Security proof of the two-way quantum secure direct communication with channel loss and noise

Jianyong Hu, Mingyong Jing, Peng Zhang, Qiangqiang Zhang, Huifang Hou, Liantuan Xiao, and Suotang Jia
State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Laser Spectroscopy, Shanxi University, Taiyuan 030006, China
Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China; *Corresponding author E-mail address: xlt@sxu.edu.cn

Quantum secure direct communication is one of the important mode of quantum communication, which sends secret information through a quantum channel directly without setting up a prior key. Over the past decade, numerous protocols have been proposed, and part of them have been experimentally demonstrated. However, the strict security proof is still in suspense. Two-way protocol is seen as one of the most practical protocol, in this paper, the security of the two-way quantum secure direct communication protocol will be proved against general attacks when the noisy and lossy channel is taken into account. There are two steps included in the proof, firstly, we need to prove that the mutual information between Alice and Bob is larger than the mutual information shared between Alice and the eavesdropper when the error rate in control mode is less than the predetermined threshold. Secondly, once the error rate is lower than the threshold, one can always find out a forward error correction code to guarantee the security of information transmission.

Keywords: quantum secure direct communication, security proof, two-way protocol, channel loss, channel noise.
PACS: 03.67.-a, 03.67.Hk, 03.67.Dd, 03.65.Ud

I. INTRODUCTION

Quantum communication enables two remote parties to share secret information securely over a long distance [1]. Since the pioneering protocol was presented by Bennett and Brassard [2], different modes of quantum communication have been developed, such as quantum key distribution (QKD), quantum secret sharing, quantum secure direct communication (QSDC), quantum teleportation, quantum dense coding, and so on [2-6].

QSDC is one of the important mode of the quantum communication, in contrast to QKD, QSDC sends secret information directly through a quantum channel with unconditional security without setting up a prior key [7]. Since the first QSDC protocol was proposed [4], it has become one of the hot research topics in quantum communication over the past decade [8, 9]. To the entanglement carriers, in 2003, Deng, Long and Liu proposed the two-step QSDC protocol where the criteria for QSDC were explicitly stated [10]. QSDC protocols based on high-dimensional entanglement, multipartite entanglement, and hyperentanglement were developed [11-14]. To the single photons carriers, the first QSDC protocol was proposed in Ref. [15], the so-called DL04 protocol, its feasibility have been demonstrated [16-18]. Wei Zhang et al carried out QSDC experiment with quantum memory [19]. In addition, protocols of quantum signature, quantum dialogue, and quantum direct secret sharing have been constructed based on QSDC [20-22].

In the practice, the channel loss and noise may lead to the error of the information bit when it is encoded on the individual photon [23]. Therefore, QSDC protocol uses a block transmission technique was proposed by Long and Liu, in which the quantum information carriers such as single photons or Einstein-Podolsky-Rosen entanglement pairs are transmitted in a block of N particles [4]. However, when there is noise in the quantum channel, an adversary Eve can gain a certain amount of qubits by hiding her presence in the channel noise. The information leakage may be eliminated by using quantum privacy amplification [24]. Unfortunately, quantum privacy amplification ruins the direct communication picture as it involves the merger and order reshuffling of qubits.

An efficient way to implement QSDC in noisy and lossy channel is to use classical forward error correction (FEC) code. Two-way protocol is seen as one of the most practical protocol [25-30]. In the previous work [16,31], a FEC code, named frequency coding scheme, was used in the two-way QSDC to overcome the channel loss and noise, however, the strict security proof of the protocol is still an outstanding question. In this work, we present a security proof of the two-way QSDC protocol against general attacks. There are two steps in the proof, we first prove that secure qubits is not zero when the error rate in control mode is lower than the predetermined threshold. Secondly, once the first condition is satisfied, one can always find out a FEC coding scheme which can transmit information securely.

