Security of a practical semi-device-independent quantum key distribution protocol against collective attacks*

Wang Yang(汪 洋)[a)b)], Bao Wan-Su(鲍皖苏)[a)b)†], Li Hong-Wei(李宏伟)[a)b)], Zhou Chun(周 淳)[a)b)], and Li Yuan(李 源)[a)b)]

[a)] *Institute of Cryptographic Engineering, The PLA Information Engineering University, Zhengzhou* 450001, *China*
[b)] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 8 November 2013; revised manuscript received 6 January 2014; published online 10 June 2014)

Similar to device-independent quantum key distribution (DI-QKD), semi-device-independent quantum key distribution (SDI-QKD) provides secure key distribution without any assumptions about the internal workings of the QKD devices. The only assumption is that the dimension of the Hilbert space is bounded. But SDI-QKD can be implemented in a one-way prepare-and-measure configuration without entanglement compared with DI-QKD. We propose a practical SDI-QKD protocol with four preparation states and three measurement bases by considering the maximal violation of dimension witnesses and specific processes of a QKD protocol. Moreover, we prove the security of the SDI-QKD protocol against collective attacks based on the min-entropy and dimension witnesses. We also show a comparison of the secret key rate between the SDI-QKD protocol and the standard QKD.

Keywords: quantum key distribution, semi-device-independent, collective attacks, secret key rate

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/23/8/080303

1. Introduction

Quantum key distribution (QKD) allows two distant parties, Alice and Bob, to share secret keys, with security guaranteed by the laws of quantum mechanics.[1] Since Bennett and Brassard proposed the first QKD protocol, namely the BB84 protocol,[2] QKD has been developed rapidly both in theoretical research and experimental realizations.[3–11] The unconditional security of the idea QKD has been proved based on various methods, such as entanglement distillation,[12,13] uncertainty relation,[14–16] and quantum information theory.[17,18] However, unavoidable imperfections of the devices in practical QKD systems bring about differences between theoretical and practical security of QKD. Taking advantage of security loopholes in practical quantum systems, various attacks have been effectively launched in recent years, for instance, time-shift attacks,[19,20] phase remapping attacks,[21,22] blinding attacks,[23,24] and wavelength-dependent attacks.[25]

In order to overcome these security loopholes, one promising approach is device-independent QKD (DI-QKD).[26–28] DI-QKD does not need any assumptions about the internal workings of the QKD devices and its strong form of security is based on the violation of a Bell inequality.[29] For example, it is not necessary to consider the Hilbert space dimension of the quantum states and the kind of measurements acting on them. However, since the detection loophole,[30] which demands high detection efficiencies, is needed to close in the Bell test, DI-QKD imposes severe requirements on the QKD devices. So a demonstration of fully DI-QKD is an extremely difficult challenge at present. Moreover, the fact that the security of DI-QKD is based on quantum nonlocality indicates that only entanglement-based protocols are suitable for DI-QKD. Remarkably, most practical QKD systems or commercial QKD systems are implemented in a one-way prepare-and-measure configuration, which is much easier to implement compared with the entanglement-based protocol. Hence, researchers are enthusiastic about intermediate schemes between standard QKD and DI-QKD.[31–36]

Instead of full device independence, Pawłowski *et al.*[31] proposed a semi-device-independent quantum key distribution (SDI-QKD) scenario, which also needed no assumption about the internal workings of the preparation and measurement devices but only an assumption about the bounded dimensionality of the quantum systems. Based on dimension witnesses[37] and random-access codes,[38] they also proved the security of a SDI-QKD protocol with four input states and two measurement bases against individual attacks for one-way prepare-and-measure configuration. Besides, inspired by the semi-device-independent idea, Li *et al.* proposed semi-device-independent randomness expansion protocols.[39,40] Though Pawłowski *et al.*[31] analyzed the security of a SDI-QKD protocol with four input states and two measurement bases against individual attacks, they do not present a practical SDI-QKD protocol. Here, we design a practical SDI-QKD with four

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grant Nos. 11304397 and 11204379).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2014 Chinese Physical Society and IOP Publishing Ltd

preparation states and three measurement bases by considering the maximal quantum witness violation and specific processes of a QKD protocol, which includes the choices of preparation states and measurement bases, the sifting and so on. Furthermore, we will analyze the security of the SDI-QKD protocol against collective attacks based on the min-entropy and the dimension witnesses.

