 90847262; % put in the serial number of the hardware
38 set(hx, 'HWSerialNum', SNx);
39 set(hy, 'HWSerialNum', SNy);
40 set(hz, 'HWSerialNum', SNz);
41
42 % Indentify the device
43 hx.Identify;
44 hy.Identify;
45 hz.Identify;
46
47 pause(3); % waiting for the GUI to load up;
48 %% Controlling the Hardware
49 %h.MoveHome(0,0); % Home the stage. First 0 is the channel ID (
       channel 1)
50                  % second 0 is to move immediately
51 %% Event Handling
52 hx.registerevent({'MoveComplete' 'MoveCompleteHandler'});
53 hy.registerevent({'MoveComplete' 'MoveCompleteHandler'});
54 hz.registerevent({'MoveComplete' 'MoveCompleteHandler'});
55
56 %% Sending Moving Commands
57 timeout = 10; % timeout for waiting the move to be completed
58
59 optx= .396;
60 opty= .481;
61 optz= .827;
62 scanSize = .05;
63 scanStep = .001;
64
65
66 row =1;
67 col =1;
68
69 format long;
70
```

```
hy.SetAbsMovePos(0,opty);
hy.MoveAbsolute(0,opty);
%pause for ack
while ~ack pause(0.01); end
ack=0;
pause(0.1);%pause for vibration
hx.SetAbsMovePos(0,optx);
hx.MoveAbsolute(0,optx);
while ~ack pause(0.01); end
ack=0;
pause(0.1);
hz.SetAbsMovePos(0,optz);
hz.MoveAbsolute(0,optz);
while ~ack pause(0.01); end
ack=0;
pause(0.1);

%%%%PORT INITIATE%%%%%%
d1 = serial('COM7');
d2 = serial('COM8');
d3 = serial('COM9');
d4 = serial('COM10');

fopen(d1);
fopen(d2);
fopen(d3);
fopen(d4);

fprintf(d1,'MODE0');                    %MODE 0 - TIME COUNTING
fprintf(d1,'AUTM0');
%fprintf(sport,'SRCE1');                    %SOURCE: 0A AND 1B
fprintf(d1,'LEVL1,1');
fprintf(d1,'LEVL2,1');
fprintf(d1,'SIZE1');
fprintf(d1,'GATE0.1');
fprintf(d1,'DISP0');

fprintf(d2,'MODE0');                    %MODE 0 - TIME COUNTING
```

```
109 fprintf(d2,'AUTM0');
110 %fprintf(sport,'SRCE1');                    %SOURCE: 0A AND 1B
111 fprintf(d2,'LEVL1,1');
112 fprintf(d2,'LEVL2,1');
113 fprintf(d2,'SIZE1');
114 fprintf(d2,'GATE0.1');
115 fprintf(d2,'DISP0');
116
117 fprintf(d3,'MODE0');                       %MODE 0 - TIME COUNTING
118 fprintf(d3,'AUTM0');
119 %fprintf(sport,'SRCE1');                    %SOURCE: 0A AND 1B
120 fprintf(d3,'LEVL1,1');
121 fprintf(d3,'LEVL2,1');
122 fprintf(d3,'SIZE1');
123 fprintf(d3,'GATE0.1');
124 fprintf(d3,'DISP0');
125
126 fprintf(d4,'MODE0');                       %MODE 0 - TIME COUNTING
127 fprintf(d4,'AUTM0');
128 %fprintf(sport,'SRCE1');                    %SOURCE: 0A AND 1B
129 fprintf(d4,'LEVL1,1');
130 fprintf(d4,'LEVL2,1');
131 fprintf(d4,'SIZE1');
132 fprintf(d4,'GATE0.1');
133 fprintf(d4,'DISP0');
134
135 %%%%%%%%%%+=====END PORT INITIALIZE===%%%%%%%
136
137 %%%Begin Scan
138 finy = opty+scanSize;
139 beginy = opty-scanSize;
140 finz = optz+scanSize;
141 beginz = optz-scanSize;
142
143 for yPos = beginy:scanStep:finy;
144     hy.SetAbsMovePos(0,yPos);
145     hy.MoveAbsolute(0,yPos);
146     while ~ack pause(0.01); end
```

```
147       ack=0;
148       pause(0.1);
149     %disp(time)
150     for zPos = beginz:scanStep:finz;
151         hz.SetAbsMovePos(0,zPos);
152         hz.MoveAbsolute(0,zPos);
153         while ~ack pause(0.01); end
154         ack=0;
155         pause(0.1);
156         disp(yPos);
157         disp(zPos);
158
159         fprintf(d1,'MEAS?0');
160         det1(row,col) = fscanf(d1,'%g');
161
162         fprintf(d2,'MEAS?0');
163         det2(row,col) = fscanf(d2,'%g');
164
165         fprintf(d3,'MEAS?0');
166         det3(row,col) = fscanf(d3,'%g');
167
168         fprintf(d4,'MEAS?0');
169         det1(row,col) = fscanf(d4,'%g');
170        %det4(row,col)
171         row = row+1;
172     end
173     row =1;
174     col = col+1;
175
176 end
177
178 fclose(instrfind);
179
180 figure(5);
181 mesh(det1);
182 figure(6)
183 mesh(det2);
184 figure(7);
```

```
185 mesh(det3);
186 figure(8);
187 mesh(det4);
188
189 filename = '2014-06-10-noPinHole_50umCore_2_noEpd.xlsx';
190 xlswrite(filename,det1,'Sheet1','A1');
191 xlswrite(filename,det2,'Sheet2','A1');
192 xlswrite(filename,det3,'Sheet3','A1');
193 xlswrite(filename,det4,'Sheet4','A1');
194 disp('Scan Finished')
```

A.2 Post processing

After acquired the count rate for each angle, we searched for specific angles that causes detection efficiency mismatch for each polarization orientation using code A.3. The goal is tho find an angle that yield highest efficiency ratio δ_j and absolute efficiency η_j defined in section 4.1.2.

Listing A.2: Matlab code for mismatch angle finding.

```
1 %------======= mismatchFinding =======------
2 % Code to find mismatch area
3 clear; clear all; clc;
4
5 p = xlsread('APDcorrection_poly8fit.xlsx');
6
7 fileName = '2014-08-18.xlsx';
8 det_d = xlsread(fileName,'Sheet1');
9 det_a = xlsread(fileName,'Sheet2');
10 det_h = xlsread(fileName,'Sheet3');
11 det_v = xlsread(fileName,'Sheet4');
12
13 det_d = correction(det_d,p(2,2:10));
14 det_a = correction(det_a,p(4,2:10));
15 det_h = correction(det_h,p(3,2:10));
16 det_v = correction(det_v,p(1,2:10));
17
```

```
18 %normalize the count to get rid of the effect of elliptical-
       polarization of the laser source.
19 det_d = det_d/max(max(det_d));
20 det_a = det_a/max(max(det_a));
21 det_h = det_h/max(max(det_h));
22 det_v = det_v/max(max(det_v));
23
24 det_hh = det_h(3:99,3:99);
25 det_vv = det_v(3:99,3:99);
26 det_dd = det_d(3:99,3:99);
27 det_aa = det_a(3:99,3:99);
28
29
30
31 dataSize = size(det_hh);
32
33 %Set mismatch parameters
34 h_threshold = 0.2;  % ratio threshold compare to the center peak
35 v_threshold = .002;
36 d_threshold = .08;
37 a_threshold = 0.001;
38 ratio_h = 100;  % ratio threshold compare to other two channel in
       the different basis
39 ratio_v = 1.01;
40 ratio_d = 40;
41 ratio_a = 1.13;
42 e_h = 100;  % ratio threshold compare to the orthogonal
       polarization
43 e_v = 2;
44 e_d = 30;
45 e_a = 1.15;
46
47 %find the mismatch points and paint that coordinate with
       respective color
48 for i = 1:dataSize(1)
49     for j = 1:dataSize(2)
50         if ((det_h(i,j) > h_threshold) && ((det_h(i,j)/det_d(i,j)
               ) > ratio_h)...
```

```
51                  && ((det_h(i,j)/det_a(i,j)) > ratio_h) && ((det_h
                        (i,j)/det_v(i,j)) > e_h ) )
52              bias(i,j) = 10000; % value correspond to a color in
                    surface plot
53
54          elseif ((det_v(i,j) > v_threshold) && (det_v(i,j)/det_d(i
                ,j) > ratio_v)...
55                  && (det_v(i,j)/det_a(i,j) > ratio_v) && (det_v(i,
                        j)/det_h(i,j) > e_v) )
56              bias(i,j) = 8000;
57
58          elseif ((det_d(i,j) > d_threshold) && (det_d(i,j)/det_h(i
                ,j) > ratio_d)...
59                  && (det_d(i,j)/det_v(i,j) > ratio_d) && (det_d(i,
                        j)/det_a(i,j) > e_d))
60              bias(i,j) = 6000;
61
62          elseif ((det_a(i,j) > a_threshold) && (det_a(i,j)/det_h(i
                ,j) > ratio_a)...
63                  && (det_a(i,j)/det_v(i,j) > ratio_a) && (det_a(i,
                        j)/det_d(i,j) > e_a))
64              bias(i,j) = 4000;
65          else
66              bias(i,j) = 0;
67
68          end
69      end
70  end
71
72  surf(bias) %plot the result
73
74  %------====== end mismatchFinding ======------
```

For j-polarization, the search performed manually by first set $j_threshold = 0, e_j = ratio_j = 1000$, then decreased $ratio_j and e_j$ until we found a group of adjacent points (area) that satisfied the condition for that polarization. We search for an 'area' instead of 'point' to neglect the effect of noise spike in the low-count-rate region. After that, we increased $j_threshold$ until the area shrank down to a group of 5-10 points. Use that final value of

$j_t hreshold, e_j, and ratio_j$ for optimization.

Next program is an optimization program to determine the success of Eve's attack on the system. The model of the attack was stated in section 4.1.2. Eve's attack is success if she can match the detection rate predicted by Alice and Bob, with error under a certain threshold. The following is an optimization program I developed independently. Goal of this program was to find a set of mean photon number sent by Eve for each polarization orientation, which optimized the detection rate of Bob while limited the error rate below a certain threshold. This program capable of handle the model where Eve use photon-number-state with arbitrary distribution. But in this case, we assumed that Eve's photon source followed Poisson distribution. This was different from the final program stated in section 4.1.2 and [1]. The reason was that, at the mismatch angles, the detection efficiency of Bob was lower compared to the ideal case at the center. At first, we did not know how much detection rate Eve could generate and whether the rate could keep up with Bob's expectation from the channel without Eve.

Listing A.3: Matlab code for mismatch angle finding.

```
%-----=====Main=====-----
%main program
clear; clear all;

--set variables--
nCrTmp = zeros(101,101); %Combination function
for i = 0:100
    for j = 0:i
        nCrTmp(i+1,j+1)= nCr(i,j);
    end
end
global nCrTmp ;

ub = Inf(4,1);
ub(:)=100;
lb = zeros(4,1);
b = 0;
Aeq = zeros(1,4);
mu0 = zeros(4,1);
mu = zeros(4,1);

--optimization--
```

```
23 options = optimoptions('fmincon','UseParallel',true); %enable
       multi-CPU calculation
24
25 mu = fmincon(@rateOpt,mu0,Aeq,b,Aeq,b,lb,ub,@rateCon,options) %
       call optimization function, fmincon, to find set of mean
       photon number, mu, that optimize detection rate in rateOpt
       module, under the constraint defined in rateCon module.
26
27 etas =
       {0.02,0.0,0.0015,0.002;0,0.01,0.0025,0.0012;0.0075,0.007,0.03,0;0.006,0.0
        %efficiency mismatch parameters from the experiment
28
29 ---calculate optimized key rate and error rate---
30 HIn = detRate1(mu(1),etas{1,1},etas{1,3},etas{1,4});
31 VIn = detRate1(mu(2),etas{2,2},etas{2,3},etas{2,4});
32 DIn = detRate1(mu(3),etas{3,3},etas{3,1},etas{3,2});
33 AIn = detRate1(mu(4),etas{4,4},etas{4,1},etas{4,2});
34 H = (HIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
35 V = (VIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
36 D = (HIn(3)/2+VIn(4)/2+DIn(1)/2)/4;
37 A = (HIn(3)/2+VIn(4)/2+AIn(1)/2)/4;
38 rateTot = H+V+D+A
39 errRate = (HIn(3)+HIn(4)+VIn(3)+VIn(4)+DIn(3)+DIn(4)+AIn(3)+AIn
       (4))/4/2/2/rateTot %denominators are AliceBitChoice, evePick,
       incompBasis
40
41 %-----=====end Main=====------
42
43 %-----=====detRate1=====------
44 %detection rate calculation module. Get mean photon number(mu)
       and mismatch parameters(eta), then calculate detection rate
       for the channel that match incoming photon polarization(
       thisRate), the orthogonal channel(ortRate), and two other
       channel in the other basis (oth1Rate,oth2Rate)
45 function x = detRate1(mu,etaThis,etaOth1,etaOth2)
46
47 global nCrTmp
48
```

```
49 thisRate = 0; %initial background count rate
50 ortRate = 0;
51 oth1Rate = 0;
52 oth2Rate = 0;
53
54 %---calculate key rate using equation 4.1---
55 for n = 1:50
56     nRate = mu^n*exp(-mu)/factorial(n);
57     for m = 0:n
58         dummyH = 0;
59         dummyD = 0;
60         dummyA = 0;
61         for l = 0:(n-m)
62             dummyH = dummyH+(nCrTmp(n-m+1,l+1))*(0.5^(n-m))*((1-
                   etaOth1)^(n-m-l))*((1-etaOth2)^l);
63             dummyD = dummyD+(nCrTmp(n-m+1,l+1))*(0.5^(n-m))
                   *(1-(1-etaOth1)^(n-m-l))*((1-etaOth2)^l+0.5*(1-(1-
                   etaOth2)^l));
64             dummyA = dummyA+(nCrTmp(n-m+1,l+1))*(0.5^(n-m))
                   *(1-(1-etaOth2)^(l))*((1-etaOth1)^(n-m-l)
                   +0.5*(1-(1-etaOth1)^(n-m-l)));
65         end
66         thisRate = thisRate+nRate*(nCrTmp(n+1,m+1))*(0.5^n)
               *((1-(1-etaThis)^m))*dummyH;
67         oth1Rate = oth1Rate+nRate*(nCrTmp(n+1,m+1))*(0.5^n)*((1-
               etaThis)^m)*(dummyD);
68         oth2Rate = oth2Rate+nRate*(nCrTmp(n+1,m+1))*(0.5^n)*((1-
               etaThis)^m)*(dummyA);
69     end
70 end
71 x = [thisRate,ortRate,oth1Rate,oth2Rate];
72 %-----======end detRate1======-----
73
74 %-----======rateOpt======-----
75 %calculate 1-(detection rate) for the minimization program
76
77 function rateTot = rateOpt(mu)
78 global nCrTmp ;
```

```
79 global etas;
80 for i = 0:100
81     for j = 0:i
82         nCrTmp(i+1,j+1)= nCr(i,j);
83     end
84 end
85
86 etas =
       {0.02,0.0,0.0015,0.002;0,0.01,0.0025,0.0012;0.0075,0.007,0.03,0;0.006,0.0
87
88     HIn = detRate1(mu(1),etas{1,1},etas{1,3},etas{1,4});
89     VIn = detRate1(mu(2),etas{2,2},etas{2,3},etas{2,4});
90     DIn = detRate1(mu(3),etas{3,3},etas{3,1},etas{3,2});
91     AIn = detRate1(mu(4),etas{4,4},etas{4,1},etas{4,2});
92     H = (HIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
93     V = (VIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
94     D = (HIn(3)/2+VIn(4)/2+DIn(1)/2)/4;
95     A = (HIn(3)/2+VIn(4)/2+AIn(1)/2)/4;
96     rateTot = 1-(H+V+D+A);
97
98 %-----=====end rateOpt=====------
99
100 %-----=====rateCon=====------
101 %Constraint module. To make sure that Eve induce error rate lower
       than the threshold(errTh), this module calculate c = (error
       rate)-(errTh) to be used as constraint c<=0 in the
       optimization program.
102 function [c,ceq] = rateCon(mu)
103 global nCrTmp ;
104 global etas;
105
106     errTh = 0.3;
107
108     HIn = keyRate1(mu(1),etas{1,1},etas{1,3},etas{1,4});
109     VIn = keyRate1(mu(2),etas{2,2},etas{2,3},etas{2,4});
110     DIn = keyRate1(mu(3),etas{3,3},etas{3,1},etas{3,2});
111     AIn = keyRate1(mu(4),etas{4,4},etas{4,1},etas{4,2});
```

```
    H = (HIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
    V = (VIn(1)/2+DIn(3)/2+AIn(4)/2)/4;
    D = (HIn(3)/2+VIn(4)/2+DIn(1)/2)/4;
    A = (HIn(3)/2+VIn(4)/2+AIn(1)/2)/4;

    ceq = 0;
    rateTot = H+V+D+A
    c = (HIn(3)+HIn(4)+VIn(3)+VIn(4)+DIn(3)+DIn(4)+AIn(3)+AIn(4))
        /4/2/2/rateTot-errTh; %error rate-threshold
%-----=====end rateCon=====-----
```

The result showed that, for an ideal channel without noise and transmission loss, Eve able to find set of mean photon number that produce detection rate at Bob higher than 0.5, while induced error rate lower than 0.02. From this result, we shifted our focus to an optimization program that match Bob's detection rate while minimize error rate as stated in section 4.1.2 and [1], this program was developed with Shihan Sajeed. The photon-number-state model in the previous program was used as a cross-check with the Poisson distribution assumption used in the new program. Though it was not as efficient as the new program, the program with photon-number-state shall be useful for future analysis where one consider Eve with single photon source or source with non-Poisson statistics.

Listing A.4: Matlab code for error rate optimization (developed with Shihan Sajeed).

