Measurement-Device-Independent Quantum Key Distribution with Two-Way Local Operations and Classical Communications *

Yong-Gang Tan(谭勇刚)**, Qiang Liu(刘强)

Physics and Information Engineering Department, Luoyang Normal College, Luoyang 471022

(Received 18 May 2016)

Measurement-device-independent quantum key distribution (MDI-QKD) is proven to be immune to all the detector side channel attacks. With two symmetric quantum channels, the maximal transmission distance can be doubled when compared with the prepare-and-measure QKD. An interesting question is whether the transmission distance can be extended further. In this work, we consider the contributions of the two-way local operations and classical communications to the key generation rate and transmission distance of the MDI-QKD. Our numerical results show that the secure transmission distances are increased by about 12 km and 8 km when the 1 B and the 2 B steps are implemented, respectively.

PACS: 03.67.Dd, 03.67.Hk, 03.67.Mn DOI: 10.1088/0256-307X/33/9/090303

Quantum key distribution (QKD) is an art of generating secure key bits between remote partners, usually called Alice and Bob, in the presence of the eavesdropper, Eve.[1−3] Its security is based on the fundamental principles of quantum mechanics. The key bit string is proven to be unconditionally secure when ideal devices are used.[4,5] In practical implementation of QKD protocols, the QKD systems are imperfect. It is proven that secure key bit string can still be generated when the tagged key bits are well restricted.[6] For example, phase-randomized weakened coherent sources are used in practical QKD. There are multi-photon pulses emitted from the source. Eve can launch the photon-number-splitting (PNS) to tag the multi-photon events.[7,8] If the amount of the tagged event can be well bounded, secure key bits can be generated between remote partners.[9−12]

Recently, the detector side channel attacks have attracted great attention. Eve exploits the drawbacks of the detectors to control their detections. Moreover, the photons registered by the detectors may not be the ones expected by Bob, but well devised by Eve to obtain illegal information. In the fake state attack, Eve intercepts the photons from Alice and reads out the bit values on them. According to her measurement outcomes, she exploits the detection efficiency mismatches and prepares fake states to be detected by Bob.[13] The time-shift attack uses the detection efficiency mismatches to eavesdrop on the communication without intercepting on Alice's photons.[14,15] Furthermore, the problem of information leaking from the detector side channels also exists in the blinding attack[16−18,20] and the phase re-mapping attack.[21,22]

The security of the quantum cryptography (QC) is claimed to be superior to that of its classical counterpart because Eve's interventions inevitably cause disturbances. However, the detector side channel attacks cause great harm to the security of QKD due to the fact that Eve's illegal information gain obtained in the attacks cannot be well bounded.[6] Great improvement must be made to the detectors to avoid the detector side channel attacks.[19,23] Recently, it was proven the MDI-QKD protocol can be used to exclude all detector side channel information leaking.[24] In this protocol, Alice and Bob prepare their states on their photons and transfer them to be measured by an untrusted third party.[25,26] The monogamy of entanglement ensures the security of the final key bits.[27,28]

The MDI-QKD not only refutes the detector side channel attacks, but also doubles the transmission distance of the QKD. Thus an interesting question is whether the transmission distance can be extended further. In this work, we consider the contribution of the two-way local operations and classical communications (LOCC) on the key generation rate and transmission distance of the MDI-QKD. We will show that the transmission distance and the key generation rate of the MDI-QKD can indeed be increased by introducing the two-way LOCC. Numerical results show that one B step can increase the transmission distance of the MDI-QKD by 12 km, and another B step can increase the transmission distance by 8 km. Thus after two B steps, the total increased distance is calculated to be about 20 km. This is very attractive in practical implementation of MDI-QKD protocol.

The two-way LOCC was originally applied for entanglement distillation.[29−31] In the entanglement distillation protocols (EDPs), such as the Gottesman–Lo EDP and recurrence EDP, Alice and Bob use the two-way LOCC to correct the bit errors and phase errors on the entangled state. The Gottesman–Lo EDP consists of a series of B steps and P steps. In the B steps, Alice and Bob perform a bilateral XOR (BXOR) between pairs of the shared EPR pairs and

*Supported by the National Natural Science Foundation of China under Grant No 61378011, and the Program for Science and Technology Innovation Research Team in University of Henan Province under Grant No 13IRTSTHN020.

