Proof of Security of a Semi-Device-Independent Quantum Key Distribution Protocol *

Peng Xu(徐鹏)**, Wan-Su Bao(鲍皖苏), Hong-Wei Li(李宏伟), Yang Wang(汪洋), Hai-Ze Bao(包海泽)
The PLA Information Engineering University, Zhengzhou 450001

(Received 9 October 2016)

Semi-device-independent quantum key distribution (SDI-QKD) has been proposed by applying the quantum dimension correlation, and the security relies on the violation of quantum dimension witness inequalities. We prove the security of the SDI-QKD protocol under the depolarization channel by considering the quantum dimension witness inequalities and minimum entropy and the specific process of the QKD protocol, combining with a four-quantum-state preparation and three measurement bases. We also provide the relationship between the dimension witness value, the error rate and the security key rate by the numerical simulation.

PACS: 03.67.Dd, 03.67.Hk DOI: 10.1088/0256-307X/34/2/020302

Since Bennett and Brassard came up with the first quantum key distribution (QKD) protocol in 1984, called the BB84 protocol,[1] QKD has made a rapid development in both theory and experiment. Its security has been proved.[2–5] However, there are still some potential security threats in practical implementation because of imperfections of the QKD devices, which can be used to perform attacks by eavesdroppers. In recent years, researchers have made great contributions in the theoretical and experimental research.[6–12] Device-independent quantum key distribution (DI-QKD) is the most promising scenario to overcome the security loopholes. It does not need any assumption about the internal workings of the QKD devices security and the security is based on the idea of the Bell inequality[13] violation. However, to solve the problem of detecting loopholes[14] in the Bell tests, DI-QKD requires very high detection efficiency.[15] Moreover, the entangled preparation efficiency in DI-QKD is very low.

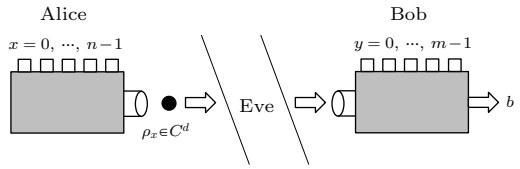

Fig. 1. The SDI-QKD model.[11]

To release the requirements of DI-QKD, inspired by the semi-device-independent dimension witness,[16] Pawłowski *et al.*[17] proposed a semi-device-independent quantum key distribution (SDI-QKD) protocol. In their protocol, they adapted four preparations and two measuring bases, and proved the security against individual attacks by dimension witnesses and quantum random access codes (QRACs).[18] Then, Li *et al.*[19–21] proposed the SDI random-number expansion protocol and presented the relationship between DI protocol and SDI protocol. Wang[22] showed a practical SDI-QKD protocol that uses four preparations and three measuring bases, and proved its security under the condition of depolarization channel.

Like the DI-QKD protocol, the SDI-QKD protocol also does not need any assumptions about Alice and Bob using the quantum device internal working mechanism, that is, Alice and Bob's quantum devices can be described as a black box. Compared with the DI-QKD protocol, the SDI-QKD protocol requires an additional assumption that the dimension of the Hilbert space is limited. However, its advantage is that the protocol can be realized under unidirectional preparation measuring configuration and does not need to use the entangled state.

In this study, we consider the SDI-QKD model in Ref. [17], as shown in Fig. 1. What is more, we assume that the quantum system of Hilbert space dimension is d. The model with the black box of state preparation and state measurement can be described as follows: (1) Alice randomly chooses one $x \in \{0, \ldots, n-1\}$ of the n inputs. The corresponding quantum state is $\rho_x \in \mathbb{C}^d$ to each input. (2) Alice sends the selected corresponding quantum state to Bob as the input. (3) After receiving Alice's quantum state, Bob chooses a basis to perform measurement M_y^b ($y \in \{0, \ldots, m-1\}$) and obtains the result $b \in \{0, \ldots, k-1\}$. (4) Repeating this process many times later, Alice and Bob can estimate the conditional probability distribution of the input and output results as follows:

$$P(b|x,y) = \mathrm{tr}(\rho_x M_y^b), \tag{1}$$

where $P(b|x,y)$ is the probability of obtaining b when Alice prepares ρ_x and Bob performs measurement M_y^b. In the SDI-QKD scenario, the security of a given protocol against a quantum eavesdropper is only guaranteed by its associated probability distribution