II. SECURITY OF TWO-WAY QSDC PROTOCOL
Suppose that Alice wants to send secret information to Bob. The two-way QSQC protocol works as follows:

1. Bob prepares a block of $N_c$ single photons. Each photon in the block is randomly in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli $Z$ operator, and $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ are the eigenstates of the Pauli $X$ operator. Then Bob sends the single-photon block to Alice, Alice acknowledges this fact.

2. Because of channel noise and loss, Alice receives only $N_e$ single photons ($N_e=N_c-\eta$), where $\eta$ is the transmission efficiency of Bob-Alice channel i.e. forward channel. He selects $CN_e$ number ($C$ is a positive number less or equal to 1/2) of photons randomly from the $N_e$ received photons for eavesdropping check by measuring them randomly in the $X$-basis or the $Z$-basis (Control mode). Then Alice tells Bob the positions, the measuring-basis and the measuring results of these measured photons. Bob compares his results with those of Alice and obtains an error rate $e$. If the error rate is higher than the threshold, they will abort the communication. If the error rate is less than the threshold, the Bob-Alice communication is considered as safe, and continue to the next step.

3. The remaining $1-C)N_e$ received photons are used for encoding secret information (Encode mode). She also selects $C(1-C)N_e$ single photons from the remaining photons randomly as check bits for the Alice-Bob transmission, and applies randomly one of the two operations, $U=\text{NOT}=[0\rangle\langle 1|+|1\rangle\langle 0|$, and $I=[0\rangle\langle 0|+|1\rangle\langle 1|$, which flip or not flip the state of the photon. The rest of the single photons will be encoded for information transmission, the coding scheme is pre-negotiated and proper designed according to the error rate measured in the control mode.

4. Alice sends the encoded photon block back to Bob who can deterministically decode the qubits by using the same measuring basis when he prepared the single photon. Bob gets the bit value of each single photon in the block and their arrival time. Because of channel loss, Bob receives only $N_p$ (here $N_p=(1-C)N_e-\eta_p$, $\eta_p$ is the transmission efficiency of Alice-Bob channel i.e. backward channel) photons in each block after subtracting the check photons. Alice and Bob will also publicly compare the results of the checking bits to ensure if there exists eavesdropping in the Alice-Bob transmission. Next, Bob decodes the secret information from the block of qubits.

The security proof of the above QSQC protocol includes two steps, in the next section, we will show that if the error rate $e$ is less than the preset threshold $e_s$, secure qubit rate would bigger than zero, i.e. $I_{AB}^s>I_{AE}$, where $I_{AB}$ is the mutual information between Alice and Bob, $I_{AE}$ is the mutual information between Alice and eavesdropper (Eve). Then, we will prove once $I_{AB}^s>I_{AE}$, Alice can always find out a FEC code scheme to make the information transmission securely.

### A. Security against general attacks

The security analysis in this section draw on the work in Ref. [32-35]. At first, Bob prepares a block of qubits which randomly in the state $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ with the same probability, i.e., the qubits are prepared in a mixed state, $\rho^B=\frac{1}{4}|0\rangle\langle 0|+|1\rangle\langle 1|+|+\rangle\langle +|+|-angle\langle -|/4$. After Alice’s encoding operation, to gain Alice’s information bits, Eve has to distinguish $\rho^A=\rho^B\rho^I$ from $\rho^I=U\rho^BPU$ in the Alice-Bob channel. Since $\rho^B=\rho^B=\frac{1}{2}|0\rangle\langle 0|+|1\rangle\langle 1|/2$, Eve cannot gain any information about Alice’s information bits if she only attacks the qubits after Alice’s encoding operation. Eve has to attack the qubits traveling on both the Bob-Alice channel and the Alice-Bob channel in order to gain Alice’s information bits.