```
%-----===== Main =====-----
% This is the main program. It uses three functions for
    optimization
% get_parameters have all the data inside it
% constraints have all the constraints required by the solver
% minimize error is the funstion that has the main objective
    function as
% required by the solver


% the resultant plot that this program shows depends on two
    choice values
% in function constraints and minimize_error

clear all; clc; format shortG;

```

```
global losss   % global function loss used by all the functions
i = 1;
for losss = 30; % choose a range of losses

[eta_t, eta_d, eta0, mu0, eta, v_b, v_e,te,ne,pd_b,pd_e] =
    get_parameters;

lb = zeros(4,1);
ub = inf(4,1);
% for individual rate optimization keep x0 =2;
% for total rate optimization keep x0 =1;

x0 = 1*ones(4,1); % initial guess

options = optimset('Algorithm','interior-point','display','iter')
    ; % options for the solver
[mu,qber,exitflag,output] = fmincon(@minimize_error,x0
    ,[],[],[],[],lb,ub,@constraints,options); % call the solver
    fmincon
mus(i,1:4) = mu; % the values of mu that matches rates while
    minimizing qber
iterations = output.iterations; %debuging purpose
[c,ceq(i,1:4),errors(i,1:5)] = constraints(mu); %debuging purpose
diff_attack(i) = .25*(abs(ceq(i,1))+abs(ceq(i,2))+abs(ceq(i,3))+
    abs(ceq(i,4))); %debuging purpose
check(i) = exitflag; % exitflag that shows the condition of
    ending iteration (check fmincon exit flag in mathworks website
final_loss(i) = losss;  % x-values to plot
err(i) = qber*100;      %y-values to plot
i = i+1;
end

plot(final_loss,err,'r','Linewidth',4);

hold off;
title('Loss versus error curve','fontsize',26);
xlabel('Loss (db)','fontsize',18);
ylabel('error (%)','fontsize',18);
```

```
45 grid on;
46
47
48 set(findall(gcf,'type','axes'),'fontname','cambria','fontsize'
       ,16);
49
50 max(err)
51
52 %-----=====end Main=====-----
53
54 %-----=====getParameter=====-----
55 %Return all parameter needed for optimization
56 function [eta_t, eta_b, eta_0, mu0, eta, v_b, ve,te,eta_e,pd_b,
       pd_e] = get_parameters
57
58 global losss;
59 %alpha = 1;  %in db/km
60 eta_t = 10^(-losss/10); %line transmission loss
61 eta_b = .7;  % detector efficiency in the middle
62 eta_0 = eta_t *eta_b; % total loss
63 mu0 = eta_t; % optimal mu chosen to be equal to line transmission
       loss
64
65
66 % practical biased point data from the 2014-08-18.xslx files
67 h_th = 0.2;
68 v_th = 0.002;
69 d_th = 0.08;
70 a_th = 0.001;
71 r_h = 100;
72 r_v = 1.01;
73 r_d = 40;
74 r_a = 1.13;
75 e_h = 100;
76 e_v = 2;
77 e_d = 30;
78 e_a = 1.15;
79
```

```
80 v_b = .99; %visibility in Bob
81 ve = .99; %visibility Eve
82 te = 1;  %losses in Eve
83 eta_e = .85;  %effciciency of Eve's detector
84 pd_b = 300*1e-9;
85 pd_e = 1*1e-9;
86
87 %2014-07-18 data
88 eta(1) = h_th;      %eta_h_h
89 eta(2) = h_th/e_h;        %eta_v_h
90 eta(3) = h_th/r_h; %eta_d_h
91 eta(4) = h_th/r_h; %eta_a_h
92
93 eta(5) = v_th/e_v;        %eta_h_v
94 eta(6) = v_th;      %eta_v_v
95 eta(7) = v_th/r_v; %eta_d_v
96 eta(8) = v_th/r_v; %eta_a_v
97
98
99 eta(9)  = d_th/r_d;%eta_h_d
100 eta(10) = d_th/r_d;%eta_v_d
101 eta(11) = d_th;    %eta_d_d
102 eta(12) = d_th/e_d;       %eta_a_d
103
104
105 eta(13) = a_th/r_a;%eta_h_a
106 eta(14) = a_th/r_a;%eta_v_a
107 eta(15) = a_th/e_a;       %eta_d_a
108 eta(16) = a_th;    %eta_a_a
109
110 %-----=====end getParameter=====-----
111
112 %%-----=====Constraint=====-----
113 % this part is for providing the rate constraints as required by
      the
114 % fmincon functino.
115 %note that the error equations included in this code are only for
      debugin
```

```
116 %purposes. They can be deleted if required.
117
118 function [c,ceq,e] = constraints(mu)
119
120 % 1 = match total rate
121 % 2 = match individual rates
122 choice = 1;  % choose whether to match total error rate ot
      individual error rates
123
124 [eta_t, eta_b, eta0, mu0, eta, v_b, ve,te,eta_e,pd_b,pd_e] =
      get_parameters;
125
126 p_t_ab = 1 - exp(-v_b*mu0*eta0/2)+pd_b;      %probability that
      target detector clicks
127 p_o_ab = 1 - exp(-(1-v_b)*mu0*eta0/2)+pd_b; %probability that
      orthogonal detector clicks
128 p_x_ab = 1 - exp(-.5*mu0*eta0/2)+pd_b;     %probability that other
       basis detector clicks
129
130 % Individual rates when there is no Eve
131 % rate_h_ab means, rate when Alice send 'H' and Bob measures in
      HV basis.
132 rate_h_ab = (1-p_x_ab)*(1-p_x_ab)*(p_t_ab + p_t_ab - p_t_ab*
      p_t_ab);
133 rate_v_ab = (1-p_x_ab)*(1-p_x_ab)*(p_t_ab + p_t_ab - p_t_ab*
      p_t_ab);
134 rate_d_ab = (1-p_x_ab)*(1-p_x_ab)*(p_t_ab + p_t_ab - p_t_ab*
      p_t_ab);
135 rate_a_ab = (1-p_x_ab)*(1-p_x_ab)*(p_t_ab + p_t_ab - p_t_ab*
      p_t_ab);
136 rate_ab = (rate_h_ab + rate_v_ab + rate_d_ab + rate_a_ab)/4;
137
138 % The following four are click probability when input angle is at
       detector H
139 % This part can be replaced by detRate1 module from previous
      program.
140 % p_hh means click probaility of detector h when angle is towards
       h
```

```
141 p_hh = 1 - exp(-mu(1)*eta(1)*eta_b/2) +pd_b;
142 p_vh = 1 - exp(-mu(1)*eta(2)*eta_b/2) +pd_b;
143 p_dh = 1 - exp(-mu(1)*eta(3)*eta_b/4)+pd_b;
144 p_ah = 1 - exp(-mu(1)*eta(4)*eta_b/4)+pd_b;
145 % The following four are click probability when input angle is at
      detector V
146 p_hv = 1 - exp(-mu(2)*eta(5)*eta_b/2)+pd_b;
147 p_vv = 1 - exp(-mu(2)*eta(6)*eta_b/2)+pd_b;
148 p_dv = 1 - exp(-mu(2)*eta(7)*eta_b/4)+pd_b;
149 p_av = 1 - exp(-mu(2)*eta(8)*eta_b/4)+pd_b;
150 % Following four are click probability when input angle is at
     detector D
151 p_hd = 1 - exp(-mu(3)*eta(9)*eta_b/4)+pd_b;
152 p_vd = 1 - exp(-mu(3)*eta(10)*eta_b/4)+pd_b;
153 p_dd = 1 - exp(-mu(3)*eta(11)*eta_b/2)+pd_b;
154 p_ad = 1 - exp(-mu(3)*eta(12)*eta_b/2)+pd_b;
155 % Following four are click probability when input angle is at
     detector A
156 p_ha = 1 - exp(-mu(4)*eta(13)*eta_b/4)+pd_b;
157 p_va = 1 - exp(-mu(4)*eta(14)*eta_b/4)+pd_b;
158 p_da = 1 - exp(-mu(4)*eta(15)*eta_b/2)+pd_b;
159 p_aa = 1 - exp(-mu(4)*eta(16)*eta_b/2)+pd_b;
160
161 %calculating the probability of detection at a particular basis
     as a
162 %function of angle
163
164 p_hv_h = (p_hh + p_vh - p_hh*p_vh)*(1-p_dh)*(1-p_ah);
165 p_da_h = (1-p_hh)*(1-p_vh)*(p_dh + p_ah - p_dh*p_ah);
166
167 p_hv_v = (p_hv + p_vv - p_hv*p_vv)*(1-p_dv)*(1-p_av);
168 p_da_v = (1-p_hv)*(1-p_vv)*(p_dv + p_av - p_dv*p_av);
169
170 p_da_d = (1-p_hd)*(1-p_vd)*(p_dd + p_ad - p_dd*p_ad);
171 p_hv_d = (p_hd + p_vd - p_hd*p_vd)*(1-p_dd)*(1-p_ad);
172
173 p_da_a = (1-p_ha)*(1-p_va)*(p_da + p_aa - p_da*p_aa);
174 p_hv_a = (p_ha + p_va - p_ha*p_va)*(1-p_da)*(1-p_aa);
```

```
175
176 % eve detection probability
177 p_r = pd_e + 1 - exp(-mu0*te*ve*eta_e);
178 p_w = pd_e + 1 - exp(-mu0*te*(1-ve)*eta_e);
179 p_x = pd_e + 1 - exp(-mu0*te*.5*eta_e);
180 %rate in presence of Eve
181 rate_h_e = .5*p_r*p_hv_h + .5*p_w*p_hv_v + .5*p_x*p_hv_d + .5*p_x
       *p_hv_a
182 rate_v_e = .5*p_w*p_hv_v + .5*p_r*p_hv_v + .5*p_x*p_hv_d + .5*p_x
       *p_hv_a
183 rate_d_e = .5*p_r*p_da_d + .5*p_w*p_da_a + .5*p_x*p_da_h + .5*p_x
       *p_da_v
184 rate_a_e = .5*p_w*p_da_d + .5*p_r*p_da_a + .5*p_x*p_da_h + .5*p_x
       *p_da_v
185
186 rate_e = (rate_h_e + rate_v_e + rate_d_e + rate_a_e)/4;
187
188 %error calculation for H
189 p_v_h = (p_vh - p_hh*p_vh/2)*(1-p_dh)*(1-p_ah);
190 p_v_v = (p_vv - p_hv*p_vv/2)*(1-p_dv)*(1-p_av);
191 p_v_d = (p_vd - p_hd*p_vd/2)*(1-p_dd)*(1-p_ad);
192 p_v_a = (p_va - p_ha*p_va/2)*(1-p_da)*(1-p_aa);
193
194 %error calculation for V
195 p_h_h = (p_hh - p_hh*p_vh/2)*(1-p_dh)*(1-p_ah);
196 p_h_v = (p_hv - p_hv*p_vv/2)*(1-p_dv)*(1-p_av);
197 p_h_d = (p_hd - p_hd*p_vd/2)*(1-p_dd)*(1-p_ad);
198 p_h_a = (p_ha - p_ha*p_va/2)*(1-p_da)*(1-p_aa);
199
200 %error calculation for d
201 p_a_h = (p_ah - p_dh*p_ah/2)*(1-p_hh)*(1-p_vh);
202 p_a_v = (p_av - p_dv*p_av/2)*(1-p_hv)*(1-p_vv);
203 p_a_d = (p_ad - p_dd*p_ad/2)*(1-p_hd)*(1-p_vd);
204 p_a_a = (p_aa - p_da*p_aa/2)*(1-p_ha)*(1-p_va);
205
206 %error calculation for a
207 p_d_h = (p_dh - p_dh*p_ah/2)*(1-p_hh)*(1-p_vh);
208 p_d_v = (p_dv - p_dv*p_av/2)*(1-p_hv)*(1-p_vv);
```