*Supported by the National Basic Research Program of China under Grant No 2013CB338002, and the National Natural Science Foundation of China under Grant Nos 11304397 and 61505261.
**Corresponding author. Email: 554725043@qq.com
© 2017 Chinese Physical Society and IOP Publishing Ltd

$P(b|x,y)$. The probability distribution can establish the relation between the security and the quantum dimension witness. Gallego *et al.*[10] put forward and developed the dimension witness. The form of the quantum dimension witness is

$$W = \sum_{x,y,b} w_{xyb} P(b|x,y) \leq Q_d, \tag{2}$$

where Q_d represents the maximum available that W can reach when Alice prepares for a d-dimension quantum system. The quantum dimension witness shows that by arbitrarily given probability distribution cannot be copied by using quantum states with the same dimension. In SDI-QKD with the two-dimensional Hilbert space, the following part conditional probability can be used to analyze its security

$$E_{x,y} = P(b=0|x,y), \tag{3}$$

where $x \in \{00,01,10,11\}$, $y \in \{0,1\}$ and $P(b=0|x,y) + P(b=1|x,y) = 1$. This work considers a tighter two-dimensional quantum dimension witness inequality and its quantum dimension is bounded as follows:[17]

$$\begin{aligned} W \equiv\, & E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} \\ & + E_{10,1} - E_{11,0} - E_{11,1} \leq 2.828. \end{aligned} \tag{4}$$

The SDI-QKD protocol is described in the following. (1) State preparation: Alice randomly selects its input $x \in \{00,01,10,11\}x \in \{00,01,10,11\}$ and prepares the corresponding quantum state $|\alpha(x)\rangle$ in the two-dimensional Hilbert space, specifically as shown in Eq. (4). Let $\{|\alpha(00)\rangle, |\alpha(01)\rangle\}$ denote the classic bit 0, and $\{|\alpha(10)\rangle, |\alpha(11)\rangle\}$ denote the classic bit 1. Then, Alice records the classical bit string and sends all quantum states to Bob through the quantum channel. (2) Measurement: Bob chooses a basis from T_0, T_1 and T_2 randomly and independently to measure the quantum state received from Alice. The selections of the basis and corresponding measurement results were recorded by Bob. (3) Basis reconciliation: Bob publishes his basis selection bases through the authenticated classic channel. Then Alice and Bob can sift the respective raw key according to quantum states prepared and measured by T_2. The results from T_0 and T_1 bases will be used for parameter estimation. (4) Parameter estimation: Alice and Bob estimate the error rate by randomly sampling the results obtained from T_0 and T_1 bases. (5) Classical information post-processing: after the above steps, they can build their distilled key. If the key is greater than zero, they can apply error correction and privacy amplification on their data set to establish some amount of secret key.

Firstly, the relevant definitions and lemma are introduced as follows.

Definition 1 (minimum entropy):[23] let $\rho = \rho_{UV}$ be the quantum state about two systems U and V, then the minimum entropy of U in conditional V is defined as

$$H_{\min}(U|V)_\rho \equiv -\inf D_\infty(\rho_{UV}|id_U \otimes \sigma_V), \tag{5}$$

where σ_V is the arbitrary density operator on B, id_U is the unit operator about U, $D_\infty(\tau|\tau')$ represents the relative Renyi entropy of the order ∞ of the exchange density operators τ and τ'.

Lemma 1:[23] let $\rho = \rho_{UV} = \sum_{u\in U} P_U(u)|u\rangle\langle u| \otimes \rho_{V|U=u}$ represent the quantum state system of U and V, the probability $P_U(u)$ represents when $U = u$, then

$$H_{\min}(U|V)_\rho \equiv -\log P_{\text{guess}}(U|V)_\rho, \tag{6}$$

where $P_{\text{guess}}(U|V)_\rho$ is the maximum probability of decoding U from V using POVM.

Pawłowski *et al.*[17] only proved the security against individual attacks. Here we consider Eve performing collective attacks on Alice's and Bob's system, respectively, before the classic post processing. In addition to the limitation of the dimension of the quantum system and Eve's individual attack, it is also required to have a basic assumption of the black box information leakage, which is necessary in either the DI-QKD protocol or the SDI-QKD protocol. The assumption shows that Eve cannot obtain any information about the random input bits and the measurement results (x, y and b). Furthermore, the quantum channel can be completely controlled by Eve and the classical channel is authenticated.