The rest of this paper is organized as follows. In Section 2, we introduce the SDI-QKD model. The practical SDI-QKD protocol is proposed in Section 3 and Section 4 presents the secret key rate of SDI-QKD against collective attacks. The conclusion and discussion are summarized in Section 5.

2. SDI-QKD model

Since the SDI-QKD protocol needs an extra assumption about the known dimensionality of the quantum systems, we can see it as a weaker version of DI-QKD. It also needs no assumption about the internal workings of the quantum devices used by Alice and Bob. The SDI-QKD model[31] that we consider in this paper is illustrated in Fig. 1.

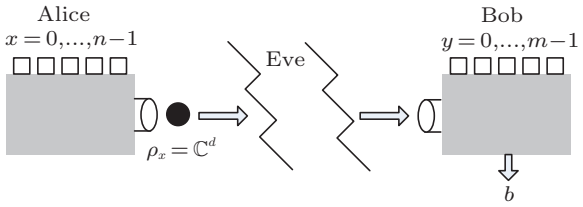


Fig. 1. The scenario of SDI-QKD.[31]

In a semi-device-independent scenario, we assume that the Hilbert space dimension of the quantum systems is d. However, as Alice does not trust her preparation apparatuses and Bob does not trust his measurement apparatuses, we can conveniently treat the devices of Alice and Bob as black boxes.

State preparation black box: Alice chooses randomly one of the n inputs $x \in \{0,\ldots,n-1\}$. There is a quantum state $\rho_x \in \mathbb{C}^d$ corresponding to each input. Then Alice sends the corresponding quantum states to Bob.

State measurement black box: After receiving quantum states from Alice, Bob can choose to perform a measurement M_y^b with $y \in \{0,\ldots,m-1\}$ and gets the outcome $b \in \{0,\ldots,k-1\}$.

After repeating this procedure many times, Alice and Bob can estimate the probability distribution

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

In the SDI-QKD model, the security of a given protocol against a quantum eavesdropper can be guaranteed solely from its associated probability distribution $P(b|x,y)$. The probability distribution $P(b|x,y)$ can be established in relation to quantum dimension witnesses. Dimension witnesses have been developed in Ref. [37]. The form of quantum dimension witnesses is given as follows:

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

where Q_d is the obtainable maximal value of W when Alice prepares quantum d-dimensional systems. The quantum dimension witnesses suggest that any given probability distribution cannot be reproduced by applying quantum states with the same dimension. That is, the dimension of quantum states is required to be strictly larger than d in order to violate the inequality (2). Just as the violation of a Bell inequality in DI-QKD, the violation of dimension witnesses is a necessary condition for guaranteeing the security of the SDI-QKD protocol.

3. A practical SDI-QKD protocol

Pawłowski *et al.*[31] have pointed out that the choices of preparation states and measurement bases in BB84 are not secure in the SDI-QKD model; however, they do not present a practical protocol with the specific choices of preparation states and measurement bases. For the purpose of simplicity and efficiency, we will present a practical SDI-QKD protocol with four preparation quantum states and three measurement bases in two-dimensional Hilbert space.

3.1. BB84 is not secure in SDI-QKD model

For BB84, the state preparation of Alice can be given by

$$\begin{aligned} &|\varphi_0\rangle = |0\rangle, \ \ |\varphi_1\rangle = |-\rangle, \\ &|\varphi_2\rangle = |+\rangle, \ \ |\varphi_3\rangle = |1\rangle. \end{aligned} \tag{3}$$

The two measurement bases of Bob are $\{M_0^0 = |0\rangle\langle 0|, M_0^1 = |1\rangle\langle 1|\}$ and $\{M_1^0 = |+\rangle\langle +|, M_1^1 = |-\rangle\langle -|\}$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

Here, we consider a tight two-dimensional quantum witness as follows:[31]

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

where the set of probability distributions $E_{x,y} = P(b=0|x,y)$ with $x \in \{00,01,10,11\}$, $y \in \{0,1\}$, and $P(b=0|x,y) + P(b=1|x,y) = 1$, are used to describe simply the quantum dimension witnesses.