**Corresponding author. Email: ygtan@lynu.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

measure the target qubits in Z-basis.[29,32] If Alice and Bob's measurement outcomes disagree, they discard the remaining EPR pair. Otherwise, they keep the control qubit. In the P steps, Alice and Bob group the EPR pairs into sets of three, and measure X_1X_2 and X_1X_3 on each set.[29,32] If Alice and Bob disagree on one measurement, Bob will conclude that the phase error is probably on one of the EPR pairs which was measured, and carry out nothing; if both measurements disagree for Alice and Bob, Bob assumes that the phase error is on the surviving EPR pair and corrects it by performing a Z operation.

In the recurrence scheme, compared with the Gottesman–Lo EDP, Alice and Bob group the bit error syndromes of all target EPR pairs together and learn about all the syndromes using random hashing.[31] Furthermore, the recurrence scheme requires some extra maximally entangled EPR pairs to begin with to learn about the bit error syndromes. However, no extra pairs are required in the Gottesman–Lo EDP. Alice and Bob perform two BXOR operations on two noisy EPR pairs and one perfect maximally entangled EPR pair. The maximally entangled EPR pair is used as the target and the two noisy EPR pairs are used as the sources. Alice and Bob perform random hashing on the target EPR pairs to learn about the parities of the noisy EPR pairs. Then they perform error correction and privacy amplification for even-parity and odd-parity EPR pairs separately.

In the entanglement-based QKD, after applying the EDP, Alice and Bob implement the error correction and privacy amplification with one-way LOCC for key generation. The Gottesman–Lo EDP was shown to be able to achieve a higher tolerable bit error rate, while the recurrence method was shown to be able to achieve a higher key generation rate. This is also true for decoy state QKD. The bit flips and phase flips both affect the entanglement between Alice and Bob. Thus both the B steps and the P steps are important in the EDPs. In contributing the key generation rate, however, it is proven that the P steps are not as useful as the B steps. In the following we only consider the contribution of the B steps used in the Gottesman–Lo EDP.

In the MDI-QKD protocol, both Alice and Bob randomly choose between the rectilinear basis and the diagonal basis. Together with their randomly chosen bit values, they prepare their photons and transfer them to Eve who launches the Bell basis measurement (BSM) on the incoming photons.[24] After the BSM, Eve announces to Alice and Bob the measurement outcomes. Then they exchange information of basis choice and keep the events when the same bases are chosen. This process ensures that the photons prepared by Alice and Bob are post-selected to be entangled. Time reversely, entangled photon pairs are generated from the source located between Alice and Bob and distributed to them. That is, the MDI-QKD is a time-reversal entanglement-based QKD protocol. The security of the measurement outcomes relies on the monogamy of entanglement.[27,28]

In the MDI-QKD, the entanglement is post-selected from the BSM. Alice and Bob cannot apply the two-way LOCC directly on the entanglement state as that in the EDP. However, a QKD protocol based on Calderbank–Shor–Steane (CSS)[33,34] EDPs can be reduced to a prepare-and-measure protocol. CSS codes correct bit errors and phase errors separately, which respectively turn out to be the bit error correction and privacy amplification in the context of QKD. Then the security of MDI-QKD with two-way LOCC can be thought to be inherited from that of the entanglement-based QKD with EDP. The Shor–Preskill security proof of QKD shows that the leaked information about the final key is negligible.

In the MDI-QKD, the key generation rate is calculated to be[24]

$$R \geq Q_z^{1,1}[1 - h(e_x^{1,1})] - Q_z f(E_z) h(E_z), \qquad (1)$$

where $Q_z^{1,1}$ is the gain of the untagged events in the rectilinear basis, $e_x^{1,1}$ is the phase error on $Q_z^{1,1}$, Q_z and E_z are the total gains and total quantum bit error rate (QBER) in the rectilinear basis respectively, $f(E_z)$ is the efficient function of error correction, and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy.