Under Eve's individual attack, the lower bound on the asymptotic secure key rate after the one-way classical post-processing is given by the Devetak–Winter bound[24]

$$R \geq S(B|E) - H(B|A), \tag{7}$$

where E is Eve's total information, A and B indicate Alice's and Bob's raw keys, respectively, $S(B|E)$ is the conditional von Neumann entropy, which means the upper bound on the information obtained by Eve from Bob's raw key, and $H(B|A)$ is the conditional Shannon entropy.

Here $H(B|A)$ is completely determined by the difference between the raw key shared by Alice and Bob. Let Q denote the quantum bit error rate (QBER) between A and B, then we have

$$H(B|A) = h(Q), \tag{8}$$

where $h(x)$ is the binary Shannon entropy function and can be written as

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

We set $P_{\text{guess}}(B|E)$ to represent the probability of guessing Bob's raw key correctly when Eve uses the best strategy. Then we have the following formula

$$P_{\text{guess}}(B|E) = \max_{b,x,y} P(b|x,y). \tag{9}$$

According to the $(2,1,0.85)$-QRAC mode, the sender has two bits of information and the receiver can accept

only one bit. Thus x can be divided into two parts: a_0 and a_1, $x = a_0a_1$, and then Eq. (9) can expressed as

$$P_{\text{guess}}(B|E) = \frac{1}{8}\sum_{a_0,a_1,y}\max_b P(b|a_0,a_1,y). \quad (10)$$

According to Lemma 1, the minimum entropy can be expressed as

$$H_{\min}(B|E) = -\log P_{\text{guess}}(B|E). \quad (11)$$

Then by using the bound of the minimum entropy $H_{\min}(B|E)$, we can obtain the upper bound on the information obtained by Eve from Bob's raw key. The bound can be expressed as

$$\begin{aligned} &S(B|E) \geq H_{\min}(B|E) \\ &= -\log P_{\text{guess}}(B|E) \\ &= -\log\Big[\frac{1}{8}\sum_{a_0,a_1,y}\max_b P(b|a_0,a_1,y)\Big]. \end{aligned} \quad (12)$$

Substituting Eqs. (9) and (12) into Eq. (8), we can obtain

$$R \geq -\log\Big[\frac{1}{8}\sum_{a_0,a_1,y}\max_b P(b|a_0,a_1,y)\Big] - h(Q). \quad (13)$$

The upper bound of $P(b|a_0,a_1,y)$ is needed to obtain the security key rate of SDI-QKD protocol against collective attacks. We use the method in Ref. [20] to solve this problem. As shown in Ref. [25] only considering two measurement results can traverse all projection measurement operators, but not arbitrary POVM. Based on this result, we can simplify the process of optimizing these equations. Considering the state of the quantum state as a pure state we set W as a linear combination of some probability distributions. According to the result in Ref. [26] we have

$$P_{\text{guess}} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\sqrt{1-[(W^2-4)/4]^2}}{2}}. \quad (14)$$

Under this limitation, we can calculate the value of the minimum entropy with different dimension witness values W by $-\log_2[f(W)]$. Because the quantum dimension witness W is limited with $2 \leq W \leq 2\sqrt{2}$, we can obtain the minimum value 0 of the minimum entropy when $W = 2$ and the maximum value 0.228 of the minimum entropy when $W = 2\sqrt{2}$. As a result, the secret key rate of SDI-QKD under collective attacks can be expressed as

$$\begin{aligned} R \geq &-\log_2\Big(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\sqrt{1-[(W^2-4)/4]^2}}{2}}\Big) \\ &-[-Q\log_2 Q - (1-Q)\log_2(1-Q)]. \end{aligned} \quad (15)$$

By the numerical simulation, we plot Fig. 2 to clarify the relationship among the security key rate R, the dimension witness value W and the bit error rate Q.

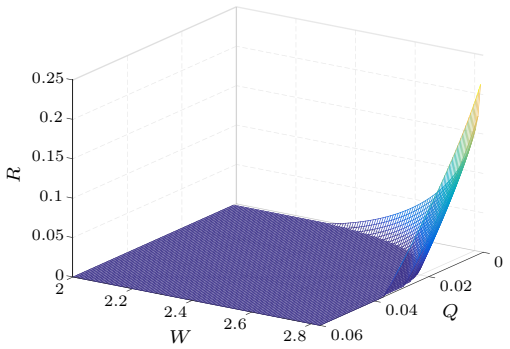

Fig. 2. The relationship between the security key rate R, the dimension witness value W and the bit error rate Q.