Thus, the dimension witness achieves $W = 2$ and it does not violate the witness (4), which indicates that equation (1) can be reproduced by an eavesdropper, namely, BB84 is not secure in the SDI-QKD model.[31]

3.2. (2, 1, 0.85) quantum random access coding (QRAC)

Ambainis *et al.*[41] introduced the notion of quantum random access coding (QRAC). For a concrete example, they give (2, 1, 0.85)-QRAC as follows. The sender, which has two-bit information, encodes the information into one qubit, which is sent to the receiver. The receiver can recover any one of the two bits correctly with probability at least 0.85 by a decoding process based on positive operator-valued measures (POVMs). For a concrete example,[41,42] the (2, 1, 0.85)-QRAC maps $a_0a_1 \in \{0,1\}^2$ to $\rho_{a_0a_1} = |\alpha(a_0a_1)\rangle\langle\alpha(a_0a_1)|$ where

$$\begin{aligned}
|\alpha(00)\rangle &= \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle,\\
|\alpha(01)\rangle &= \cos(7\pi/8)|0\rangle + \sin(7\pi/8)|1\rangle,\\
|\alpha(10)\rangle &= \cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle,\\
|\alpha(11)\rangle &= \cos(5\pi/8)|0\rangle + \sin(5\pi/8)|1\rangle. \qquad (5)
\end{aligned}$$

For decoding, we use the measurements by the following POVMs: $T_0 = \{M_0^0 = |0\rangle\langle 0|, M_0^1 = |1\rangle\langle 1|\}$ and $T_1 = \{M_1^0 = |+\rangle\langle +|, M_1^1 = |-\rangle\langle -|\}$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

3.3. Description of the SDI-QKD protocol

Since the SDI-QKD model with four input states and two measurements is equal to the (2, 1, 0.85)-QRAC and the two-dimensional quantum witness can achieve the maximal value 2.828 in (2, 1, 0.85)-QRAC,[39,40] we will apply the preparation states and measurement bases in (2, 1, 0.85)-QRAC. Besides, in order to eliminate the intrinsic errors, we will also introduce another measurement basis $T_2 = \{M_2^0 = |\alpha(00)\rangle\langle\alpha(00)|, M_2^1 = |\alpha(11)\rangle\langle\alpha(11)|\}$ on Bob's side in our protocol. The other procedures of our protocol are designed based on the idea of BB84. The sketch of our practical SDI-QKD protocol is as follows.

State preparation and distribution: Alice chooses randomly inputs $x \in \{00, 01, 10, 11\}$ and prepares the corresponding quantum state $|\alpha(x)\rangle$ in two-dimensional Hilbert space, which can be illustrated as in Eq. (5). Let $\{|\alpha(00)\rangle, |\alpha(01)\rangle\}$ correspond to classical bit 0 and $\{|\alpha(10)\rangle, |\alpha(11)\rangle\}$ correspond to classical bit 1. Then Alice records the classical bit strings and distributes all quantum states to Bob through the quantum channel.

Measurement: Bob chooses a basis among T_0, T_1, and T_2. Then Bob uses randomly and independently the chosen basis for measuring quantum states received from Alice. Bob records both choices of measurement bases and the measurement outcome.

Sifting: Bob announces his lists of basis choices publicly to Alice through the authenticated classical channel. Then Alice compares the lists of T_2 bases from Bob with her prepared quantum states and tells Bob his correct measurement results in the T_2 basis. Alice's classical bit strings, which are corresponding to Bob's correct measurements from the T_2 basis, are used as bits of the raw key together with Bob's correct measurement results in the T_2 basis. The measurement results from the T_0 and T_1 bases will be used to perform the parameter estimation.

Parameter estimation: Alice and Bob estimate the amount of errors in the quantum channel by using a random sample.

Error correction: Alice and Bob apply a one-way error correction scheme and correct their strings so that Bob's raw key matches Alice's. If error correction fails, the protocol aborts.

Error verification: In practical implementations, it is possible that Alice and Bob do not have perfectly identical bits at the end of the error correction scheme. In order to reduce the remaining errors, Alice and Bob will apply a random two-universal hash function on their strings and communicate the result of the function. If the hash values disagree, Alice and Bob may go back to the error correction step or abort the protocol.