```
209 p_d_d = (p_dd - p_dd*p_ad/2)*(1-p_hd)*(1-p_vd);
210 p_d_a = (p_da - p_da*p_aa/2)*(1-p_ha)*(1-p_va);
211
212 % Error rate due to Eve
213 e_h = .5*(p_r*p_v_h + p_w*p_v_v + p_x*p_v_d + p_x*p_v_a) ;
214 e_v = .5*(p_w*p_h_h + p_r*p_h_v + p_x*p_h_d + p_x*p_h_a) ;
215 e_d = .5*(p_x*p_a_h + p_x*p_a_v + p_r*p_a_d + p_w*p_a_a) ;
216 e_a = .5*(p_x*p_d_h + p_x*p_d_v + p_w*p_d_d + p_r*p_d_a) ;
217
218 total_error = .25*(e_h + e_v + e_d + e_a);
219
220 e(1) = e_h/rate_h_e;
221 e(2) = e_v/rate_v_e;
222 e(3) = e_d/rate_d_e;
223 e(4) = e_a/rate_a_e;
224 e(5) = total_error/rate_e;
225
226 c =[];
227 if(choice==1)
228     ceq(1) = rate_ab - rate_e;
229 end
230
231 if(choice==2)
232 ceq(1) = rate_h_ab - rate_h_e;
233 ceq(2) = rate_v_ab - rate_v_e;
234 ceq(3) = rate_d_ab - rate_d_e;
235 ceq(4) = rate_a_ab - rate_a_e;
236 end
237
238 %-----=====end Constraint=====-----
```

These same programs also used in laser damage experiment.

Appendix B

Related publications

B.1 Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch

Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch

Shihan Sajeed,[1,2,*] Poompong Chaiwongkhot,[1,3] Jean-Philippe Bourgoin,[1,3] Thomas Jennewein,[1,3,4] Norbert Lütkenhaus,[1,3] and Vadim Makarov[1,2,3]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*
[2]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*
[3]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*
[4]*Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, Ontario, M5G 1Z8 Canada*

(Received 12 February 2015; revised manuscript received 4 May 2015; published 2 June 2015)

In free-space quantum key distribution (QKD), the sensitivity of the receiver's detector channels may depend differently on the spatial mode of incoming photons. Consequently, an attacker can control the spatial mode to break security. We experimentally investigate a standard polarization QKD receiver and identify sources of efficiency mismatch in its optical scheme. We model a practical intercept-and-resend attack and show that it would break security in most situations. We show experimentally that adding an appropriately chosen spatial filter at the receiver's entrance may be an effective countermeasure.

DOI: 10.1103/PhysRevA.91.062301 PACS number(s): 03.67.Dd, 03.67.Ac, 42.50.Ex, 42.79.Sz

I. INTRODUCTION

Quantum key distribution (QKD) [1,2], in theory, allows two distant parties Alice and Bob to establish a shared secret key with unconditional security [3–7]. Although a number of successful implementations of QKD have been reported [8–11] and commercialization is underway [12], the technology has yet to achieve widespread use. One important reason is that the maximum distance is still of the order of 300 km [13] in fiber-based systems. Consequently, implementation of free-space QKD utilizing ground-to-satellite links [14–22] that promises long-distance quantum communication is now a very attractive field of research.

Implementation imperfections have enabled a number of successful attacks on QKD [23–31]. The main reason behind this is the deviation of the actual behavior of the devices from the ideal expected behavior. Thus, to guarantee the security, it is of utmost importance to scrutinize the practical device behavior for possible deviations. One such source of deviation in free-space QKD can be the assumed symmetry of detection efficiency among all received quantum states in Bob's detector [28–30,32,33]. If a deviation from this assumption exists, an adversary Eve can send light to Bob in different spatial modes so that one of his detectors has a relatively higher probability to click than the other detector(s) [34]. In this way, she can exploit the mismatch in efficiency and make Bob's measurement outcome dependent on his measurement basis and correlated to Eve, which breaks the assumptions of typical security proofs. In this work, we investigate how crucial this can be to the security of QKD.

We study a receiver designed for polarization encoding free-space QKD, described in Sec. II. We test it in Sec. III by sending an attenuated laser beam to the receiver with various angle offsets and recording the relative detection probability in each channel, with the goal being to find incidence angles with high efficiency mismatch. With these data, we show in Sec. IV by numerical modeling that an eavesdropper attack exists that enables Eve to steal the secret key. We discuss countermeasures in Sec. V and conclude in Sec. VI.

II. QUANTUM-KEY-DISTRIBUTION SYSTEM UNDER TEST

A free-space QKD receiver typically employs a telescope to reduce the size of a collimated beam, followed by a nonpolarizing beam splitter to randomly choose between two measurement bases. It is followed by polarization beam splitters and single-photon detectors to measure photons in the four states of polarization: horizontal (H), vertical (V), $+45^\circ$ (D), and -45° (A) [14–22]. The receiver we test is a prototype for a quantum communication satellite [36], operating at 532 nm wavelength [Figs. 1(a) and 1(c)]. Its telescope consists of a focusing lens L1 (diameter 50 mm, focal length $f = 250$ mm; Thorlabs AC508-250-A) and collimating lens L2 ($f = 11$ mm; Thorlabs A397TM-A). The collimated beam of $\lesssim$2 mm diameter then passes through a 50:50 beam splitter BS (custom pentaprism [36]) and pairs of polarization beam splitters PBS1 and PBS2 (Thorlabs PBS121). PBS2 increases the polarization extinction ratio in the reflected arm of PBS1. Lenses L3 (Thorlabs PAF-X-18-PC-A) focus the four beams into 105-μm-core-diameter multimode fibers (Thorlabs M43L01) leading to single-photon detectors (Excelitas SPCM-AQRH-12-FC).

Long-distance free-space QKD receivers are multimode for two reasons. First, propagation of Alice's beam, initially single mode, through a turbulent atmosphere splits it into multiple spatial modes [37]. Second, the finite precision and speed of real-time angular tracking of Alice's beam requires that Bob accepts multiple spatial modes in a certain acceptance angle [18,19,22,38]. The use of single-mode fibers under these conditions would lead to additional coupling losses $\gtrsim$10 dB [39] if the system does not include appropriate (and often expensive) adaptive correction optics [37]. Therefore, multimode fibers and detectors with larger area are generally preferred because they allow good collection efficiency without increasing complexity and cost.

*ssajeed@uwaterloo.ca

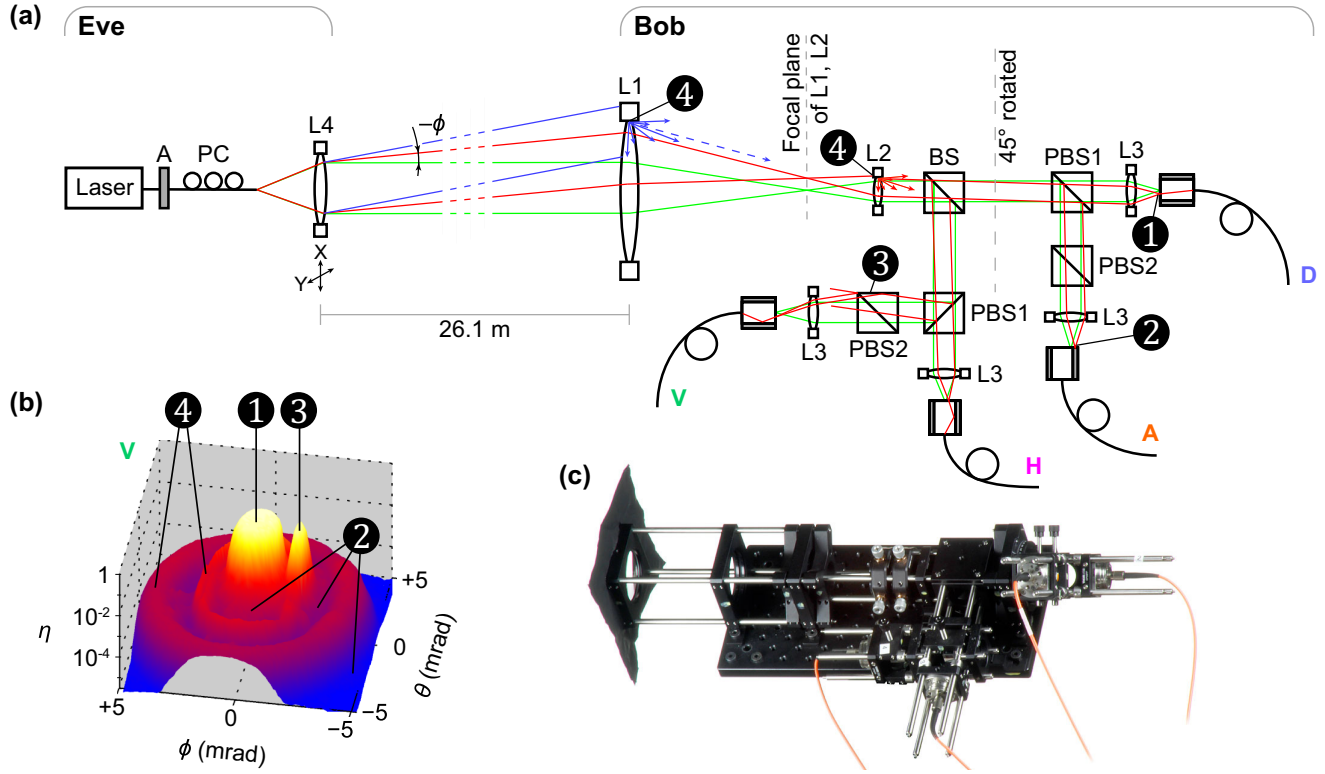

FIG. 1. (Color online) Experimental setup. (a) Scheme of the experimental apparatus, top view (drawing not to scale). Eve's source consists of a fiber-coupled 532 nm laser, attenuator *A*, polarization controller PC, and a collimating lens mounted on a two-axis motorized translation stage. The latter allows us to change the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. Green (light gray) marginal rays parallel to the optical axis denote the original alignment of Alice's beam to Bob. Red and blue (dark gray) marginal rays show a scanning beam from Eve tilted at an angle (ϕ,θ) relative to the original beam. Features ❶–❹ mark different transmission paths for light inside Bob. (b) Normalized detection efficiency η in channel *V* versus the illumination angle (ϕ,θ). This scan was taken to show the features clearly by placing Eve at a closer distance. (c) Photograph of Bob's receiver. The actual distance between facing surfaces of L2–BS is 42 mm, BS–PBS is 166 mm, PBS1–L is 331 mm, PBS1–PBS is 245 mm, PBS2–L is 310 mm in channel *A* and 5 mm in channel *V*.

III. EXPERIMENT

In order to exploit the mismatch in efficiency, Eve needs to know the mismatch for the four detectors as a function of the input angle. Hence, our first step was to scan Bob's receiver for possible efficiency mismatch. Eve's source [Fig. 1(a)] consists of a 532nm laser coupled into single-mode fiber, attenuator A, polarization controller PC, and a collimating lens L4 (Thorlabs C220TME-A) mounted on a two-axis motorised translation stage (Thorlabs MAX343/M). In Fig. 1(a), green (light gray) marginal rays denote the initial alignment from Eve, replicating the alignment from Alice to Bob. This is the initial position of the translation stage $\phi = \theta = 0$. As we moved the stage in the transverse plane, it changed the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. This is shown by red (dark gray) marginal rays in Fig. 1(a), representing a beam from Eve coming at an angle (ϕ,θ) relative to the initial beam.

Before scanning, the optics in Bob's apparatus was aligned to maximize coupling into all four detectors at the normal incidence, which is the standard alignment procedure for QKD. Note that many free-space QKD systems employ a real-time tracking system to maintain this initial alignment [18,19,22,38]. We then started the scanning procedure that involved first changing the outgoing-beam's angle (ϕ,θ), and then recording the corresponding count rate at all four detectors of Bob. For each data point, we used an integration time of 1 s. Our scan consisted of approximately 100×100 data points in a square matrix covering the whole clear aperture of Bob's front lens L1. Then during postprocessing, for each data point for each detector, we subtracted the corresponding detector's background count rate, and then normalized it by dividing by the maximum count rate in that detector.

At first, we did a preliminary scan using optical power meters (Thorlabs PM200 with S130C head) that revealed several features, highlighted in Fig. 1(b). Around $\phi = \theta = 0$, maximum light coupling resulted in the central peak ❶. With increasing scanning angle, the focused beam started missing the fiber core, and the detector count dropped off ❷. A region was found when the beam reflected off a polished edge of PBS2 back into the fiber core, causing the peak ❸. Increasing the angle further made the beam hit the anodized aluminum mount of L1 and possibly edges of other lens mounts and round elements in the optical assembly. It was scattered at these edges, producing two ring-like features ❹. Beyond these features, there were no noticeable

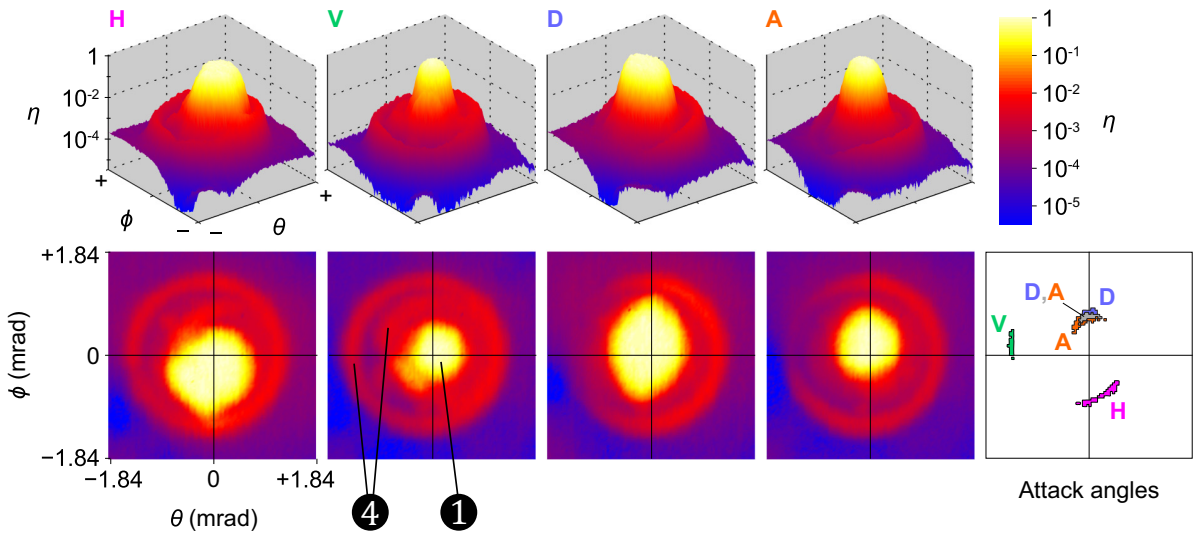

FIG. 2. (Color online) Angular efficiency scan of the receiver, and points of interest. Four pairs of plots **H, V, D, A** shown in both three-dimensions and two dimensions represent normalized detection efficiency in the four receiver channels versus illuminating beam angle (ϕ,θ). The angle $\phi = \theta = 0$ is the initial angle of QKD operation. The last plot shows angle ranges with a high mismatch, which is usable in our attack.

power reading, as the beam completely missed the receiver aperture.

We then adjusted the receiver setup to minimize the peak ❸ and performed final scans at a distance of 26.1 m by using Bob's single-photon detectors (Excelitas SPCM-AQRH-12-FC). During these scans, the beam at L1 was Gaussian shaped with 9 mm width (at $1/e^2$ peak intensity). The scans were done in 38.3 μrad steps covering a ± 1.84 mrad range, corresponding to lateral displacement of ± 48 mm at L1. Figure 2 shows the normalized detection efficiency in all four receiver channels as a function of (ϕ,θ). Most of the original features are still visible. However, outside the narrow central range of angles close to $\phi = \theta = 0$, individual-channel efficiencies vary independently. Also, the size and shape of the central peak is significantly different between channels. This was impossible to identify during the normal alignment procedure. This effect can be attributed to imprecise focusing, optical path length difference between the arms, off-centered alignment of lenses, mode-dependent bending loss in fibers, and individual variations in components. These may have also caused the efficiency at one side of the outer ring to be higher. Because of these reasons, there exist angles such that, if photons are sent at those angles, one channel has a much higher click probability than the rest.

IV. ATTACK MODEL

To emphasize the security threat, it is useful to model an attack that exploits the discovered side channel. One possible attack is the faked-state attack [30,40], which is an intercept-and-resend attack in which Eve attempts to deterministically control Bob's basis choice and detection outcome. We model a practical faked-state attack by using the data obtained and the following assumptions: Alice and Bob perform the non-decoy-state Bennett–Brassard 1984 (BB84) protocol using polarization encoding. Alice emits weak coherent pulses with mean photon number μ equal to the Alice–Bob line transmittance [5]. Whenever Bob registers a multiple click, he performs a squashing operation (double-click in one basis is mapped to a random value in that basis, while multiple clicks in different bases are discarded) [41–43]. Alice and Bob also monitor total sifted key rate, and quantum bit error ratio (QBER). Eve has information about Bob's receiver characteristics described above and only uses devices available in today's technology. She intercepts photons at the output of Alice, using an active basis choice and superconducting nanowire detectors, with overall detection efficiency $\eta_e = 0.85$ and dark-count probability $<10^{-9}$ per bit slot [44]. Then, a part of her situated close to Bob regenerates the measured signal and sends it to Bob. We assume that Alice–Bob and Alice–Eve fidelity $F = 0.9831$ [36], while Eve–Bob experimentally measured $F = 0.9904$. Here fidelity refers to the probability that a polarized photon will emerge from the PBS at the correct path, which is related to visibility by $F = (1 + \text{visibility})/2$. We also confirmed experimentally that Eve–Bob fidelity is preserved at all illumination angles shown in Fig. 2.

From Eve's point of view, she wants to maximize the detection probability when Bob measures in a compatible (i.e., same as her) basis to maximize Eve–Bob mutual information. Also, she wants to minimize Bob's detection probability in a noncompatible basis, to minimize QBER. Let $\eta_i(j)$ be the efficiency of Bob's ith channel $(i \in \{h,v,d,a\})$ given that incoming light is $j \in \{H,V,D,A\}$ polarized. Thus, to find attack points for the jth polarization, we choose angles that have higher values of $\eta_j(j)$ and $\delta_j(j) = \min\{\frac{\eta_j(j)}{\eta_{nc0}(j)}, \frac{\eta_j(j)}{\eta_{nc1}(j)}\}$, where η_{nc0} and η_{nc1} are the normalized efficiencies of the two detectors in the noncompatible basis. Our experimental attack angles are shown in the rightmost plot in Fig. 2. For example, the H attack angles were composed of points for which $\eta_h(H) \geqslant 0.2$ and $\delta_h(H) \geqslant 75$. Similarly, for the V, D, and A attack angles, $\eta_v(V) \geqslant 0.002$, $\delta_V \geqslant 8$; $\eta_d(D) \geqslant 0.4$, $\delta_D \geqslant 80$; $\eta_a(A) \geqslant 0.1$, $\delta_A \geqslant 20$. The thresholds used here

to find the attack angles were not optimal and were picked manually.

To derive the key rate and QBER formula in Eve's presence, we start with a system with only Eve and Bob. Let us consider Eve sending an H-polarized pulse to Bob within the attack angles H. Before squashing, the raw click probability $p_i(j)$ that detector i in Bob clicks given that Eve has sent j-polarized light is