Practically, weakened coherent sources are used both at Alice's side and at Bob's side. To avoid the PNS attack, decoy states are randomly added in. In this study, we consider the case that both sides have a signal state, a weaker decoy state and a vacuum decoy state. In this case, one can obtain the gains and the corresponding QBERs in the rectilinear basis and the diagonal basis[24]

$$\begin{aligned}
Q_z^{i,j} &= \sum_{m,n=0}^{\infty} \frac{\nu_i^m \nu_j^n}{m!n!} e^{-\nu_i-\nu_j} Y_z^{m,n}, \\
Q_x^{i,j} &= \sum_{m,n=0}^{\infty} \frac{\nu_i^m \nu_j^n}{m!n!} e^{-\nu_i-\nu_j} Y_x^{m,n}, \\
Q_z^{i,j} E_z^{i,j} &= \sum_{m,n=0}^{\infty} \frac{\nu_i^m \nu_j^n}{m!n!} e^{-\nu_i-\nu_j} Y_z^{m,n} e_z^{m,n}, \\
Q_x^{i,j} E_x^{i,j} &= \sum_{m,n=0}^{\infty} \frac{\nu_i^m \nu_j^n}{m!n!} e^{-\nu_i-\nu_j} Y_x^{m,n} e_x^{m,n}, \qquad (2)
\end{aligned}$$

where ν_i and ν_j are the intensities of the signal sources and the decoy sources at Alice's side and Bob's side, $Y_z^{m,n}$ and $Y_x^{m,n}$ are the yields in the rectilinear basis and in the diagonal basis when there are an m-photon pulse prepared at Alice side and an n-photon pulse prepared at Bob's side, and $e_z^{m,n}$ and $e_x^{m,n}$ are the error rates on the gains generated from the rectilinear basis and the diagonal basis, respectively.

The yield $Y_\alpha^{m,n}$ is calculated to be $Y_\alpha^m Y_\alpha^n$, with $\alpha \in \{x, z\}$. In Ref. [12], the lower bound of Y_α^1 can be well bounded with the decoy state technique. Thus

the lower bound of $Y_z^{1,1}$ is obtained. Similarly, $e_x^{m,n}$ is equal to $e_\alpha^m + e_\alpha^n - e_\alpha^m e_\alpha^n$. The upper bound of e_α^1 can also be obtained with the decoy state technique. Accordingly, the value of $e_x^{1,1}$ can be upper bounded. Then the gain $Q_z^{1,1}$ can be written as

$$Q_z^{1,1} = \mu_{\rm A}\mu_{\rm B} e^{-\mu_{\rm A}-\mu_{\rm B}} Y_z^{1,1}, \tag{3}$$

where $\mu_{\rm A}$ and $\mu_{\rm B}$ are the intensities of the signal pulses at Alice's side and at Bob's side, respectively. The total gain Q_z can be obtained by summing up the gains when there is an i-photon pulse at Alice's side and an j-photon pulse at Bob's side. The total QBER is the total error divided by the total gain. That is, one can obtain

$$\begin{aligned} Q_z &= \sum_{i,j} Q_z^{i,j}, \\ E_z &= \sum_{i,j} Q_z^{i,j} E_z^{i,j}/Q_z. \end{aligned} \tag{4}$$

Thus the key generation rate in Eq. (1) is calculated.

The two-way LOCC method based on post-processing can tolerate higher bit error rate and extend longer secure transmission distance than the one-way LOCC based on the entanglement distillation protocol (EDP).[29–31] The reason for tolerating a higher QBER is that its two primitives (B steps and/or P steps) can reduce the bit and/or phase error rate of qubits. The process of MDI-QKD with two-way LOCC is as follows: Alice and Bob perform a sequence of B steps to the sifted key bits. That is, Alice and Bob perform a bilateral XOR (BXOR) between pairs of the shared sifted keys and measure the target bits in rectilinear basis. If their measurement outcomes disagree, they discard both of the control and target bits. Otherwise, they only keep the control bits.[29,35] Thus in the B step process, only the events that Bob's results coincide with those of Alice's can survive.

The final secure key can only be distilled from the untagged qubits. Furthermore, the bit error correction and privacy amplification can only be applied to the remaining qubits which are still untagged at the end of some B steps. Thus in the sifted key bits, both the target bits and the source bits should be untagged. In the MDI-QKD, the key bits are untagged only when both sides have single-photon pulses for bit value preparations and simultaneously no phase error is gained. Therefore, the residue ratio of the key can be re-expressed, according to Eq. (1), as[35]

$$R_{\rm s} = r_{\rm B} Q_z \{\Lambda[1 - h(\tilde{E}_{\rm p}^{(\rm ut)}) - f(E)h(\tilde{E})]\}, \tag{5}$$