Privacy amplification: To reduce the information on keys, which may have been obtained by the eavesdropper Eve during the key generation, Alice chooses randomly a two-universal hash function to extract the final secret key. Then the function is communicated to Bob, who also uses it to extract the final secret key.

4. Secret key rate of SDI-QKD against collective attacks

First, we shall introduce some relevant definitions and lemmas as follows.

Definition 1 (min-entropy)[43] Let $\rho = \rho_{UV}$ be any bipartite state on two systems U and V, the min-entropy of U conditioned on V is defined as

$$H_{\min}(U|V)_\rho \equiv -\inf D_\infty(\rho_{UV}|id_U \otimes \sigma_V), \qquad (6)$$

where σ_V is any density operator on B and id_U is the identity operator on U, $D_\infty(\tau|\tau')$ corresponds to the relative Renyi entropy of order ∞ for commuting density operators τ and τ'.

Lemma 1[43] Let $\rho = \rho_{UV} = \sum_{u\in U} P_U(u)|u\rangle\langle u| \otimes \rho_{V|U=u}$ denote the state of the systems U and V, $P_U(u)$ is the probability of having $U = u$, then

$$H_{\min}(U|V)_\rho \equiv -\log P_{\text{guess}}(U|V)_\rho, \qquad (7)$$

where $P_{\text{guess}}(U|V)_\rho$ is the maximal probability of decoding U from V with a positive operator-valued measure (POVM).

The security analysis in Ref. [31] is restricted to individual attacks, in which Eve attacks independently each system before the classical postprocessing. In this paper, we consider collective attacks where Eve applies the same attack to each system of Alice and Bob before the classical postprocessing.

Our security analysis also needs no assumption about the internal workings of the quantum devices used by Alice and Bob, except that the dimensionality of quantum systems and collective attacks are bounded. Indeed, we also need the basic assumption about information leakage from the black boxes, which is required in both of DI-QKD and SDI-QKD. That is, Eve has no information about random input numbers and measurement outcomes (i.e., x, y, and b). Moreover, the quantum channel is completely controlled by the eavesdropper Eve and the classical channel is authenticated.

For collective attacks, a lower bound on the asymptotic secure key rate R under one-way classical postprocessing is given by the Devetak–Winter bound[44]

$$R \geq S(B|E) - H(B|A), \tag{8}$$

where $S(B|E)$ is the conditional von Neumann entropy, $H(B|A)$ is the conditional Shannon entropy, E is all the information that Eve obtained, and A and B denote the raw keys, which are shared between Alice and Bob, respectively.

$H(B|A)$ is defined entirely in terms of the difference of raw keys shared between Alice and Bob. If we let the quantum bit error rate (QBER) between A and B be Q, one can get

$$H(B|A) = h(Q), \tag{9}$$

where h is a binary Shannon entropy function:

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

Thus we should essentially take $S(B|E)$ into account in order to compute the secret key rate of the SDI-QKD protocol. We show how to quantitatively characterize it as a function of the probability distribution $P(b|x,y)$ in the following.

Let $P_{\text{guess}}(B|E)$ be the probability that Eve correctly guesses Bob's raw keys B when using an optimal strategy, that is

$$P_{\text{guess}}(B|E) = \max_{b,x,y} P(b|x,y). \tag{10}$$

From Lemma 1, we know that the min-entropy can be rewritten as the negative logarithm of the optimal guessing probability

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

We can estimate the upper bound of all the information that Eve obtained about Bob's raw key by using the min-entropy bound $H_{\min}(B|E)$, then we can get

$$S(B|E) \geq H_{\min}(B|E) = -\log[\max_{b,x,y} P(b|x,y)]. \tag{12}$$

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

$$R \geq -\log[\max_{b,x,y} P(b|x,y)] - h(Q). \tag{13}$$

In order to characterize the secret key rate of the SDI-QKD protocol against collective attacks, we should get the upper bound of conditional probability distribution $P(b|x,y)$. We will use the method in Ref. [40] to solve this problem. The maximal conditional probability distribution $\max_{b,x,y} P(b|x,y)$ can be achieved by the following optimization equations[40]

$$\begin{aligned} &\text{minimize}: \ \max_{b,x,y} P(b|x,y); \\ &\text{subject to}: \ E_{x,y} = \text{tr}(\rho_x M_y^0), \\ &\qquad W = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} \\ &\qquad\quad - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1}, \end{aligned} \tag{14}$$

where the optimization is implemented by arbitrary quantum states ρ_x with $x \in \{00,01,10,11\}$ and measurement operators M_y^0 with $y \in \{0,1\}$ defined over two-dimensional Hilbert space.