From Fig. 2, we can see that the security key rate will become 0 if the maximum bit error rate is over 0.05. The security key rate will always be 0 if the dimension witness value is less than 2.4. The security key rate can reach its maximum value 0.228 if and only if the bit error rate is 0 and the dimension witness value is 2.828. We plot Fig. 3 with some different bit error rate Q to show the relationship between the dimension witness value W and the security key rate R.

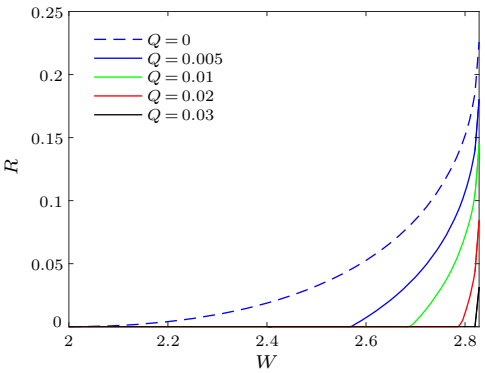

Fig. 3. When the bit error rates Q are 0, 0.005, 0.01, 0.02 and 0.03, the relationship between the dimension witness value W and the security key rate R is under the corresponding condition.

The bit error rate has a great impact on the security key rate. As shown in Fig. 3, the higher dimension the witness value could reach, and the higher the security key rate is under the same bit error rate.

In summary, we have analyzed and improved an SDI-QKD protocol with four quantum states and three measurement bases, which can be directly applied to the one-way system. We give the security proof of the SDI-QKD protocol in the depolarization channel against individual attack based on the minimum entropy and dimensions witnessed. Based on the condition, we show the relationship between the security key rate, QBER and its dimensions witnessed by numerical simulation. If the experimental verification of SDI-QKD is realized, the security of SDI-QKD under the condition of noise and imperfect detectors is worth researching further. In addition, how to improve the secret key rate of SDI-QKD protocol is also

worth investigating further.

References

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p 175
[2] Shor P and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[4] Renner R 2005 *Zürich: ETH*
[5] Renner R, Gisin N and Kraus B 2005 *Phys. Rev.* A **72** 012332
[6] Wang S, Yin Z Q 2015 *Nat. Photon.* **9** 832
[7] Wang C, Song X T 2015 *Phys. Rev. Lett.* **115** 160502
[8] Wang S, Chen W 2012 *Opt. Lett.* **37** 1008
[9] Wang S, Chen W 2014 *Opt. Express* **22** 21739
[10] Wang S, Chen W 2010 *Opt. Lett.* **35** 2454
[11] Su X, Wang Y 2016 *Opt. Lett.* **41** 5596
[12] Li F Y, Yin Z Q 2014 *Chin. Phys. Lett.* **31** 070302
[13] Bell J S 1987 *Speakable and Unspeakable in Quantum Mechanics* (Cambridge: Cambridge University Press)
[14] Pearle P M 1970 *Phys. Rev.* D **2** 1418
[15] Pironio S, Acín A, Brunner N et al 2009 *New J. Phys.* **11** 045021
[16] Gallego R, Brunner N, Hadley C et al 2010 *Phys. Rev. Lett.* **105** 230501
[17] Pawłowski M and Brunner N 2011 *Phys. Rev.* A **84** 010302
[18] Nayak A 1999 *In Proceedings of 40th IEEE FOCS* [C] p 369
[19] Li H W, Yin Z Q, Wu Y C et al 2011 *Phys. Rev.* A **84** 034301
[20] Li H W, Pawłowski M, Yin Z Q et al 2012 *Phys. Rev.* A **85** 052308
[21] Li H W, Mironowicz P, Pawłowski M et al 2013 *Phys. Rev.* A **87** 020302(R)
[22] Wang Y 2014 *Chin. Phys.* B **23** 080303
[23] Konig R, Renner R and Schaffner C 2009 *IEEE Trans. Inf. Theory* **55** 4337
[24] Devetak I and Winter A 2005 *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **461** 207
[25] Levenberg K 1944 *Q. Appl. Math.* **2** 164
[26] Li H W, Yin Z Q, Pawłowski M et al 2015 *Phys. Rev.* A **91** 032305