$$\begin{aligned} p_h(H) &\approx c_h + 1 - \exp\left(-\frac{\mu_H F \eta_h(H)}{2}\right), \\ p_v(H) &\approx c_v + 1 - \exp\left(-\frac{\mu_H (1-F) \eta_v(H)}{2}\right), \\ p_{d(a)}(H) &\approx c_{d(a)} + 1 - \exp\left(-\frac{\mu_H \eta_{d(a)}(H)}{4}\right), \end{aligned} \tag{1}$$

where μ_H is Eve's mean photon number and c_i is Bob's background click probability per bit slot in ith channel. The probability $P_{hv}(H)$ that, after squashing Bob measures in the HV basis, given that Eve has sent an H-polarized pulse, is composed of three events: when only detector H clicks, when only detector V clicks, or when both click. It can be written as

$$\begin{aligned} P_{hv}(H) = {} & [1 - p_d(H)][1 - p_a(H)] \\ & \times [p_h(H) + p_v(H) - p_h(H) p_v(H)]. \end{aligned} \tag{2}$$

Let us now include Alice into the picture. Consider that Alice sends an H-polarized pulse, and Eve intercepts it. Let $P_c^e \approx \frac{1}{2}(1 - e^{-\mu F \eta_e}) e^{-\mu(1-F)\eta_e}$ and $P_w^e \approx \frac{1}{2} e^{-\mu F \eta_e}(1 - e^{-\mu(1-F)\eta_e})$ be the probability that Eve measures in the compatible basis (i.e., the same basis as Alice) and gets a click only in the correct and wrong detector respectively. Let $P_{nc}^e \approx \frac{1}{2}(1 - e^{-\frac{\mu\eta_e}{2}}) e^{-\frac{\mu\eta_e}{2}}$ be the probability that she measures in the noncompatible basis (different basis than Alice's) and gets a click in a single detector. The sifted key rate given Alice has sent H-polarized light is

$$\begin{aligned} R_e(H) \approx {} & P_c^e P_{hv}(H) + P_w^e P_{hv}(V) \\ & + P_{nc}^e [P_{hv}(D) + P_{hv}(A)] \\ & + \left(1 - P_c^e - P_w^e - 2P_{nc}^e\right)(c_h + c_v - c_h c_v). \end{aligned} \tag{3}$$

An error can occur when Eve measures Alice's signal in a noncompatible basis or when Eve measures in a compatible basis but Bob measures a wrong value owing to imperfect fidelity or dark count. Hence, the error rate conditioned on Alice sending H-polarized light is

$$\begin{aligned} E_H \approx {} & P_c^e P_v(H) + P_w^e P_v(V) + P_{nc}^e [P_v(D) + P_v(A)] \\ & + \left(1 - P_c^e - P_w^e - 2P_{nc}^e\right)\left(c_v - \frac{c_v c_h}{2}\right), \end{aligned} \tag{4}$$

where $P_i(j)$ is the probability that Bob measures the value i after squashing, given that Eve has sent j-polarized light. For example,

$$P_v(H) = \left[p_v(H) - \frac{p_h(H) p_v(H)}{2}\right][1 - p_d(H)][1 - p_a(H)]. \tag{5}$$

Sifted key rates and errors in Eve's presence [Eqs. (3) and (4)] conditioned on V, D, A polarizations sent by Alice can be calculated similarly. The total sifted key rate and QBER in Eve's presence becomes

$$R_e = \frac{1}{4} \sum_{j=H,V,D,A} R_e(j), \quad \mathrm{QBER}_e = \frac{1}{4R_e} \sum_{j=H,V,D,A} E_j. \tag{6}$$

The only free parameters left for Eve to manipulate are the mean photon numbers of her signal. Knowing the angular scanning data, Eve can use a numerical optimization to find values of $\mu_H, \mu_V, \mu_D, \mu_A$ that minimize QBER_e while keeping $R_e = R_{ab}$, where R_{ab} is Bob's sifted key rate without Eve. Our numerical optimization achieves this for Alice–Bob channel loss $\geqslant 3$ dB if they are willing to accept a slight increase of QBER by less than 0.7% (see Fig. 3). Here we assumed Bob's detector parameters as measured by us: efficiency at $\phi = \theta = 0$ was 0.4 in all four channels, and individual detector background count probabilities were in the range of 430×10^{-9} to 1560×10^{-9} per 1 ns coincidence window. These optimization results are realistic conditions for a successful attack on most communication channels [14–17,19,20,22,36] Note that the distance Eve–Bob can be increased without affecting attack performance, by replacing Eve's illuminator with four collimators oriented at the required attack angles.

We went further and imposed an additional constraint on Eve to make $R_e(H) = R_e(V) = R_e(D) = R_e(A) = R_{ab}$. Our optimization shows that it is still possible for Eve to pick appropriate mean photon numbers and successfully attack the system with resultant QBER $<6.82\%$ in $3 - 15$ dB line loss range (Fig. 3). Similar QBER values are typical for outdoor channels, because of background light. Eve could shield Bob from the latter to hide QBER resulting from her attack.

We would like to point out that the attack angles depend on the way the setup is constructed, the imperfections of each individual sample of component, and each individual alignment procedure. In other words, no two setups are identical, even if they are produced in the same assembly line,

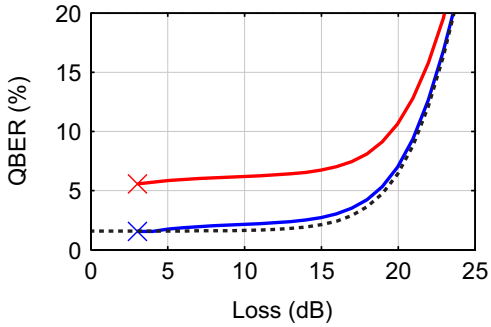

FIG. 3. (Color online) Modeled QBER observed by Bob versus line loss. The dotted curve shows QBER without Eve. At lower line loss, the QBER is due to imperfect fidelity, while at higher line loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER_e under our attack when only the total Bob's sifted key rate R_{ab} is matched. The upper solid curve (red) additionally keeps his four channel rates equal.

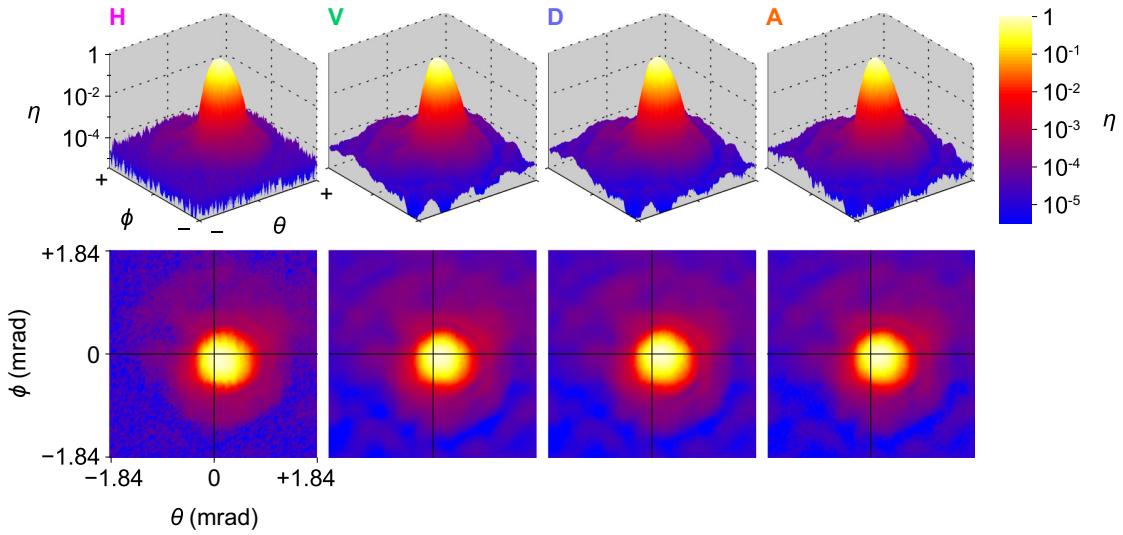

FIG. 4. (Color online) Angular efficiency scan of the receiver after a 25-μm-diameter pinhole (Thorlabs P25S) is placed in the focal plane of L1, L2 [Fig. 1(a)]. No detectable mismatch between channels was found under tight search conditions $\eta_i(j) \geqslant 0.001$ and $\delta_i(j) \geqslant 4$.

and they will generally have different attack angles. However, from a theoretical point of view, in quantum cryptography it is assumed from Kerckhoffs' principle [45] that, except for the keys themselves, Eve has knowledge about all other parameters in the system. It is thus a valid assumption that she knows the attack angles. From a practical point of view, Eve may try techniques proposed in Ref. [40]. She may replace a small fraction of the signal states with faked states at different spatial angles, then listen to the classical communication to get an estimate of the efficiency of Bob's detectors at those angles. In this way she may gradually improve her estimate on the mismatch without causing excessive QBER. When she has enough information on the statistics of the mismatch, she can launch her full-fledged attack.

V. COUNTERMEASURES

In our attack, by sending lights at different angles, Eve has broken a fundamental assumption of security proofs that detection probabilities are independent of detection basis [46,47]. We propose to restore this assumption by placing a spatial filter (pinhole) at the focal plane of Bob's L1 and L2 [Fig. 1(a)]. Spatial filtering is sometimes done before the beam splitters to increase signal-to-background ratio in the channel [17,18,21]; however, it has not been characterized as a security countermeasure. We performed scanning with 100-, 75-, and 25-μm-diameter pinholes and found that decreasing the pinhole diameter gradually reduces the mismatch. The 25-μm-diameter pinhole eliminated any visible mismatch (Fig. 4) even though we reduced our search parameters to $\eta_i(j) \geqslant 0.001$ and $\delta_i \geqslant 4$. This pinhole provides Bob's field of view of 100 μrad, which does not reduce his efficiency with turbulent atmospheric channels [19]. Hence, we conclude that a 25 μm pinhole may be an efficient countermeasure for the current setup.

Note that, in Refs. [29,48], a detector-scrambling strategy was proposed that might be an effective countermeasure against efficiency mismatch attacks for single-photon qubits. However, it is not clear how effective that countermeasure is, when one considers that the detectors operate on optical modes, not on single-photon signals. This can be a future study.

VI. CONCLUSION

Our analysis implies that data obtained during a QKD session can be explained by an intercept-resend attack exploiting the spatial mode side-channels. Therefore, there is no post-processing or privacy amplification that can eliminate Eve's knowledge without sacrificing all keys [49]. Although our practical attack should work, and the physical countermeasure seems promising, there is still room for improvement on both the attack scheme and countermeasures. Eve can employ more attack angles or combine this attack with some other suitable attack schemes, to increase the number of her free parameters. Alice and Bob can make this harder by monitoring more parameters. We expect that our attack can be conducted also in the related decoy-state protocol [50], although the requirement to match the correct decoy statistics will modify the parameter regime where it will be effective. Another possible future study is to fully implement the present attack under realistic outdoor-channel conditions.

Note added. Recently, we became aware of a similar work [35].

ACKNOWLEDGMENTS

We thank Y. Zhang and M. Mosca for discussions. This work was supported by the U.S. Office of Naval Research, Industry Canada, CFI, Ontario MRI, NSERC, Canadian Space Agency, and CryptoWorks21. P.C. acknowledges support by a Thai DPST scholarship. J.-P.B. and T.J. acknowledge support from FED DEV.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[5] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[6] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).

[7] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[8] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, J. Cryptol. **5**, 3 (1992).

[9] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[10] 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, Phys. Rev. Lett. **98**, 010504 (2007).

[11] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[12] Commercial QKD systems are available for purchase, as of 2015, from at least three entities: ID Quantique (Switzerland), http://www.idquantique.com; SeQureNet (France), http://www.sequrenet.com; and the Austrian Institute of Technology (Austria), http://www.ait.ac.at/

[13] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).

[14] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).

[15] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).

[16] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, Proc. SPIE **4917**, 25 (2002).

[17] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).

[18] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, Fortschr. Phys. **54**, 840 (2006).

[19] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).

[20] C. Erven, C. Couteau, R. Laflamme, and G.Weihs, Opt. Express **16**, 16840 (2008).

[21] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045007 (2009).

[22] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nat. Photonics **7**, 382 (2013).

[23] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).

[24] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).

[25] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).

[26] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).

[27] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[28] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[29] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Info. Comput. **7**, 73 (2007).

[30] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).

[31] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001); N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[32] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[33] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).

[34] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Info. Comput. **9**, 131 (2009).

[35] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, IEEE J. Quantum Electron. **21**, 1 (2015).

[36] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. Lütkenhaus, and T. Jennewein (unpublished).

[37] R. Tyson, *Principles of Adaptive Optics*, 3rd ed. (CRC Press, Boca Raton, Florida, 2010).

[38] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, Opt. Express **12**, 2011 (2004).

[39] H. Takenaka, M. Toyoshima, and Y. Takayama, Opt. Express **20**, 15301 (2012).

[40] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[41] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[42] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[43] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **89**, 012325 (2014).

[44] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photonics **7**, 210 (2013).

[45] A. Kerckhoffs, J. des Sciences Militaires **IX**, 5 (1883).

[46] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[47] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[48] T. F. da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, IEEE J. Sel. Top. Quantum Electron. **21**, 1 (2015).

[49] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[50] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

B.2 Spatial-mode detector efficiency mismatch security loophole in free-space QKD (QCRYPT2015 Abstract)

Spatial-mode detector efficiency mismatch security loophole in free-space QKD

Poompong Chaiwongkhot,[1,2] Shihan Sajeed,[1,3] Jean-Philippe Bourgoin,[1,2]
Thomas Jennewein,[1,2,4] Norbert Lütkenhaus,[1,2] and Vadim Makarov[1,2,3]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

Introduction. Recent studies show that free-space quantum key distribution has an ability to distribute secret keys over hundreds of kilometers above the ground. In addition, with current technology it is the only channel that can be employed for quantum key distribution on the global scale, via satellite-based systems. Although QKD protocols and security analysis have been developed in theory, deviation of the actual behavior of the devices from the ideal behavior expected in theory presents a major challenge in physical implementation. Thus, to guarantee the security, it is of utmost importance to scrutinize the practical device behaviors for possible deviations, and develop necessary countermeasures to any loophole that can be exploited.

In this submission based on our recent preprint [1], we focus on one such deviation inherent to free-space QKD receivers. We experimentally characterize it, and propose and characterize a countermeasure. We explore a violation of detection efficiency symmetry among all quantum states in Bob's receiver. If this violation exists, an adversary Eve can send light to Bob in different spatial modes so that one detector has a relatively higher probability of click than the other detectors. In this way, she can exploit the mismatch in efficiency [2] and make Bob's measurement outcome dependent on his measurement basis and correlated to Eve, which breaks the assumptions of typical security proofs. In this work, we investigate how crucial this can be to the security of QKD. (While finishing our paper, we became aware of a recent similar work [3].)

We study a receiver designed for polarization encoding free-space QKD, described in the experiment section. We begin by sending an attenuated laser beam to the receiver with various angle offsets and recording the relative detection probability in each channel, to find incidence angles with high efficiency mismatch. With these data, we show by numerical modeling that an eavesdropper attack exists that enables Eve to steal the secret key. Lastly, we discuss a countermeasure.