In our numerical calculation, the preparation states and measurement operators can be given as follows (more specific reasons and processes can be found in Ref. [40]):

$$\begin{aligned} &\rho_x = |\phi(x)\rangle\langle\phi(x)| \text{ with} \\ &|\phi(x)\rangle = \begin{pmatrix} \cos(\theta_x/2) \\ \mathrm{e}^{\mathrm{i}\eta_x}\sin(\theta_x/2) \end{pmatrix}, \end{aligned} \tag{15}$$

$$M_0^0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$M_1^0 = \begin{pmatrix} \cos^2(\theta/2) & \mathrm{e}^{-\mathrm{i}\eta}\sin(\theta)/2 \\ \mathrm{e}^{\mathrm{i}\eta}\sin(\theta)/2 & \sin^2(\theta/2) \end{pmatrix}, \tag{16}$$

where $x \in \{00,01,10,11\}$, $0 \leq \theta_x, \theta \leq \pi$, $0 \leq \eta_x, \eta \leq 2\pi$.

By solving the minimization problem with the Levenberg–Marquardt algorithm,[45] we get the upper bound of all the information that Eve obtained about Bob's raw key $S(B|E) \approx 0.228$.

In order to compare with the secret key rate in standard QKD (e.g. BB84), we consider the secret key rate of ideal BB84 protocol against collective attacks in the asymptotic case, which is given as[1]

$$r \geq 1 - 2h(Q'), \tag{17}$$

where h is a binary Shannon entropy function and Q' is the QBER between Alice's and Bob's raw keys in BB84.

We assume a basic experimental setup where the quantum channel can be described as a depolarizing channel with visibility V in the absence of an eavesdropper. Thus, the QBER Q and Q' are equal to $(1-V)/2$. Lower bounds for the secret key rates as a function of visibility V are shown in Fig. 2. The simulation results show that the secret key rate of the SDI-QKD protocol is lower than the standard QKD. But we emphasize that SDI-QKD represents a relaxation of the assumption

in security proofs of standard QKD. Compared with standard QKD, there are some advantages in SDI-QKD. The prominent advantage is the same as DI-QKD with no assumptions about the internal workings of the quantum devices.

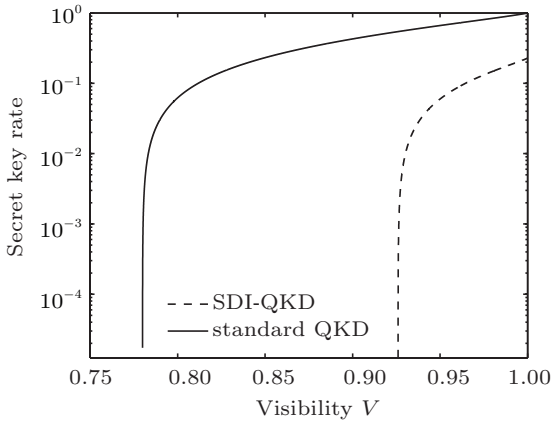


Fig. 2. Lower bound for the secret key rate as a function of visibility V. The dashed lines represent the SDI-QKD protocol considered in our paper and the solid lines represent an ideal BB84 protocol.

5. Conclusions

In this paper, we have proposed a practical SDI-QKD protocol with four preparation states and three measurement bases, which can be applied directly to the one-way configuration. Based on the min-entropy and dimension witnesses, we have also presented the security of the SDI-QKD protocol against collective attacks.

On one hand, the experimental demonstrations of estimating dimension witnesses in a prepare and measure scenario have been reported recently.[46,47] On the other hand, our SDI-QKD protocol is similar to the BB84 protocol. So the experimental demonstration of SDI-QKD can be analogously established with existing QKD devices.