where $\tilde{E}$ is the QBER of overall survival states, $r_{\rm B}$ is the total survival residue, Λ is the fraction of untagged events in the final survival states (without B step, $\Lambda = Q_z^{1,1}/Q_z$), and $\tilde{E}^{(\rm ut)}$ is the phase error rate of the untagged states. In MDI-QKD, after one B step, the overall survival probability $P_{\rm S}$ and the survival probability of the untagged states $P_{\rm S}^{(\rm ut)}$ are expressed as

$$\begin{aligned} P_{\rm S} &= E^2 + (1-E)^2, \\ P_{\rm S}^{(\rm ut)} &= (E^{(\rm ut)})^2 + (1-E^{(\rm ut)})^2, \end{aligned} \tag{6}$$

where E is the overall QBER, and $E^{(\rm ut)}$ is the QBER of the untagged states. Then the residue after one B step can be written as

$$r_{\rm B} = \frac{1}{2} P_{\rm S}, \tag{7}$$

where the factor $\frac{1}{2}$ is given due to the fact that Alice and Bob only keep the control bits in the XOR process. At the same time, the fraction of untagged states $\Lambda_{\rm B}$, the QBER of the untagged states and the overall QBER $E_{\rm B}$ after one bit step are given by

$$\begin{aligned} \hat{\Lambda} &= \frac{\Lambda^2 P_{\rm S}^{(\rm ut)}}{P_{\rm S}}, \\ \hat{E}^{(\rm ut)} &= \frac{(E^{(\rm ut)})^2}{(E^{(\rm ut)})^2 + (1-E^{(\rm ut)})^2}, \\ \hat{E} &= \frac{E^2}{E^2 + (1-E)^2}. \end{aligned} \tag{8}$$

The phase error rate of untagged states after one B step is

$$\hat{E}_{\rm p}^{(\rm ut)} = \frac{2E_{\rm p}^{(\rm ut)}(1 - E^{(\rm ut)} - E_{\rm p}^{(\rm ut)})}{(E^{(\rm ut)})^2 + (1-E^{(\rm ut)})^2}. \tag{9}$$

According to Eqs. (5)–(9), the key generation rate and the secure transmission distance of the MDI-QKD protocol with one B step can be calculated. If more B steps are required, one only needs to repeat this procedure. In the following numerical simulation, one can see that the B step can indeed improve the performance on the secure transmission distance apparently.

The B steps will decrease the key generation rate due to the fact that some of the sifted key bits may be discarded within this process. When the transmission is comparably lower, the key generation rate of the MDI-QKD with two-way LOCC is lower than that of the MDI-QKD with one-way LOCC. When the transmission distance is long, however, the channel loss affect the QBER. According to Eqs. (8) and (9), the B steps decrease the phase error rate and the bit error rate if the QBER on the sifted key bits is much smaller than one. In this case, the key distribution distance may be significantly prolonged after the B step.

In the numerical simulation, for the parameters of this study taking those of the experiment by Ursin *et al.*,[36] efficiency of detector is fixed at 14.5%, and the background count rate is 6.02×10^{-6}. The loss coefficient of quantum channel is 0.2 dB/km, and the intrinsic error rate due to misalignment and instability of the optical system is 1.5%. Moreover, the error correction protocol with inefficiency function $f(E) = 1.16$. Substituting these parameters into Eq. (7), as illustrated in Fig. 1, the numerical relationship between

the key generation rate and the secure transmission distance can be obtained.

The solid line refers to the key generation rate of MDI-QKD with one-way LOCC, whose maximal transmission distance is about 226 km.[24] The solid and dashed curves are the improvements with the two-way LOCC on the key generation rate of the former. As illustrated in the figure, with one B step, the maximal secure transmission distance for the MDI-QKD can be enlarged from 226 km to 238 km, and the maximal secure transmission distance is about 246 km by using the two B steps. Thus the two B steps improve the maximal secure transmission distance by about 20 km. This confirms that the two-way LOCC can greatly improve the performance of the MDI-QKD protocol.