Eve’s most general quantum operation can be described by a unitary operation together with an ancilla. Eve performs a collective attack, i.e., $U_{BE}$ are the same for all qubits.

$$U_{BE}^c[0]/[1],E^c=c_0[0]/[E^c_0]+c_1[1]/[E^c_1],$$

$$U_{BE}^l[0]/[1],E^l=c_0[0]/[E^l_0]+c_1[1]/[E^l_1],$$

$$U_{BE}^l[+]/[-],E^l=c_+[+]/[E^l_+]+c_-[-]/[E^-_-],$$

$$U_{BE}^l[-]/[+],E^l=c_-[-]/[E^-_-]+c_+[+]/[E^l_+].$$

(1)

Where $c_0, c_1, 0, 1, +, -$ can be treated as nonnegative real number, and $|E^c_0>, (i=0, 1, +, -)$ forms four pairs of normalized vectors. After Eve’s attack in the Bob-Alice channel, the joint state of the forward qubit and Eve’s ancilla becomes

$$\rho^I_{Bob-Alice}=U_{BE}^l(\rho^B\otimes|E^c_0><E^c_0|)U_{BE}^l.$$  

(2)

After receiving the forwarding qubits, in the control mode, Alice randomly select and measures the qubits with probability $C$ for attack-detection. By publishing the measurement results, the error rate $e$ of qubit could be obtained. In the encoding mode, Alice encode $k$ information bits onto the block of $N$ forward qubits. With probability $P_1$ and $P_0$, Alice encodes information bit 1 and 0 by the operation $I$ and $Y$, respectively. The state of the qubits and Eve’s ancillas becomes

$$\rho^{AE}_{Bob-Alice}=P_0|0\rangle\langle 0|\otimes\rho^I_{BE}+P_1|1\rangle\langle 1|\otimes\rho^I_{BE},$$

(3)

where $\rho^I_{BE}=\rho^I_{Bob-Alice}$, $\rho^I_{BE}=Y\rho^I_{Bob-Alice}Y$. Then Alice sends the encoded qubits back to Bob. The quantum efficiency of the information transmission is defined as $r_s=\lim_{n \to \infty}k/n$, $n$ is the block size of encoded pulses, $k$ is the secure qubits of the block. In the asymptotic scenario, the secure qubit rate $r_s$ is bounded by the conditional entropy of information bits that Alice sends to Bob given the quantum information of Eve, $r_s=\text{Sh}(\rho^A_{BE}|\rho^I_{AE})$. After Alice’s encoding operation, Eve can gain some quantum information about Alice’s qubit from the quantum state $\rho^I_{BE}=\text{Sh}(\rho^A_{BE})$ that is a joint state of the backward qubit and her ancilla. Here, we
assume the worst case that Eve uses the entire state \( \rho^{BE} \) to gain information bit, even though she may have to send part of the state to Bob. \( r_s = S(\rho^{ABE}) - S(\rho^{BE}) \), where \( S(\rho^{ABE}) = -\text{tr} \rho^{ABE} \log_2 \rho^{ABE} \) and \( S(\rho^{BE}) = -\text{tr} \rho^{BE} \log_2 \rho^{BE} \). In the following, we should calculate the eigenvalues of \( \rho^{ABE} \) and \( \rho^{BE} \) to get \( S(\rho^{ABE}) \) and \( S(\rho^{BE}) \). According to Ref. [1], the secure qubit rate

\[ r_s = h(P_0) - h(\xi) , \]

where \( \xi = e^{-1} - e^{-2} \), \( P_0 \) is the probability that Alice encode information bit 0 on the qubit, and \( h(x) = -x \log_2 x (1-x) \log_2 (1-x) \) is the binary Shannon entropy.