Experiment. The receiver we test is a prototype for a quantum communication satellite [4] with polarization encoding. It is a passive basis choice receiver operating at 532 nm wavelength [Fig. 1(a,c)]. 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**, $+45°$ **D** and $-45°$ **A**. In order to exploit the mismatch in efficiency, Eve needs to know the efficiency of the four detectors as a function of Bob's input illumination angle. Hence, our first step was to scan Bob's receiver for possible efficiency mismatch. Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens L4 mounted on a two-axis motorised translation stage. In Fig. 1a, green marginal rays denote the initial alignment from Eve, replicating the alignment from Alice to Bob. As we moved the stage in the transversal plane, it allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. This is shown by the red marginal rays in Fig. 1, representing a beam from Eve coming at an angle (ϕ, θ) relative to the reference beam.

At first, we did a preliminary scan using optical power meters that revealed several features which should be causes of efficiency mismatch, highlighted in Fig. 1(b). Around $\phi = \theta = 0$, maximum light coupling resulted in the central peak ❶. With increasing scanning angle, the focused beam started missing the fiber core, and the detector count dropped off ❷. A region was found when the beam reflected off the polished edge of PBS2 back into the fiber core, causing the peak ❸. Increasing the angle further made the beam hit the anodized aluminum mount of L1 and possibly edges of other lens mounts and round elements in the optical assembly. It was scattered at these edges, producing two ring-like features ❹. Beyond these features, there were no noticeable power readings, as the beam completely missed the receiver aperture.

We then adjusted the receiver setup to minimize peak ❸, and performed final scans at 26.1 m distance using Bob's single-photon detectors. Before scanning, the optics in Bob's apparatus was aligned to maximize coupling into all four detectors at normal incidence, which is the standard alignment procedure for QKD. We then started the scanning procedure that involved first, changing the outgoing beam's angle $\{\phi, \theta\}$, and then recording the corresponding count rate at all four detectors of Bob. Then during post-processing, for each data point for each detector, we subtracted the corresponding detector's background count rate, and then normalized it by dividing by the maximum count rate in that detector. The result is shown in Fig. 2.

Attack model. We numerically model and optimize a practical faked-state attack, using our experimental data and the following assumptions. Alice and Bob perform

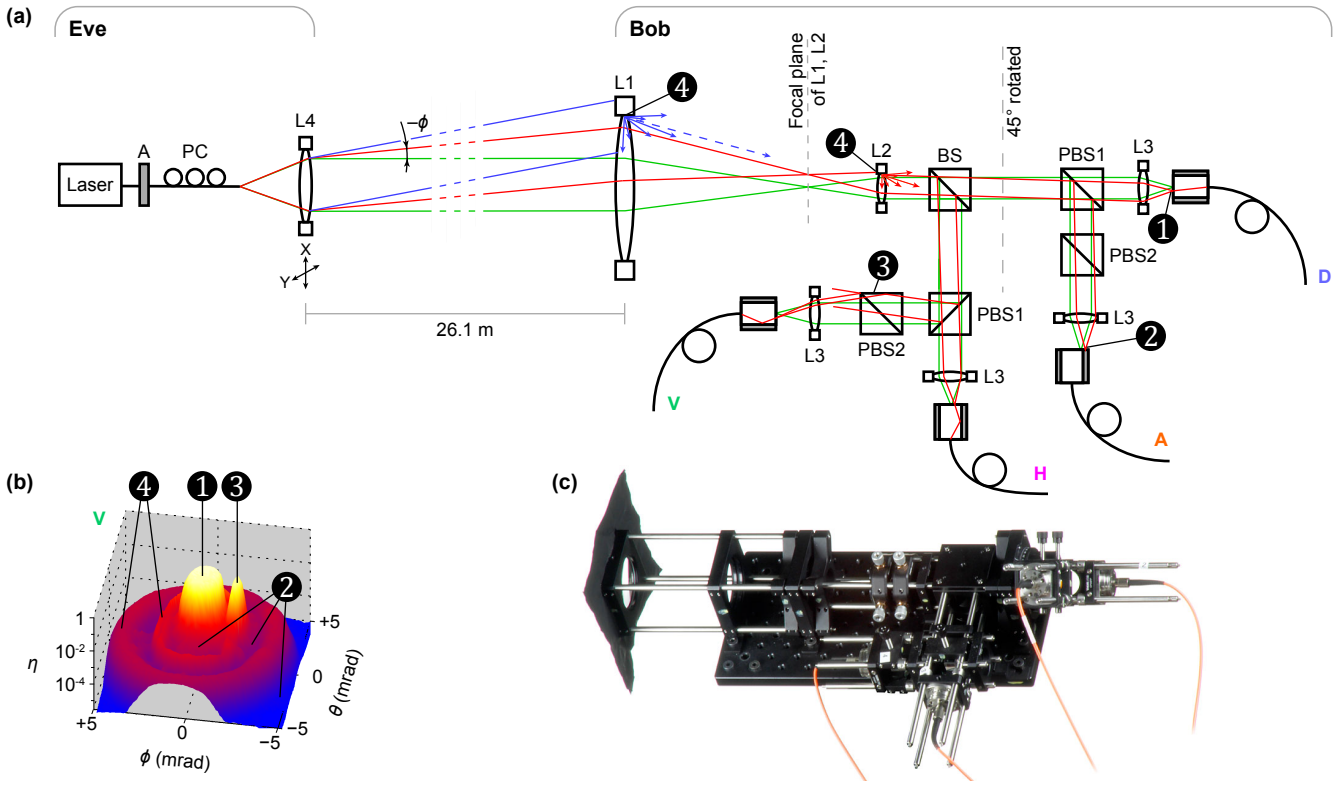

FIG. 1. Experimental setup. (a) Scheme of the experimental apparatus, top view (drawing not to scale). Eve's source consists of a fiber-coupled 532 nm laser, attenuator A, polarization controller PC, and a collimating lens mounted on a two-axis motorised translation stage. The latter allows changing the beam's incidence angle and lateral displacement at Bob's front lens L1 simultaneously. Green marginal rays denote the original alignment of Alice's beam to Bob. Red and blue marginal rays show a scanning beam from Eve tilted at an angle (ϕ, θ) relative to the original beam. Features ❶–❹ mark different transmission paths for light inside Bob. (b) Normalized detection efficiency η in channel V versus the illumination angle (ϕ, θ). This scan was taken to show the features clearly by placing Eve at a closer distance. (c) Photograph of Bob's receiver.

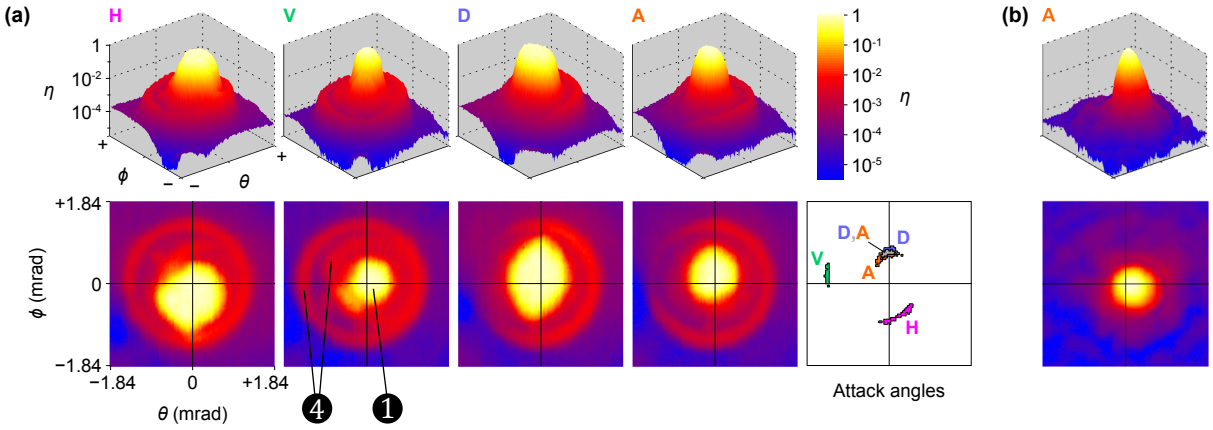

FIG. 2. Angular efficiency scan of the receiver, and points of interest. (a) Four pair of plots **H, V, D, A** shown in both 3D and 2D represent normalized detection efficiency in the four receiver channels versus illuminating beam angle (ϕ, θ). The angle $\phi = \theta = 0$ is the initial angle of QKD operation. The last plot shows angle ranges with a high mismatch, usable in our attack. (b) An example of scanning result in polarization channel **A** with 25 µm diameter pinhole at the focal plane of L1. The plots for the other three receiver channels in this case were very similar; all features that caused the efficiency mismatch disappeared.

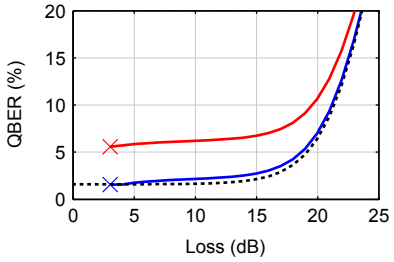

FIG. 3. Modeled QBER observed by Bob versus line loss. The dotted curve shows QBER without Eve. At lower line loss, the QBER is due to imperfect fidelity, while at higher line loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER_e under our attack when only the total Bob's sifted key rate R_e is matched. The upper solid curve (red) additionally keeps his four channel rates equal.

non-decoy-state Bennett-Brassard 1984 (BB84) protocol using polarization encoding. Eve intercepts and measures every signals from Alice using an active basis choice receiver with high-efficiency single-photon detectors. For each successful detection, Eve sends to Bob a faked-state signal which is a weak coherent pulse with polarization matching her measurement result. For each of the four polarizations, she sends at a specific angle and mean photon number. Our next task is to find these parameters, with the goal of Eve to maintain Bob's detection rate and minimize QBER.

Our experimental attack angles are shown in the rightmost plot in Fig. 2(a). For example, the H attack angles were composed of points for which the probability of detection in H channel was 75 times more than the other two non-orthogonal channels (D and A), and the normalized detection probability was at least 0.25. The thresholds used here to find the attack angles were not optimal, and were picked manually. With this information, the detection rate and QBER of Bob can be calculated. From these data, we then ran an optimization program to find optimal mean photon numbers for each attack angle. This optimization was conditioned to minimize QBER and match the total detection rate expected by Alice and Bob (calculated from the parameters at the reference angle).

Our optimization shows that it is possible for Eve to pick appropriate mean photon numbers and successfully attack the system for Alice–Bob channel loss ≥ 3 dB if they are willing to accept a slight increase of QBER by less than 0.7% (see Fig. 3), if Alice and Bob monitor only the total key rate. Furthermore, the attack is still successful at QBER $< 6.82\%$ in 3–15 dB line loss range even when Alice and Bob monitor the equality of detection rates in each channel. Similar QBER values are typical for outdoor channels, because of background light. Eve could shield Bob from the latter to hide QBER resulting from her attack.

Countermeasure. In our attack, Eve has broken a fundamental assumption of security proofs: detection probabilities are independent of detection basis. We propose to restore this assumption by placing a spatial filter (pinhole) at the focal plane of Bob's L1 and L2 [Fig. 1(a)]. We have tested several pinhole sizes, and found that 25 μm diameter pinhole eliminates any visible mismatch as shown in Fig. 2(b). Hence, we conclude that a 25 μm pinhole may be an efficient countermeasure for the current setup.

Discussion and conclusion. Since our analysis implies that data obtained during a QKD session can be explained by an intercept-resend attack exploiting the spatial mode side-channels, there is no postprocessing or privacy amplification that can eliminate Eve's knowledge without sacrificing all key [5]. Although our practical attack should work, and the physical countermeasure seems promising, there is still room for improvement on both the attack scheme and countermeasures. The effect of atmospheric turbulence on both scanning and signal transmission needs to be studied. The resilience of pinhole against laser damage needs to be tested. At last, all these tests need to be performed again on the compact receiver with integrate optics that is going to be installed in the satellite.

Our study summarised here [1] is an excellent example of deviation in device's behavior that is not predicted in theory but affects the security of the protocol. The practical results of this study are applicable to most free-space quantum communication systems. We hope that this work will emphasise the necessity of investigating physical side-channels in every implementation of QKD. Iterations of finding vulnerabilities and testing countermeasures should eventually guarantee the high level of security promised by the theory of QKD.

[1] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, arXiv:1502.02785 [quant-ph].
[2] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).
[3] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, IEEE J. Quantum. Electron. **21**, 6600905 (2015).
[4] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. Lütkenhaus, and T. Jennewein, (manuscript in preparation).
[5] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

B.3 Laser damage creates backdoors in quantum communications

Laser damage creates backdoors in quantum communications

Vadim Makarov,[1,2,3,4,a)] Jean-Philippe Bourgoin,[2,3] Poompong Chaiwongkhot,[2,3] Mathieu Gagné,[5] Thomas Jennewein,[2,3,6] Sarah Kaiser,[2,3] Raman Kashyap,[5] Matthieu Legré,[7] Carter Minshull,[2] and Shihan Sajeed[2,4]

[1)]*The rest of the authors are listed alphabetically.*

[2)]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

[3)]*Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

[4)]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

[5)]*Department of Engineering Physics and Department of Electrical Engineering, École Polytechnique de Montréal, Montréal, QC, H3C 3A7 Canada*

[6)]*Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*

[7)]*ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Geneva, Switzerland*

(Dated: 12 October 2015)

Quantum communication protocols such as quantum cloud computing[1], digital signatures[2], coin-tossing[3], secret-sharing[4], and key distribution[5], using similar optical technologies, claim to provide unconditional security guaranteed by quantum mechanics. Among these protocols, the security of quantum key distribution (QKD) is most scrutinized and believed to be guaranteed as long as implemented devices are properly characterized and existing implementation loopholes are identified and patched[6,7]. Here we show that this assumption is not true. We experimentally demonstrate a class of attacks based on laser damage[8], capable of creating new security loopholes on-demand. We perform it on two different implementations of QKD and coin-tossing protocols, and create new information leakage side-channels. Our results show that quantum communication protocols cannot guarantee security alone, but will always have to be supported by additional technical countermeasures against laser damage.

Cryptography, an art of secure communication, has traditionally relied on either algorithmic or computational complexity[9]. Even the most state-of-the-art classical cryptographic schemes do not have a strict mathematical proof to ascertain their security. With the advance of quantum computing, it may be a matter of time before the security of the most widely used public-key cryptography protocols is broken[10]. However, QKD (popularly known as quantum cryptography)[5] allows remote key distribution with unconditional security[6,7]. Its complete security model is based on the laws of quantum mechanics, security proofs and model of equipment. When we go from theory to practice, the practical behaviour of the implemented equipment often deviates from its modeled behaviour, leading to a compromise of security[11–16]. However, it is widely assumed that as long as these deviations are properly characterized and security proofs are updated accordingly[7,17], QKD can provide unconditional security. In this work we show that this is not always true for QKD and other secure quantum communication protocols. Even if a system is perfectly characterized and deviations are included into the security proofs, an eavesdropper can still create a new deviation on-demand, unlike in classical cryptography schemes.

The reason behind this is that in classical communication systems, the security-critical parts can be physically separated from the communication channel, thus making them isolated from physical access and alteration by the eavesdropper[18]. However, the front-end of a quantum communication system is essentially an analog optical system connected to the channel, and easily accessible by an eavesdropper. The latter may shoot a high-power laser from the communication channel to damage a security-critical component of the system, rendering the system insecure[8]. To verify this possibility, we perform laser damage on two completely different widely used implementations: a commercial fiber-optic system for QKD and coin-tossing with phase-encoded qubits[19,20], and a free-space system for QKD with polarization-encoded qubits[21]. In both systems, the damage opens up a new side-channel, which can compromise the security of QKD even with today's technology[16,22].

Although we have only tested implementations of QKD and coin-tossing, the security of other quantum communication protocols seems to rely on broadly similar assumptions, and they use similar optical technology. For example, in quantum cloud computing[1] and digital signatures[2], client's and Alice's state preparation may be eavesdropped on. Quantum implementations of oblivious transfer[23] and relativistic bit commitment[24] are based on modified QKD setups and thus suffer from the same vulnerabilities. However the implementations and security criteria of those protocols are less developed, making their battle-testing a future task.

Laser damage in fiber-optic quantum communication system. To demonstrate the threat of laser damage in a fiber-optic quantum communication implementation, we chose a plug-and-play QKD[19] and loss-tolerant quantum coin tossing (QCT)[3]. Both were implemented using a commercial system Clavis2 from ID Quantique[20]. In both cases, Bob sends bright light pulses to Alice. Alice randomly encodes her secret bits

[a)]Electronic mail: makarov@vad1.com

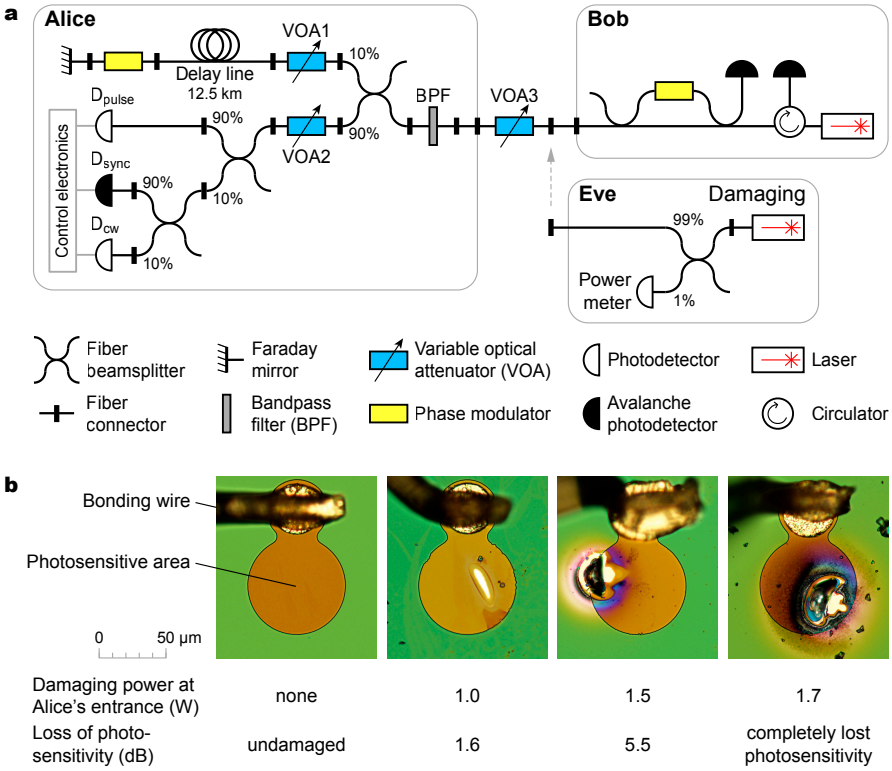

FIG. 1. **Attack on fiber-optic system Clavis2.** **a**, Experimental setup. The system consists of Alice and Bob connected by a lossy fiber communication channel (simulated by variable optical attenuator VOA3). Bob sends to Alice pairs of bright coherent optical pulses, produced by his laser and two fiber arms of unequal length[19,20]. Alice uses fiber beamsplitters to divert parts of incoming pulse energy to monitoring detector D_{pulse}, synchronization detector D_{sync} and line-loss measurement detector D_{cw}. She prepares quantum states by phase-modulating the pulses, reflecting them at a Faraday mirror and attenuating to single-photon level with VOA1. Bob measures the quantum states by applying his basis choice via phase modulator and detecting outcome of quantum interference with single-photon avalanche photodetectors. Eve's damaging laser is connected to the channel manually. BPF, bandpass filter. **b**, Pulse-energy-monitoring photodiode before and after damage. Brightfield microphotographs show top-view of decapsulated photodiode chips. The last two samples have holes melted through their photosensitive area. Scattered dark specks are debris from decapsulation.