In future works, similar to the security proof presented by Masanes *et al.*,[27] it is interesting to give an analytical bound of the eavesdropper's information by considering the quantum dimension witnesses violation W. If the experimental demonstration of SDI-QKD becomes real, the security of SDI-QKD in the presence of noise and imperfect detectors opens an interesting area to further research.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[2] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India) p. 175

[3] Li H W, Chen W, Huang J Z, Yao Y, Liu D, Li F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Li Y H, Yu N H and Han Z F 2012 *Sci. Sin.: Phys. Mech. Astron.* **42** 1237 (in Chinese)

[4] Zhou Z W, Chen W, Sun F W, Xiang G Y and Li C F 2012 *Chin. Sci. Bull.* **57** 1498 (in Chinese)

[5] Liu D, Yin Z Q, Wang S, Wang F M, Chen W and Han Z F 2012 *Chin. Phys. B* **21** 060202

[6] Zhou Y Y, Zhou X J, Tian P G and Wang Y J 2013 *Chin. Phys. B* **22** 010305

[7] Jiao R Z, Ding T, Wang W J and Ma H Q 2013 *Acta Phys. Sin.* **62** 180302 (in Chinese)

[8] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 3547

[9] Wang X Y, Bai Z L, Wang S F, Li Y M and Peng K C 2013 *Chin. Phys. Lett.* **30** 010305

[10] Zhao S M, Gong L Y, Li Y Q, Yang H, Sheng Y B and Cheng W W 2013 *Chin. Phys. Lett.* **30** 060305

[11] Guo B H, Yang L, Xiang C, Guan C, Wu L A and Liu S H 2013 *Acta Phys. Sin.* **62** 130303 (in Chinese)

[12] Lo H K and Chau H F 1999 *Science* **283** 2050

[13] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[14] Mayers D 2001 *J. ACM* **48** 351

[15] Koashi M 2009 *New J. Phys.* **11** 045018

[16] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506

[17] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

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

[19] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73

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

[21] Fung C H F, Qi B, Tamaki K and Lo H K 2007 *Phys. Rev. A* **75** 032314

[22] Xu F, Qi B and Lo H K 2010 *New J. Phys.* **12** 113026

[23] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686

[24] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349

[25] Li H W, Wang S, Huang J Z, Chen W, Yin Z Q, Li F Y, Zhou Z, Liu D, Zhang Y, Guo G C, Bao W S and Han Z F 2011 *Phys. Rev. A* **84** 062308

[26] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[27] Masanes L, Pironio S and Acín A 2011 *Nat. Commun.* **2** 238

[28] Pironio S, Masanes L, Leverrier A and Acín A 2013 *Phys. Rev.* X **3** 031007

[29] Bell J S 1964 *Physics* (NY) **1** 195

[30] Pearle P M 1970 *Phys. Rev. D* **2** 1418

[31] Pawłowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302

[32] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 *Phys. Rev. A* **85** 010301

[33] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2013 *Phys. Rev. A* **88** 052322

[34] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[35] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502

[36] Zhou C, Bao W S, Chen W, Li H W, Yin Z Q, Wang Y and Han Z F 2013 *Phys. Rev. A* **88** 052333

[37] Gallego R, Brunner N, Hadley C and Acín A 2010 *Phys. Rev. Lett.* **105** 230501

[38] Nayak A 1999 *Proceedings of 40th IEEE FOCS* p. 369

[39] Li H W, Yin Z Q, Wu Y C, Zou X B, Wang S, Chen W, Guo G C and Han Z F 2011 *Phys. Rev. A* **84** 034301

[40] Li H W, Pawłowski M, Yin Z Q, Guo G C and Han Z F 2012 *Phys. Rev. A* **85** 052308

[41] Ambainis A, Nayak A, Ta-Shma A and Vazirani U 2002 *J. ACM* **49** 496

[42] Hayashi M, Iwama K, Nishimura H, Raymond R and Yamashita S 2006 *New J. Phys.* **8** 129

[43] König R, Renner R and Schaffner C 2009 *IEEE Trans. Inf. Theory* **55** 4337

[44] Devetak I and Winter A 2005 *Proc. R. Soc. A* **461** 207

[45] Levenberg K 1944 *Q. Appl. Math.* **2** 164

[46] Hendrych M, Gallego R, Micuda M, Brunner N, Acín A and Torres J P 2012 *Nat. Phys.* **8** 588

[47] Ahrens J, Badziag P, Cabello A and Bourennane M 2012 *Nat. Phys.* **8** 592