For the practical quantum channels, channel loss and noise should be considered. Alice and Bob should estimate the error rate in the Bob-Alice channel, we assume that the error rate in the backward channel is the same as the error rate in the forward channel. In the asymptotic scenario, after verifying

\[ e < 1/4 , \]

Alice can send the secret information against collective attacks with secure qubit rate

\[ r_s = I_{AB} - I_{AE} = h(P_0) - h(\xi) - h(e) - \eta , \]

where \( \eta \) is the channel loss in the backward channel. \( I_{AB} \) is the mutual information between Alice and Bob, and \( I_{AE} \) is the mutual information between Alice and Eve. As you can see, the final secure qubit rate relates not only to the error rate but also the coding scheme and channel loss.

B. Secure information bit rate

In this part, we will prove that once the secret information transmission rate \( r_s > 0 \), Alice can always find a coding scheme to transmit information securely. Assume there is a binary asymmetric channel, the channel loss is \( \eta \), and error rate is \( p_i \). When the photon is detected

\[ p(0|0) = 1 - p_i, \]

\[ p(1|0) = p_i, \]

\[ p(0|1) = p_i, \]

\[ p(1|1) = 1 - p_i, \]

when the photon is lost

\[ p(0|0) = p(1|0) = 1/2. \]

Therefore, the binary entropy can be expressed as

\[ H(p) = (1 - \eta) [-p_i \log p_i - (1 - p_i) \log (1 - p_i)] + \eta \cdot \log (1 - p_i) \log (1 - p_i) \]

\[ = (1 - \eta) [-p_i \log p_i - (1 - p_i) \log (1 - p_i)] + \eta \]

where \( p_s = 1/2 \) signify the loss of the qubit.

An \( n \) bits sequence can be seen as a point in \( n \)-dimensional Hilbert space, at the receiving end, it change to a ‘sphere’ because of channel loss and noise. The number of point in the ‘sphere’ is

\[ 2^{AD(p)} = 2^{n(-p_1 \log p_1 - (1 - p_1) \log (1 - p_1) + \eta)} . \]

In order to decode correctly, the Hamming distance of each code word should be bigger than \( 2^{AD(p)} \), in addition,

\[ 2^{AD(p)} \cdot 2^{R} = 2^{((1 - \eta) [-p_i \log p_i - (1 - p_i) \log (1 - p_i)] + \eta) \cdot 2^{R}} \leq 2^n \]

That is

\[ 0 \leq R \leq C(p) \equiv 1 - H(p) , \]

where \( R \) is the transmission efficiency, when \( R < C(p) \) one can always find a coding scheme to transmit information correctly according to Shannon’s noisy-channel coding theorem.

Assume that \( k (k < n) \) information bits are encoded on the \( n \) qubits. Because of channel loss and noise, part of qubits can be leaked to Eve as we discussed above. Therefore, Eve can be seen as a receiver whose loss rate is \( \eta_E \), which means Eve gains \( n (1 - \eta_E) \) qubits, here the loss rate is originated from the uncertainty principle and control mode. The loss rate of legitimate receiver Bob is \( \eta_B \), which is caused by channel loss and imperfect detection efficiency.

The error code is caused by channel noise and imperfect encoding operation of Alice, to consider the worst case, Eve use a perfect channel without noise and loss. The error rate caused by the channel loss and Alice’s encoding operation is \( p_1 \) and \( p_2 \), respectively.

The code word is expanded to a Hamming sphere because of the channel loss and noise. The number of typical code words of Eve is

\[ 2^{2(n(1 - \eta_E) \log p_E - (1 - p_E) \log (1 - p_E) + \eta_E)} \]

The number of typical code words of Bob is

\[ 2^{2(n(1 - \eta_B) \log p_B - (1 - p_B) \log (1 - p_B) + \eta_B)} \]

The Hamming distance of each typical code word that Alice used must bigger than the radius of the Hamming sphere. If the Hamming distance of the detected code word and the typical code word is bigger than the radius of the Hamming sphere, error would be happened. The following two condition must be satisfied

\[ 2^{2(n(1 - \eta_B) \log p_B - (1 - p_B) \log (1 - p_B) + \eta_B)} \cdot 2^{2R} \leq 2^n , \]

\[ 2^{2(n(1 - \eta_E) \log p_E - (1 - p_E) \log (1 - p_E) + \eta_E)} \cdot 2^{2R} > 2^n . \]

The condition (15a) keep the information transmission accurately, the condition (15b) assure the security of information transmission.