by applying one out of four phases $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$, attenuates the pulses and reflects them back to Bob (Fig. 1a). The security of both protocols requires an upper bound on the mean photon number μ coming out of Alice. Otherwise, an eavesdropper Eve can perform a Trojan-horse attack[25] by superimposing extra light to the bright pulses on their way to Alice from Bob. If Alice is unaware of this and applies the same attenuation, then light coming out of her has a higher μ than allowed by the security proofs[7], making the implementations insecure. It is thus crucial for the security of both protocols that Alice monitors the incoming pulse energy. This is achieved by employing a pulse-energy-monitoring detector (D_{pulse} in Fig. 1a). A portion of the incoming light is fed to D_{pulse} such that whenever extra energy is injected, an alarm is produced[22]. The sensitivity of D_{pulse} is factory-calibrated, thus closing the side-channel associated with the Trojan-horse attack.

We tested the endurance of this countermeasure against laser damage. During normal QKD operation, we disconnected the fiber channel Alice–Bob temporarily and connected Eve (Fig. 1a). She then injected $1550\ \mathrm{nm}$ laser light from an erbium-doped fiber amplifier for 20–30 s, delivering continuous-wave (c.w.) high power into Alice's entrance. 44% of this power reached the fiber-pigtailed InGaAs p-i-n photodiode D_{pulse} (JDSU EPM 605LL), and damaged it partially or fully. It became either less sensitive to incoming light (by 1–6 dB after 0.5–1.5 W illumination at Alice's entrance) or completely insensitive (after ≥ 1.7 W). The physical damage is shown in Fig. 1b. No other optical component was damaged. We repeated the experiment with 6 photodiode samples. In half of these trials, QKD continued uninterrupted after we reconnected the channel back to Bob, as if nothing has happened. In the other half, a manual software restart was needed. However, in all the trials the damage was sufficient to permanently open the system up to the Trojan-horse attack. As modeled in Ref. 22, in the QKD protocol, Eve can eavesdrop partial or full key using today's best technology if the sensitivity of D_{pulse} drops by more than $5.6\ \mathrm{dB}$. In the QCT implementation, a sensitivity reduction by $2.6\ \mathrm{dB}$ can increase Bob's cheating probability above a classical level, removing any quantum advantage of coin-tossing. Laser damage thus compromises both the QKD and QCT implementations. See Methods for details.

Laser damage in free-space quantum communication system. As a representative of free-space quantum communi-

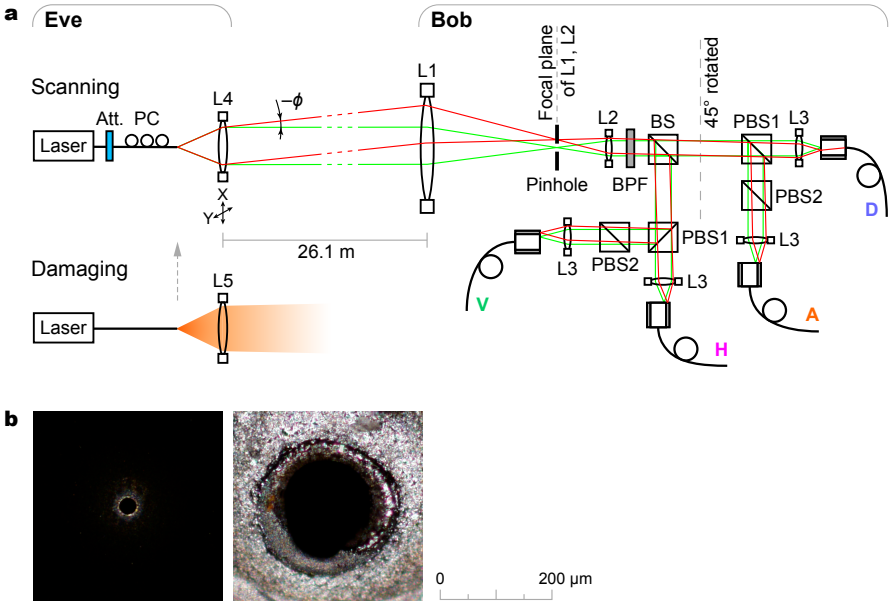

FIG. 2. **Attack on free-space QKD system. a**, Experimental setup. QKD receiver Bob consists of two lenses L1, L2 reducing input beam diameter, 50:50 beamsplitter BS, and two arms measuring photons in HV and DA polarizations using polarizing beamsplitters PBS[16,21]. Photons are focused by lenses L3 into multimode fibers leading to single-photon detectors. Setup drawing is not to scale. Eve's apparatus contains a scanning laser source that tilts the beam angle (ϕ, θ) by laterally shifting lens L4. Green marginal rays denote initial Eve's alignment, replicating the alignment Alice–Bob at $\phi = \theta = 0$. Red marginal rays show a tilted scanning beam missing fiber cores V, H, A, but coupling into D. Eve's damaging laser source can be manually inserted in place of the scanning source. Att., attenuator; PC, polarization controller. **b**, Spatial filter before and after damage. Darkfield microphotographs show front view of the pinhole. See Supplementary Video 1 for real-time recording of laser damage to the pinhole inside Bob.

cation, we chose a long-distance satellite QKD prototype operating at 532 nm wavelength[21] employing Bennett-Brassard 1984 (BB84) protocol[5]. At each time slot, Alice randomly sends one out of four polarizations: horizontal (H), vertical (V), $+45°$ (D), or $-45°$ (A) using a phase-randomized attenuated laser. Bob randomly measures in either horizontal-vertical (HV) or diagonal-antidiagonal (DA) basis, using a polarization-beamsplitter receiver (Fig. 2a). It has been shown in Ref. 16 that an eavesdropper can, in practice, tilt the beam going towards Bob by an angle (ϕ, θ) such that the beam misses, partially or fully, the cores of fibers leading to three detectors while being relatively well coupled into the core leading to the fourth detector, as illustrated in Fig. 2a. This happens because real-world optical alignments are inherently imperfect and manufacturing precision is finite. By sending light at different spatial angles, the eavesdropper can have control over Bob's basis and measurement outcome and steal the key unnoticed[14,16,26]. This attack can be prevented by placing a spatial filter or 'pinhole' at the focal plane of lenses L1 and L2, as shown in Fig. 2a[16]. Since the pinhole limits the field of view, any light entering at a higher spatial angle is blocked and Eve no longer has access to the target angles required to have control over Bob. As was demonstrated in Ref. 16, a pinhole of 25 µm diameter eliminates this side-channel by making the angular efficiency dependence identical between the four detectors (Fig. 3a).

We tested the endurance of this countermeasure against laser damage. From a distance of 26.1 m, we shot an 810 nm collimated laser beam delivering a 10 s pulse of 3.6 W c.w. power at the pinhole inside Bob's setup. The intensity there was sufficient to melt the material (13 µm thick stainless steel) and enlarge the hole diameter to $\approx$ 150 µm. The state of the pinhole before and after damage is shown in Fig. 2b, and the damage process in real time is shown in Supplementary Video 1. Although Bob was up and running in photon counting mode during the test, none of his other components were damaged. See Methods for experimental details.

With this larger pinhole opening, it was again possible to send light at angles that had relatively higher mismatches in efficiency, as shown in Fig. 3b. This enabled a faked-state attack under realistic conditions of channel loss in 1–15 dB range with quantum bit error ratio (QBER) $< 6.6\%$ (see Methods). Thus laser damage completely neutralizes this countermeasure, and makes this free-space QKD system insecure.

Discussion. The crucial step of the attack, creating the loophole, has thus been experimentally demonstrated for both systems tested. After this, building a complete eavesdropper would be a realistic if time-consuming task[27].

Countermeasures to the laser-damage attack may include a passive optical power limiter[28], a single-use 'fuse' that permanently breaks the optical connection if a certain power is exceeded, or battery-powered active monitoring supplemented with wavelength filtering. Hardware self-characterization may be promising[29], however to protect from an arbitrary damage it must monitor a potentially large number of hardware parameters. Any countermeasure must be tested in all

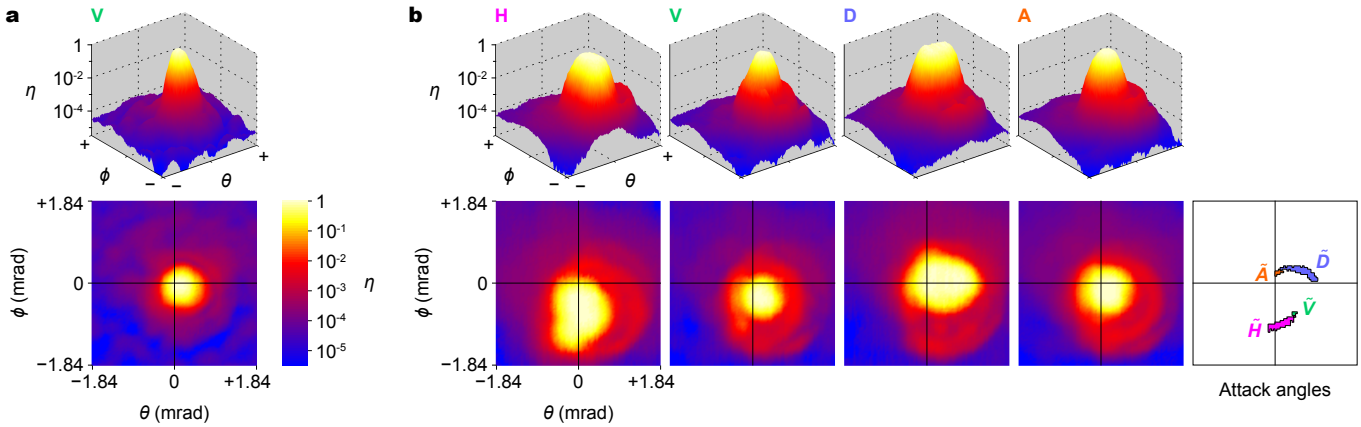

FIG. 3. **Efficiency-mismatch side-channel opened after laser damage in free-space QKD system**. Each pair of 3D–2D plots shows normalised photon detection efficiency η in a receiver channel versus illuminating beam angles ϕ and θ. **a**, Before laser damage, the angular dependence is essentially identical between the four channels[16]. Plot for one channel (V) before damage is shown. **b**, After the laser damage, the four receiver channels H, V, D, A exhibit unequal sensitivity to photons outside the middle area around $\phi = \theta = 0$. The last plot shows angular ranges for targeting the four detectors that satisfy conditions for the faked-state attack.

possible illumination regimes. Eve can use a wide range of wavelengths and optical pulse durations. Optical fiber transmits wavelengths from ultraviolet to ~ 2000 nm, while free-space optics may also be transparent at longer wavelengths. While we have demonstrated c.w. thermal laser damage on the timescale of seconds, short-pulsed laser radiation may induce different damage mechanisms[30]. Furthermore, systems can be attacked in both powered and unpowered state (e.g., during an outage or maintenance). By Kerckhoffs' principle[31], Eve is assumed to predict and know the damage precisely. In practice when attacking installed systems, she may characterize them by imaging, reflectometry[25] and watching public communication Alice–Bob while probing their response to attack sporadically, adjusting her attack parameters until they enable full eavesdropping[26]. In summary, construction of countermeasures that guarantee security remains an open question.

In this work we have tested two QKD systems and a QCT system against laser damage, and compromised the security of each. Although we have not experimentally tested this, it seems the security parameters, characteristics and assumptions of any other implementations of quantum communication protocols might also be vulnerable to laser damage. For example, in a coherent-one-way QKD scheme[32], the front-end contains an attenuator, coupler, and monitoring p-i-n detector, all of which are potentially vulnerable. Similarly, there is no guarantee that the measurement-device-independent[33] and fully-device-independent[34] QKD implementations cannot be altered by laser damage (potentially breaking the assumptions of a trusted source in the former and the absence of information-leakage channels in the latter). Any alteration of characteristics might compromise the security either directly by leading to an attack, or indirectly by shifting some parameter in the security proof so it would no longer apply. Since the laser damage is a new eavesdropping tool that alters a well-characterized system, the community needs to think again how to ascertain the security proofs against changing security parameters. We expect that testing against optical attacks including laser damage will become an obligatory part of security assurance for future quantum communications.

[1]Barz, S. *et al.* Demonstration of blind quantum computing. *Science* **335** 303–308 (2012).

[2]Collins, R. J. *et al.* Realization of quantum digital signatures without the requirement of quantum memory. *Phys. Rev. Lett.* **113** 040502 (2014).

[3]Pappa, A. *et al.* Experimental plug and play quantum coin flipping. *Nat. Commun.* **5** 3717 (2014).

[4]Grice, W. P. *et al.* Two-party secret key distribution via a modified quantum secret sharing protocol. *Opt. Express* **23** 7300 (2015).

[5]Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (IEEE Press, New York, Bangalore, India, 1984).

[6]Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283** 2050–2056 (1999).

[7]Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4** 325–360 (2004).

[8]Bugge, A. N. *et al.* Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **112** 070503 (2014).

[9]Singh, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Fourth Estate, London, 1999).

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

[11]Bennett, C. H., Bessette, F., Salvail, L., Brassard, G. & Smolin, J. Experimental quantum cryptography. *J. Cryptology* **5** 3–28 (1992).

[12]Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems.

Phys. Rev. A **74** 022313 (2006). Erratum ibid. **78**, 019905 (2008).

[13]Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comp.* **7** 73–82 (2007).

[14]Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4** 686–689 (2010).

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

[16]Sajeed, S. *et al.* Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **91** 062301 (2015).

[17]Fung, C.-H. F., Tamaki, K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quant. Inf. Comp.* **9** 131–165 (2009).

[18]*National security telecommunications and information systems security advisory memorandum (NSTISSAM) TEMPEST/2-95, red/black installation guidance* (US National Security Agency, 1995). Declassified in 2000. `http://cryptome.org/tempest-2-95.htm`.

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

[20]Clavis2 specification sheet, `http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf`, visited 27 July 2015.

[21]Bourgoin, J.-P. *et al.* Experimentally simulating quantum key distribution with ground-to-satellite channel losses and processing limitations (manuscript in preparation).

[22]Sajeed, S. *et al.* Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **91** 032326 (2015).

[23]Erven, C. *et al.* An experimental implementation of oblivious transfer in the noisy storage model. *Nat. Commun.* **5** 3418 (2014).

[24]Lunghi, T. *et al.* Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111** 180504 (2013).

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

[26]Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **52** 691–705 (2005).

[27]Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2** 349 (2011).

[28]Tutt, L. W. & Boggess, T. F. A review of optical limiting mechanisms and devices using organics, fullerenes, semiconductors and other materials. *Prog. Quant. Electr.* **17** 299–338 (1993).

[29]Lydersen, L., Makarov, V. & Skaar, J. Secure gated detection scheme for quantum cryptography. *Phys. Rev. A* **83** 032306 (2011).

[30]Wood, R. M. *Laser-Induced Damage of Optical Materials* (CRC Press, 2003).

[31]Kerckhoffs, A. La cryptographie militaire. *J. des Sciences Militaires* **IX** 5–38 (1883).

[32]Walenta, N. *et al.* A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* **16** 013047 (2014).

[33]Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108** 130503 (2012).

[34]Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97** 120405 (2006).

[35]Jain, N. *et al.* Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107** 110501 (2011).

[36]Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13** 123001 (2011).

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

Acknowledgements. We thank Q. Liu, E. Anisimova and O. Di Matteo for early experimental efforts, S. Todoroki, N. Lütkenhaus, M. Mosca, Y. Zhang and L. Lydersen for discussions. This work was supported by the US Office of Naval Research, Industry Canada, CFI, Ontario MRI, NSERC, Canadian Space Agency, ID Quantique, European Commission's FET QICT SIQS project, EMPIR 14IND05 MIQC2 project, and CryptoWorks21. We acknowledge using University of Waterloo's Quantum NanoFab. P.C. was supported from Thai DPST scholarship. J.-P.B. was supported by FED DEV.

Conflicts of interest. A part of this study was supported and M.L. was employed by ID Quantique. The company has been informed prior to this publication, and is developing countermeasures for their affected QKD system. The other authors declare no competing financial interests.

Author contributions. V.M. conceived and led the study. S.K. implemented the fiber-optic experiment. S.S. implemented the free-space experiment and contributed to the fiber-optic experiment. P.C. contributed to the free-space experiment. M.G. contributed to the fiber-optic experiment. C.M. made minor contributions to the free-space experiment. M.L. provided and supported the fiber-optic QKD system under test. T.J. and J.-P.B. provided the free-space QKD receiver under test and contributed to the free-space experiment. R.K. provided the fiber laser facility and co-supervised the fiber-optic experiment. S.S. and V.M. wrote the article, with contributions from all authors.