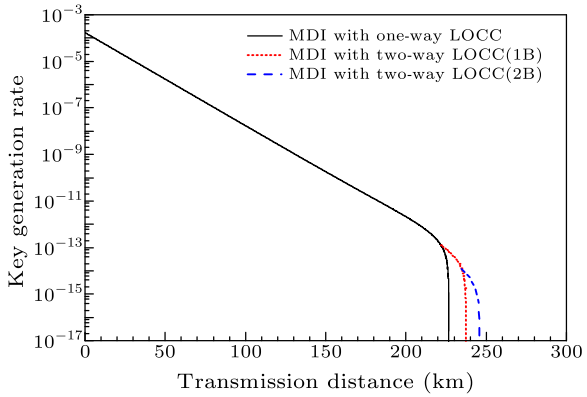

Fig. 1. (Color online) The relations between the the lower bound of the key generation rate and the secure key transmission distance. The solid line refers to the case when only one-way LOCC is used. The dotted line refers to the case of the two-way LOCC with the 1 B step. The dashed line refers to the case of the two-way LOCC with the 2 B step.

In summary, the crux of QKD is to generate secure keys between the legitimate users. Then the maximal transmission distance and the secure key generation rate are very important factors for QKD. In MDI-QKD protocol, Eve cannot obtain any information with passively monitoring the detectors or implementing a detector side-channel attack. This means that all detector side channels are closed in MDI-QKD.[37–41] Furthermore, the transmission distance can be doubled when compared with the traditional prepare-and-measure QKD. In this work, we have shown that the two-way LOCC method is an efficient way for extending the transmission distance of MDI-QKD further. The numerical simulation results indicate that about 12 km and 8 km of the secure transmission distance can be enlarged when one B step and two B steps are carried out, respectively.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Internatio Conference Computers, Systems and Signal Proces Bangalore* (India, December 9–12 1984) p 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Hoi-Kwong L and Chau H F 1999 *Science* **283** 2050
[6] Gottesman D, Hoi-Kwong L, Lü tkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **5** 325
[7] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[8] Lü tkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44.1-44.9
[9] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[10] Hoi-Kwong L, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[11] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[12] Ma X, Qi B, Zhao Y and Hoi-Kwong L 2005 *Phys. Rev.* A **72** 012326
[13] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[14] Qi B, Fred H, Hoi-Kwong L and Ma X F 2007 *Quantum Inf. Comput.* **7** 073
[15] Zhao Y, Fred H, Qi B, Chen C and Hoi-Kwong L 2008 *Phys. Rev.* A **78** 042333
[16] Makarov V 2009 *New J. Phys.* **11** 065003
[17] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[18] Yuan Z L, Dynes J F and Shields A J 2010 *Nat. Photon.* **4** 800
[19] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 801
[20] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[21] Fung C H F, Qi B, Tamaki K and Hoi-Kwong L 2007 *Phys. Rev.* A **75** 032314
[22] Xu F, Qi B and Hoi-Kwong L 2010 *New J. Phys.* **12** 113026
[23] Zhang J, Itzle M A, Zbinden H and Pan J W 2015 *Light: Sci. Appl.* **4** e286
[24] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[25] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651
[26] Inamori H 2002 *Algorithmica* **34** 340
[27] Wootters W K 1998 *Phys. Rev. Lett.* **80** 2245
[28] Coffman V Kundu J and Wootters W K 2000 *Phys. Rev.* A **61** 052306
[29] Gottesman D and Hoi-Kwong L 2003 *IEEE Trans. Inf. Theory* **49** 457
[30] Chau H F 2002 *Phys. Rev.* A **66** 060302
[31] Gerd K, Vollbrecht H and Verstraete F 2005 *Phys. Rev.* A **71** 062325
[32] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[33] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
[34] Steane A M 1996 *Proc. R. Soc. London* A **452** 2551
[35] Ma X, Fung C H F, Dupuis F, Chen K, Tamaki K and Hoi-Kwong L 2006 *Phys. Rev.* A **74** 032330
[36] Ursin R et al 2007 *Nat. Phys.* **3** 481
[37] Ma X, Fung C F and Razavi M 2012 *Phys. Rev.* A **86** 052305
[38] Ma X and Razavi M 2012 *Phys. Rev.* A **86** 062319
[39] Koashi M 2009 *New J. Phys.* **11** 045018
[40] Xu F, Curty M, Qi B and Hoi-Kwong L 2013 *New J. Phys.* **15** 113007
[41] Sun S H, Gao M, Li Y C and Liang L M 2013 *Phys. Rev.* A **87** 052329