When the radius of Eve’s Hamming sphere is three times of Bob’s, Eve can’t distinguish adjacent typical code words, here the adjacent typical code words means the typical code words which has closest Hamming distance. Although, the maximum transmission capacity is \( nR \), to guarantee the security of information transmission, only one information bit could be encoded on the block, and the information bit should be encoded on the adjacent typical code words. With the increase of the radius of Eve’s Hamming sphere, more information bits could be encoded on the block. The final information transmission efficiency is

\[ r = \log(2^{2(n(1 - \eta_E) \log p_E - (1 - p_E) \log (1 - p_E) + \eta_E)} \cdot 2^{2R}) \]

\[ = (1 - \eta_E) [-p_E \log p_E - (1 - p_E) \log (1 - p_E) + \eta_E] \]

\[ - (1 - \eta_B) [-p_B \log p_B - (1 - p_B) \log (1 - p_B) + \eta_B] . \]

Figure 1 shows the distribution of information transmission efficiency changes with \( \eta_E \) and \( \eta_B \). Only when \( \eta_E > \eta_B \), the secure encoding efficiency may bigger than zero. The
The transmission rate is always \( H_B \equiv 0 \). Secondly, once the mission securely.

We are grateful to professor Guilu Long for helpful discussions. The project is sponsored by the Natural Science Foundation of China (Nos. 61527824, 11374196, and 61675119) and PCSIRT (No. IRT 13076).

III. CONCLUSION

In this paper, the security of the two-way QSDC protocol is proved against general attacks. The proof included two steps: firstly, we proved that when the system noise is lower than the preset threshold, the mutual information between Alice and Bob is larger than the mutual information shared between Alice and the eavesdropper. Secondly, once the first step is in the affirmative, one can always find a proper FEC to make the information transmission securely. Our work may be extended to other QSDC protocols, such as two-step protocol, multi-step protocol, high-dimension protocol, and so on.

ACKNOWLEDGMENTS

We are grateful to professor Guilu Long for helpful discussions. The project is sponsored by the Natural Science Foundation of China (Nos. 61527824, 11374196, and 61675119) and PCSIRT (No. IRT 13076).

[1] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Physical Review Letters, 117, 190501 (2016).

[2] Bennett CH, Brassard G. Quantum Cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India. IEEE, New York, USA, 1984, pp175-179.

[3] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A 1999; 59: 1829-1834.

[4] Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A 2002; 65: 032302.

[5] Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett 1993; 70: 1895-1899.

[6] Bennett CH, Wiesner SJ. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett 1992; 69: 2881-2884.

[7] Guilu Long, Chuan Wang, Yansong Li, and Fuguo Deng, Quantum secure direct communication, Scientia Sinica Phys, Mech & Astron, 41, 332-342 (2011).

[8] Long GL, Deng FG, Wang C, Li XH, Wen Ket al. Quantum secure direct communication and deterministic secure quantum communication. Front Phys China, 2, 251–272 (2007).

[9] Zhu ZC, Hu AQ, Fu AM. Cryptanalysis and improvement of the controlled quantum secure direct communication by using four particle cluster states. Int J Theor Phys, 53, 1495–1501 (2014).

[10] Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky–Rosen pair block. Phys Rev A, 68, 042317 (2003).

[11] Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 71, 044305 (2005).

[12] Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 253, 15–20 (2005).

[13] Yanbing Li, Tingting Song, Wei Huang, Weiwai Zhan, Fault-Tolerant Quantum Secure Direct Communication Protocol Based On Decoherence-Free States, Int J Theor Phys 54, 589-597 (2015).