METHODS

Laser-damage experiment on fiber-optic system. In our experiment, we damaged D_{pulse} during QKD operation, trying not to interrupt it. The system was allowed to start up and produce a secret key for several QKD cycles, using BB84 protocol[5]. To perform laser damage, we disconnected the channel for 2–3 min, giving us enough time to apply high power to Alice, and then reconnected the channel. We tried this at different points in the QKD operation cycle. Sometimes the software recovered and resumed QKD, and sometimes it got stuck in recalibration routines. In the latter case, a manual software restart resumed QKD. Owing to a limited number of trials, we did not perfect this timing aspect.

We tested a total of 6 photodiode samples. We damaged each of them by applying high power laser light at Alice's entrance. We then used the manufacturer's factory-calibration software to measure how much extra signal power (compared to the pre-calibrated power level) could be injected without triggering the alarm[22]. This quantified the reduction in sensitivity due to the damage. Three samples were exposed twice to a progressively higher power. For example, one sample was first exposed to 0.5 W power at Alice's entrance that reduced its photosensitivity by 1 dB, then to 0.75 W power that reduced its photosensitivity by 6 dB. For the other two samples these numbers were 0.75 W with no change in sensitivity then 1.0 W, 1.6 dB (shown in 2nd microphotograph in Fig. 1b); 1.0 W, 5 dB then 1.5 W, 5.5 dB (shown in 3rd microphotograph in Fig. 1b). For the remaining three samples, 1.7 W was applied at Alice's entrance, and D_{pulse} completely lost photosensitivity, becoming electrically either a large resistor (shown in 4th microphotograph in Fig. 1b) or an open circuit. After we were done with each sample, we used the same manufacturer's factory-calibration software to pre-calibrate the sensitivity of the next undamaged D_{pulse} sample, following the factory procedure.

No other component in Alice was damaged during these trials. We also tested some components separately. FC/PC and FC/APC optical connectors used in Alice and in the channel withstood 3 W c.w., while copies of Alice's 10:90 fiber beamsplitters (AFW Technologies FOSC-1-15-10-L-1-S-2) withstood up to 8 W c.w. with no damage.

Figure 4 summarizes a system operation log when it recovered automatically after the damage that made the photodiode an open-circuit with no photosensitivity. In the current system implementation, this represents an ideal outcome for an attacker.

For damaging and component tests, Eve used an erbium-doped fiber amplifier seeded from a 1550.7 nm laser source (EDFA; IPG Photonics ELR-70-1550-LP). She injected 0–2 W c.w. power at Alice's entrance. The injected power was monitored with a 1:99 fiber beamsplitter tap and a power meter (Fig. 1a). A manually operated shutter at the output of EDFA allowed to ramp the power up and down smoothly between 0 and the target level, with tens of milliseconds transition time. The spectral characteristics of EDFA's built-in seed laser did not precisely match the passband of the BPF at Alice's entrance (1551.32–1552.12 nm passband at −0.5 dB level, < 0.7 dB insertion loss; AFW Technologies BPF-1551.72-2-B-1-1). We therefore removed the BPF for the duration of experiment. The BPF was separately tested in-passband using a different EDFA (PriTel LNHPFA-37) with a narrowband seed laser, and passed more than 1 W c.w. with no damage.

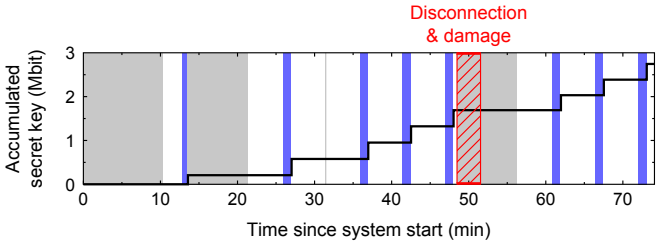

FIG. 4. **Fiber-optic QKD system operation during laser damage.** The plot shows accumulated secret key amount versus time. Grey bands denote the system performing recalibration routines, white bands denote the quantum bit sending and receiving, and blue (darker) bands denote classical post-processing. All this information was extracted from the QKD system log files after the experiment. The band hatched in red denotes the time when the fiber channel Alice–Bob was temporarily disconnected and the laser damage to Alice was done by 1.7 W laser power, resulting in D_{pulse} becoming an open circuit with no photosensitivity.

The system QKD software ('QKD Sequence' application[20]) set the variable attenuator VOA2 at 2 dB. Thus, 44% of Alice's incoming light impinged D_{pulse}, while smaller fractions impinged D_{sync} and D_{cw}. The alarm threshold of D_{pulse} is calibrated when the system is assembled at the factory, and is not changed after that[22]. VOA3 introduced channel loss of 1.87 dB, to simulate the effect of ≈9 km long fiber line Alice–Bob.

The QKD system Clavis2 normally operates automatically in cycles consisting of sending and receiving quantum states until either the memory buffer is full or photon detection efficiency has dropped significantly. It then uses the classical link Alice–Bob to post-process the detected data and distill the secret key[11]. Each cycle takes several minutes. If the last QKD cycle was interrupted because the detection efficiency was too low, or the key distillation failed, the system returns to start-up routines such as timing recalibration[35] before it resumes sending quantum states. This happens often in normal operation, because of naturally occurring drift of hardware and channel parameters. The software generally tries to recover automatically from various error conditions, to provide long-term unattended operation[36].

Predicted attacks on fiber-optic system with damaged pulse-energy-monitoring photodiode. As modeled in Ref. 22, for BB84 QKD protocol Eve can eavesdrop partial or full key information using today's best photonics technologies when the sensitivity of D_{pulse} has dropped by 4.3–5.6 dB, given that communication channel loss Alice–Bob is in a 1–7 dB range. (This corresponds to a multiplication factor x in the range of 2.7–3.6, see Fig. 11 in Ref. 22.) If we assume that Eve's equipment is only limited by the laws of quantum mechanics, then she can extract the full key information after

only 0.4–0.8 dB reduction in sensitivity (x of 1.1–1.2). Similarly, for QCT with a dishonest Bob only limited by the quantum mechanics, all the quantum advantages of the protocol are eliminated if sensitivity reduction of 2.6 dB is obtained in Alice ($x = 1.805$), for a 15 km long communication channel. For a 10 dB sensitivity reduction, Bob's cheating probability approaches unity[22]. Since we have surpassed the above sensitivity reduction thresholds in our laser damage experiment, we consider the security of both QKD and QCT implementation compromised.

Laser-damage experiment on free-space QKD system. In order to neutralize the effect of the pinhole and reproduce the side-channel of spatial-mode detector-efficiency mismatch, our experiment consisted of three steps. Firstly, we performed scanning to certify that the system is secure against this side-channel. Secondly, we laser-damaged the pinhole to open the side-channel. Finally, we performed scanning again to demonstrate that the system's security has been compromised. In all three steps, Eve was placed at a distance of 26.1 m away from Bob and the steps were performed in sequence without making any interactions with Bob.

The first step involved changing the outgoing beam's angle (ϕ, θ) emitted from Eve's scanning setup shown in Fig. 2a, then recording the corresponding count rate at all four detectors in Bob. This step is identical to that in Ref. 16. The scanning result is shown in Fig. 3a, where a pair of 3D–2D plots shows the normalized photon detection efficiency in one receiver channel versus the illuminating beam angles ϕ and θ. With the pinhole in place, the angular dependence of efficiency is essentially identical between the four channels, hence only a plot for channel V is shown. No measurable amount of efficiency mismatch was found and no attack angles existed[16].

Then as the second step, Eve's scanning setup was replaced with the damaging setup. The latter contained a 810 nm laser diode (Jenoptik JOLD-30-FC-12) pumped by a current-stabilized power supply and connected to 200 µm core diameter multimode fiber. It provided continuously adjustable 0 to 30 W c.w. power into the fiber. An almost-collimated free-space beam was subsequently formed by a plano-convex lens L5 (Thorlabs LA1131-B; Fig. 2a). The beam's intensity was nearly uniformly distributed across Bob's L1 (50 mm diameter achromatic doublet, Thorlabs AC508-250-A), with less than $\pm 10\%$ intensity fluctuation across Bob's input aperture. Transmission of L1 was about 82%, owing to its antireflection coating being designed for a different wavelength band. In the test detailed here, the power delivered at the pinhole plane was 3.6 W, sufficient to reliably produce a hole of ≈ 150 µm diameter in less than 10 s in a standard stainless-steel foil pinhole (Thorlabs P25S). We also tested that power decreased to 2.0 W still produced a hole. No other component in Bob was damaged during the tests. Bob's lenses L4 received ~ 1 µW power each, and single-photon detectors only received on the order of a few nW each, mainly owing to the presence of BPF after the pinhole. The BPF was used by Bob to increase the signal-to-noise ratio during QKD by heavily attenuating all light outside the 531–533 nm passband (it consisted of two stacked filters, Thorlabs FESH0700 followed by Semrock LL01-532-12-5)[21]. While the damaging beam was on, the detectors counted at their saturation rate of ~ 35 MHz, which did not look abnormal to Bob as this sometimes occurs naturally owing to atmospheric conditions (during sunset, sunrise, fog). We remark that this type of detector usually survives tens of mW for a short time[8,37]. Even if we had to use a wavelength within the BPF's passband, detector exposure to higher power could likely be avoided by shaping Eve's damaging beam.

After the damage, as the third step we replaced the damaging setup with the scanning setup again, and performed the final scanning of Bob's receiver with the damaged pinhole. The results are shown in Fig. 3b. Now, the four receiver channels H, V, D, A exhibited unequal sensitivity to photons outside the middle area around $\phi = \theta = 0$. These efficiency plots were different from those measured in Ref. 16 without the pinhole, because of extra scattering at the edges of our laser-enlarged pinhole.

Predicted attack on free-space QKD system with damaged pinhole. We model a practical faked-state attack as described in Ref. 16. We assume a part of Eve is situated outside Alice and measures the quantum states coming out. Then, another part of her regenerates the measured quantum states as attenuated coherent pulses and sends them to Bob, tilting her beam at an angle such that it has a relatively higher probability of being detected by the desired detector. Eve has information about Bob's receiver characteristics after the laser damage, and only uses devices available in today's technology[16]. For example, let's assume Eve sends a horizontally polarized light pulse. In this case, she should choose her tilt angle (ϕ, θ) from a subset $\tilde{H}$ selected in such a way that the efficiency $\eta_h(\tilde{H})$ of Bob's horizontal channel in $\tilde{H}$ is as high as possible, in order to maximize mutual information Eve–Bob. On the other hand, if Bob measures in the opposite (DA) basis, the detection probabilities in the D and A channels $\eta_d(\tilde{H})$ and $\eta_a(\tilde{H})$ should be as low as possible, to minimize QBER. Thus, to find attack angles for the horizontally polarized light, we choose $\tilde{H}$ that satisfies $\eta_h(\tilde{H}) \geq 0.6$ and

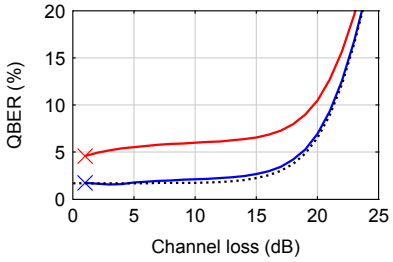

FIG. 5. **Modeled QBER observed by Bob in free-space QKD system.** The dotted curve shows QBER without Eve. At lower channel loss, the QBER is due to imperfect fidelity, while at higher channel loss Bob's detector background counts become the dominant contribution. The lower solid curve (blue) shows QBER under our attack when only Bob's sifted key rate is kept the same as before the attack. The upper solid curve (red) additionally keeps the same sifted key rates conditioned on each polarization sent by Alice, which more closely mimics a realistic system operation (see Ref. 16 for details).

$\delta(\tilde{H}) = \min\left\{\frac{\eta_h(\tilde{H})}{\eta_d(\tilde{H})}, \frac{\eta_h(\tilde{H})}{\eta_a(\tilde{H})}\right\} \geq 100$. Similarly, for V, D and A polarized pulses, we choose attack angles that satisfy $\eta_v(\tilde{V}) \geq 0.03$, $\delta(\tilde{V}) \geq 4.5$; $\eta_d(\tilde{D}) \geq 0.6$, $\delta(\tilde{D}) \geq 120$; $\eta_a(\tilde{A}) \geq 0.2$, $\delta(\tilde{A}) \geq 22$. These subsets of angles are shown in the rightmost plot in Fig. 3b. Note that the thresholds η and δ used here are not optimal and have been picked manually. However, they satisfy the required conditions to successfully perform the faked-state attack with a resultant QBER $\leq 6.6\%$ in 1–15 dB channel loss range, as shown in Fig. 5. In the simulation, we assumed that Alice–Bob and Alice–Eve fidelity $F = 0.9831$[16,21], while Eve–Bob experimentally measured $F = 0.9904$. All other assumptions were the same as in Ref. 16.

Additional considerations in experiment on fiber-optic system. When we began testing the system components for laser damage, the synchronization detector D_{sync} initially presented an obstacle. This detector was based on an optical receiver module (Fujitsu FRM5W232BS) incorporating an avalanche photodiode biased below breakdown at > 30 V, providing an avalanche multiplication factor ≈ 6. It only took about 6 mW of optical power at the photodiode (translating to about 0.15 W at Alice's entrance) to die. It stopped providing the synchronization signal for Alice and thus broke the system. After an investigation, it turned out that the energy that killed it was chiefly provided by its high-voltage electrical bias circuit and not the optical signal. The bias circuit was based on a specialised integrated circuit with overcurrent protection (Maxim Integrated MAX1932ETC) followed by an LC low-pass filter with inductor L = 330 µH and capacitor C = 0.47 µF. If the optical power is applied suddenly, with sub-nanosecond rise time, it momentarily induces a large photocurrent supplied from C that destroys the avalanche photodiode. If, however, the optical power is applied gradually, with millisecond rise time, C discharges slowly and then the relatively slow overcurrent protection reacts in the integrated circuit, lowers the bias voltage and saves the photodiode. We thus added a manual shutter to the EDFA to make the damaging power rise from zero slowly, allowing D_{sync} to easily withstand the optical power used in our attack while being electrically powered up. Another solution could be to damage the system when it is without electrical power. It can also be said that we could choose to selectively damage one of two components in Alice, albeit one of them bricking the system.

We ran our damage tests with VOA2 (OZ Optics DD-600-11-1300/1550-9/125-S-40-3S3S-1-1-485:1-5-MC/IIC) set at 2 dB, because this is what the manufacturer's QKD software available for the research system Clavis2 set it at. The support of the pulse-energy-monitoring countermeasure was not implemented in this software[22]. In contrast, the manufacturer's factory-calibration software supported it fully and set VOA2 between 2 and ≈ 15 dB, complementary to the channel loss, in order to maintain constant power at the three Alice's detectors D_{pulse}, D_{sync}, and D_{cw}. The higher settings of VOA2 would require more laser power to damage D_{pulse}. However, D_{pulse} could also be damaged during the system start-up time, when it sends the homing command to VOA2. The homing command causes it to traverse its lowest attenuation values for a few seconds, likely being sufficient for Eve to do the damage at already demonstrated power levels.

Supplementary Video 1. **Real-time video recording of laser damage to the spatial filter inside Bob's setup.** Download the video at `http://vad1.com/pinhole-laser-damage-20140825.wmv` (Windows Media Video, 14.4 MiB) or `http://vad1.com/pinhole-laser-damage-20140825.ppsx` (PowerPoint Show, 17.0 MiB). The video shows the spatial filter (Thorlabs P20S) illuminated by 3.6 W c.w. 810 nm laser beam for 10 s, focused in a spot much wider than the original pinhole diameter of 20 µm. This is a filter sample with a slightly smaller original pinhole diameter than the one used to obtain efficiency mismatch data in this article and shown in Fig. 2b. The samples were otherwise of the same type and damaged under the same conditions. The video was taken via a mirror lowered inside Bob's setup. The pinhole plane was imaged from the front side at an angle slightly off normal, in order for the mirror not to obstruct the damaging beam. Canon MP-E 65 mm lens was used at 2.8× magnification and f/16 lens aperture (f/60 effective aperture), with Canon EOS 7D camera body. The pinhole was brightly lit sideways with a fiber-optic illuminator bundle, in order to bring up detail. During the laser exposure, the steel foil can be seen deforming from heat, popping out of focus and apparently shifting laterally in the image; however the lateral shift is an artefact of the camera's angle of view being off-normal. After the laser is switched off, the foil cools and returns to the original position, now with about 150 µm diameter hole in it. Sound was added later for an artistic effect.

B.4 Finite-key-size effect on plug-and-play QKD system (unpublished manuscript)

Finite-key-size effect on plug-and-play QKD system

Poompong Chaiwongkhot,[1,2,*] Shihan Sajeed,[1,3] Lars Lydersen,[4] Norbert Lütkenhaus,[1,2] and Vadim Makarov[1,2,5]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[5] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

(Dated: August 26, 2015)

In this work, we investigate the finite key size effect on a commercial plug-and-play QKD system Clavis2 from ID Quantuque. We demonstrated the ability of an eavesdropper to control the raw-key size at Alice and Bob, and its effect on security analysis. We also investigated a countermeasure for this effect.

INTRODUCTION

Quantum key Distribution (QKD) system are expected to provide highly secure keys between two parties. To fulfill that expectation, every feature, imperfection, and loophole both in theory and in physical implementation have to be taken into account. One of these features is that, with limited resource and time, a QKD system can exchange a limited length of raw key. This results in a deviation of statistical variables from what was predicted in the security proof. Finite key size analysis takes those statistical deviation into account and modifies the amount of the secret key generated after privacy amplification process. This is done by introducing the security parameter ϵ, which is the probability that non-zero secret key has been generated according to the protocol but the third party still got knowledge about this key.

The aim of this study is to emphasize the significance of including the finite key analysis in the implementation of QKD system, especially the commercial systems. We demonstrate Eve's ability to control the size of raw key in a running commercial QKD system, and the effect on security of secret key generated in the process.

QKD SYSTEM UNDER TEST

We studied a commercial plug-and-play QKD system, Clavis2, by ID Quantique. This system was a fiber-optics-based QKD system using phase-encoding scheme and weak coherence pulse to exchange the secret key under non-decoy-state BB84(a protocol introduced by C. Bennet and G. Brassard in 1984) [1] and SARG(a protocol introduced by V. Scarani et.al. in 2004) [2] protocols. The detail specification of the system can be seen in [3, 4]. The security of this system is based on the security analysis in [5] which didn't considered the finite key-size effect.

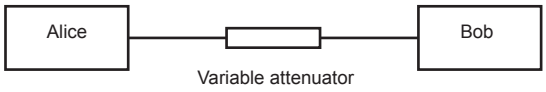

FIG. 1. Scheme of experiment

EXPERIMENT

Under the normal operation, the system exchanged the quantum signal and saves the raw key until the memory buffers in Alice and Bob are filled. Then, they perform sifting, error correction and privacy amplification. [3, 6]. One of the features of Clavis2 is that the system will terminate the raw key exchange process when the photon detection efficiency in quantum channel dropped below a certain value, and perform the post-processing from the raw key already exchanged until then. This feature was implemented to compensate the drift of timing alignment of detector gates. Since the security proof of the system did not take account the statistical deviation of non-infinite key length, if Eve can force the system to generate secret keys from a shorter raw key length, the security proof would no longer apply.

To demonstrate the ability of Eve to force the system to work with a small key length, we began our experiment by setting the system in a normal operation. A variable attenuator was inserted in between the quantum channel. The attenuator was set to 0dB at the beginning. During the raw-key exchange phase, we let the system exchange the raw-key for a set period then change the value of the variable attenuator to induced a 40dB-loss in the fiber. This reduce the detection efficiency in Bob and forced the process to terminated and began the post-processing. For all non-zero distilled key, we recorded the length of sifted key, number of bits disclosed in the error correction, error rate, and length of secret key reported by the system. We varied the duration of each raw key exchange to correct the parameter for various lengths of

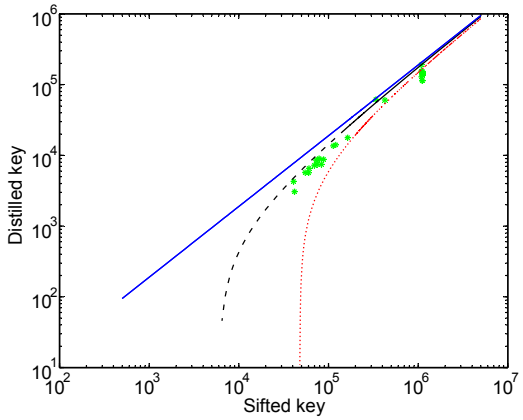

FIG. 2. Secret key rate vs raw key rate. Blue dashed line is the infinite key bound. Red dotted line is finite-key size bound with $\epsilon = 10^{-10}$. Black line is finite-key size bound with $\epsilon = 10^{-1}$. Green dots are experimental result with 3 dB line loss and 5.2% error rate.

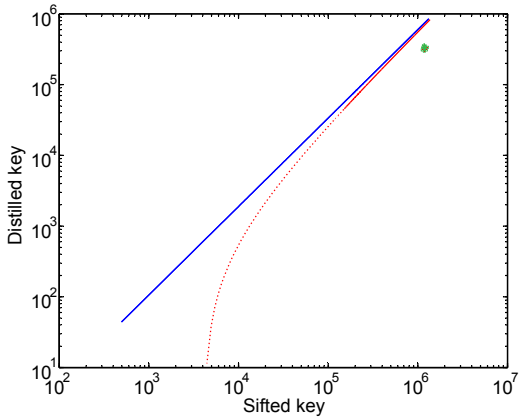

FIG. 3. Experiment result with the new software. Blue line is the infinite key bound. Red-dotted line is finite-key size bound with $\epsilon = 10^{-10}$. Green stars are experiment results

sifted key. We found that the length off distilled key was decreased as the length of sifted key decrease. Next step is to verify if this data agree with the theoretical bound.

RESULT/DISCUSSION

We formulated the key rate equation based on GLLP security proof [7] which gives the lower bound of secret key rate under asymptotic assumption. For finite key size effect, we used correction terms based on previous analysis on BB84 system [8, 9]. Note that this equation is the secret key length as a function of sifted key and other system-reported-parameters.

$$\begin{aligned} l \leq nA(1-h(\frac{E}{A})) - leak_{EC} \\ -\frac{1}{2}\sqrt{(\frac{\ln(1/\epsilon_{PE})\ln(n+1)^2)}{n}} \\ -7\sqrt{\frac{1}{n}log(\frac{2}{\epsilon})) - 2log\frac{1}{\epsilon_{PA}} - log\frac{2}{\epsilon_{EC}}} \end{aligned} \quad (1)$$

where n is sifted-key size, E is error per sifted key reported by the system,$leak_{EC} = 1.2h(E)$ is the estimated keys disclosed in error correction where h(E) is Shannon limit of error correction. The correction term $A = \frac{(p_{det}-p_{multi})}{p_{det}}$ where p_{det} is the probability of detection and p_{multi} is the probability of multi-photon pulse generated by Alice. The last four terms are the correction terms due to finite key statistics [8, 9].

After substituting parameters from the experiment into equation 1, we obtained a lower bound of secret key length as shown in Fig.2. The blue line was calculated under asymptotic assumption as used in the system's protocol. The red and black line is the bound of secret key rate under the finite-key size assumption (the area below each line are secure zone correspond to the security conditions applied to that plot). It can be seen from 2 that the experimental distilled key-size from the system, green stars, satisfied the security criteria for asymptotic assumption. However, the experiment result fall out of bound of finite-key size analysis upto security parameter $\epsilon = 10^{-1}$. As a result, security of the system is not covered by this security proof.

In the middle of our study, IDQ has released a new patch for Clavis2. This patch reduced the QBER and let the system perform post-processing only when the sifted key in the memory exceed a threshold of around 1 million bits. We perform our experiment and recalculated our plot using the new parameters. The experiment distilled is within the secure bound, Fig 3.

CONCLUSION

We have demonstrated the ability of Eve to control the length of raw key in a commercial system, Clavis2, and its effect against finite key analysis. We also investigated the countermeasure from ID Quantique. We hope that this study presented the significance of finite key size analysis and why this effect should be included in the implementations of QKD, especially for commercial QKD systems.

We thank R. Renner, and J. Skaar for discussions. This work was supported by Industry Canada, NSERC, CFI and Ontario MRI. P.C. and S.S. acknowledge support from CryptoWorks21. P.C. acknowledges support by Thai DPST scholarship.

References

[1] 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.

[2] Poompong Chaiwongkhot Mathieu Gagne Thomas Jennewein Sarah Kaiser Raman Kashyap Matthieu Legre Carter Minshull Shihan Sajeed Vadim Makarov, Jean-Philippe Bourgoin. Laser damage creates backdoors in quantum communications. arXiv:1510.03148v1.

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

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

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

[6] Buhler J.P., Lenstra H.W. Jr., and Pomerance Carl. Factoring integers with the number field sieve. *The development of the number field sieve*, 1554:50–94, 1993.

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

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

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

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

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

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

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

[19] 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).

[20] 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.

[21] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers,*

Systems, and Signal Processing, pages 175–179, Bangalore, India, 1984. IEEE Press, New York.

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

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

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

[25] Wolfgang Tittel, Gregoire Ribordy, and Nicolas Gisin. Quantum cryptography. *Physics World*, 11(3):41–5, 1998.

[26] Louis Salvail Gilles Brassard. Secret-key reconciliation by public discussion. *Advances in Cryptology EUROCRYPT 93*, pages 410–423, 1994.

[27] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59(5):3301–3319, 1999.

[28] C. G. Gunther. An identity-based key-exchange protocol. *Advances in Cryptology EUROCRYPT '89*, pages 29–37, 1990.

[29] C. H. Bennett. Quantum cryptography using any 2 nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

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

[31] R. Jozsa C. Macchiavello S. Popescu A. Sanpera D. Deutsch, A. Ekert. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys.Rev.Lett.*, 77:2818–2821, 1996.

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

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

[34] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin, and Anton Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489:269, 2012.

[35] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. Lütkenhaus, and T. Jennewein. Experimentally simulating quantum key distribution with ground-to-satellite channel losses and processing limitations. (manuscript in preparation).

[36] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283, 1998.

[37] 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.

[38] Henning Weier, Tobias Schmitt-Manderbach, Nadja Regner, Christian Kurtsiefer, and Harald Weinfurter. Free space quantum key distribution: Towards a real life application. *Fortschr. Phys.*, 54:840, 2006.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.*, 4:41–41, 2002.

[44] Clavis2 specification sheet, http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf, visited 25 May 2015.

[45] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3–28, 1992.

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

[47] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601, 2008.

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

[49] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat. Commun.*, 3:634, 2012.

[50] 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.

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

[52] 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.

[53] 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.

[54] V. Makarov and J. Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quant. Inf. Comp.*, 8:622–635, 2008.

[55] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma. Security proof of quantum key distribution with detection efficiency mismatch. *Quant. Inf. Comp.*, 9(1 & 2):131–165, 2009.

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

[57] 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.

[58] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, Charles W. Clark, and Carl J. Williams. Quantum key distribution with 1.25 Gbps clock synchronization. *Opt. Express*, 12:2011, 2004.

[59] T. Tsurumaru and K. Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78(3):032302, 2008.

[60] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. Romero Alvarez, T. Moroder, and N. Lütkenhaus. Squashing model for detectors and applications to quantum-key-distribution protocols. *Phys. Rev. A*, 89:012325, 2014.

[61] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics*, 7:210, 2013.

[62] 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.

[63] 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.

[64] Armand Niederberger, Valerio Scarani, and Nicolas Gisin. Photon-number-splitting versus cloning attacks in practical implementations of the bennett-brassard 1984 protocol for quantum cryptography. *Phys. Rev. A*, 71:042316, Apr 2005.