[14] Fahimeh Zarmehi, Monireh Houshmand, Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement, IEEE Communications Letters, 20, 10 (2016).

[15] Deng FG, Long GL. Secure direct communication with a quantum one-time pad. Physical Review A, 69, 052319 (2004).
[16] Jianyong Hu, Bo Yu, Mingyong Jing, Liantuan Xiao, Suotang Jia, Guoqing Qin, and Guilu Long, Experimental quantum secure direct communication with single photons, Light: Science and Applications 5, e16144 (2016).

[17] Alessandro Cerè, Marco Lucamarini, Giovanni Di Giuseppe, and Paolo Tombesi, Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise, Physical review letters, 96, 200501 (2006).

[18] Rupesh Kumar, Marco Lucamarini, Giovanni Di Giuseppe, Riccardo Natali, Giorgio Mancini, and Paolo Tombesi, Two-way quantum key distribution at telecommunication wavelength, PHYSICAL REVIEW A77, 022304 (2008).

[19] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo, Quantum Secure Direct Communication with Quantum Memory, Phys. Rev. Lett. 118, 220501 (2017).

[20] Yoon CS, Kang MS, Lim JI, Yang HJ. Quantum signature scheme based on a quantum search algorithm. Phys Scr, 90, 15103-15108 (2015).

[21] Gao G. Two quantum dialogue protocols without information leakage. Opt Commun, 283, 2288-2293 (2010).

[22] Zhang ZJ. Multiparty quantum secret sharing of secure direct communication. Phys Lett A, 342, 60-66 (2005).

[23] Qingyu Cai, The “Ping-Pong” protocol can be attacked without eavesdropping, Physical Review Letters, 91, 109801 (2003).

[24] Deng FG, Long GL. Quantum privacy amplification for a sequence of single qubits. Commun Theor Phys, 46, 443–446 (2006).

[25] Caiqing Yu, Libai Wen, Deterministic secure communication without using entanglement, Chin. Phys. Lett. 21, 601-603, (2004).

[26] Marco Lucamarini, Stefano Mancini, Quantum key distribution using a two-way quantum channel, Theoretical Computer Science, 560, 46-61 (2014).

[27] Yunguang Han, Zhenqiang Yin, Hongwei Li, Wei Chen, Shuang Wang, Guangcan Guo, and Zhengfu Han, Security of modified Ping-Pong protocol in noisy and lossy channel, Scientific Reports, Sci. Rep. 4, 4936 (2014).

[28] Jesni S. Shaari, Marco Lucamarini, and Stefano Mancini, Checking noise correlations for safer two-way quantum key distribution, Quantum Inf Process, 13, 1139–1153 (2014).

[29] C. Ivan Henao, and Roberto M. Serra, Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states, Physical Review A, 92, 052317 (2015).

[30] Hua Lu, Two-way deterministic quantum key distribution against passive detector side channel attacks in the forward line, Quantum Inf Process, 14, 3827–3834 (2015).

[31] Jianyong Hu, Yan Liu, Lingling Liu, Bo Yu, Guofeng Zhang, Liantuan Xiao, and Suotang Jia, Quantum description and measurement for single photon modulation, Photon. Res. 3, 24-27 (2015).

[32] Hua Lu, Chi-Hang Fred Fung, Xiongfeng Ma, and Qing-yu Cai, Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel, Physical Review A, 84, 042344 (2011).

[33] Chi-Hang Fred Fung, Xiongfeng Ma, H. F. Chau, and Qingyu Cai, Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol, Physical Review A, 85, 032308 (2012).

[34] Hua Lu, Chi-Hang Fred Fung, and Qingyu Cai, Two-way deterministic quantum key distribution against detector-side-channel attacks, Physical Review A, 88, 044302 (2013).

[35] Normand J. Beaudry, Marco Lucamarini, Stefano Mancini, and Renato Renner, Security of two-way quantum key distribution, Physical Review A, 88, 062302 (2013).