CHIN. PHYS. LETT. Vol. 33, No. 10 (2016) 100301

Polarization-Encoding-Based Measurement-Device-Independent Quantum Key Distribution with a Single Untrusted Source *

Chuan-Qi Liu(刘传起), Chang-Hua Zhu(朱畅华)**, Lian-Hui Wang(王连辉),
Lin-Xi Zhang(张林曦), Chang-Xing Pei(裴昌幸)

State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071

(Received 13 April 2016)

Measurement-device-independent quantum key distribution (MDI-QKD) can be immune to all detector side-channel attacks and guarantee the information-theoretical security even with uncharacterized single photon detectors. MDI-QKD has been demonstrated in both laboratories and field-tests by using attenuated lasers combined with the decoy-state technique. However, it is a critical assumption that the sources used by legitimate participants are trusted in MDI-QKD. Hence, it is possible that a potential security risk exists. Here we propose a new scheme of polarization-encoding-based MDI-QKD with a single untrusted source, by which the complexity of the synchronization system can be reduced and the success rate of the Bell-state measurement can be improved. Meanwhile, the decoy-state method is employed to avoid the security issues introduced by a non-ideal single photon source. We also derive a security analysis of the proposed system. In addition, it seems to be a promising candidate for the implementation for QKD network in the near future.

PACS: 03.67.Ac, 03.67.Dd, 03.67.Hk, 42.50.Ex DOI: 10.1088/0256-307X/33/10/100301

Since the proposal of the Bennett–Brassard-1984 (BB84) quantum key distribution (QKD) protocol,[1] quantum secure communication based on QKD[1–4] together with one-time-pad(OTP)[5] encryption has been an active research field and developed quickly. The QKD systems have experienced demonstrations at the laboratories to practical field tests in a wide-area multi-user network. In the last few decades, QKD has been rigorously proved to offer unconditional security in communication between two remote parties, traditionally called Alice and Bob, with ideal source and detectors.[6] In addition, some semi-quantum key distribution (SQKD) protocols have also been discussed in the idealized scenario.[7] Moreover, quantum secure direct communication (QSDC) is a new research direction in the quantum cryptography. It is possible that, simultaneously, not only both parties are quantum, but also the sender Alice is classical and the receiver Bob is quantum, e.g., the semi-quantum secure direct communication (SQSDC) protocol.[8] Furthermore, its security is guaranteed by the complete robustness of SQKD protocols and the classical one-time pad encryption. Because of the unconditional security of quantum cryptography with its core of QKD, quantum signature has also been investigated.[9,10] However, throughout the whole development of QKD, there has always been struggle between attacks and anti-attack strategies, which mainly focus on the discrepancy between perfect theory and practice.[11] Typical attacks include photon number splitting (PNS) attack,[12,13] time-shift attack,[14,15] detector efficiency mismatch attack,[16] and phase-remapping attack,[17] etc. Among these attacks, the most harmful attack is the PNS attack, where an eavesdropper (Eve) stops all single-photon signals and splits multi-photon signals, keeping one copy herself and re-sending the rest to Bob. To avoid PNS attacks, the idea of decoy state was proposed.[18–21] To solve attacks against the measurement system, e.g., time-shift, phase-remapping attack, researchers proposed the measurement-device-independent quantum key distribution (MDI-QKD).[22] Hence, the MDI-QKD combined with decoy state can remove all detector side-channel attacks with imperfect single-photon sources. Numerous efforts have been devoted to research on the decoy state MDI-QKD protocol which has been extensively studied theoretically[23–29] and experimentally.[30–34]

Furthermore, the decoy state MDI-QKD technology can be used to build an MDI quantum network with an untrusted network server.[35] Nevertheless, a critical challenge in MDI-QKD network is to maintain the indistinguishability of all the users' lasers. Although the lasers are the same model, its performance may be different, e.g., the light pulse generated by each laser has a different spectrum, with which Eve can distinguish the light pulse by judging the spectrum of the light. Moreover, the performance of high-fidelity interference among photons from different lasers is also a crucial issue in real implementation. It is possible that a potential security risk exists in communication among the legitimate participants

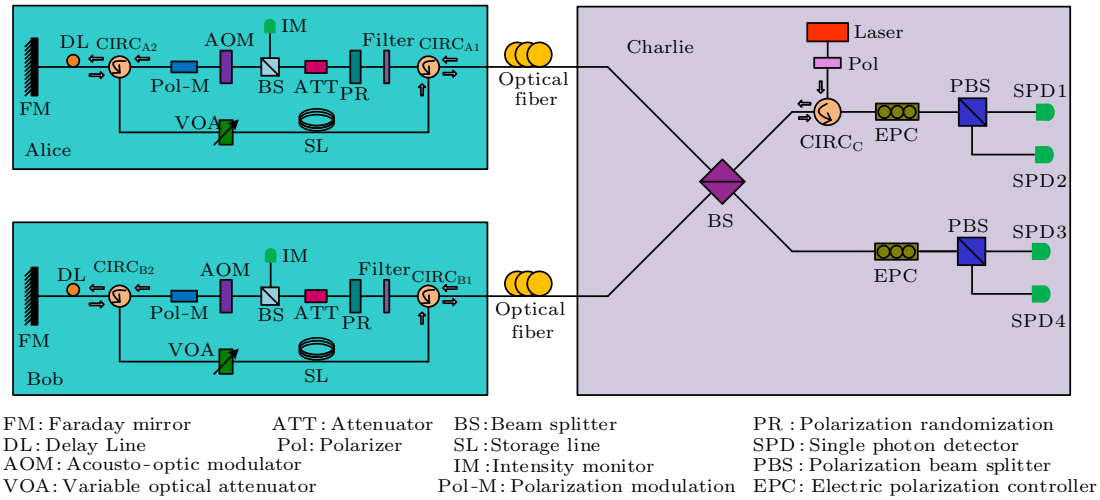
*Supported by the National Natural Science Foundation of China under Grant Nos 61372076 and 61301171, and the 111 Project under Grant No B08038.

**Corresponding author. Email: chhzhu@xidian.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

due to the fact that they believe that there are no security loopholes in the commercial compact lasers they use and trust. Actually, the lasers with sophisticated apparatuses are not perfect. To overcome the security loophole derived from an imperfect source, a time-bin-based MDI-QKD system with an untrusted source was proposed.[36] Motivated by the security analysis for the plug-and-play QKD system,[37] they derived a lower bound of the secure key generation rate. However, in the time-bin encoding scheme, the accuracy and coincidence of the prepared states $|+\rangle$ and $|-\rangle$ in X-basis by Alice and Bob are strongly influenced by phase modulators (PMs) and other components whose performance varies with temperature and stress. In addition, strict timing circuits are required at Alice's and Bob's systems for perfect overlapping. Although the widely applied polarization encoding-based QKD system[1,38] requires efficient polarization compensation, it does not need on-time and accurate phase modulation for perfect interference at the measurement device. In this Letter, we propose a new scheme of using a single untrusted source for polarization-encoding-based MDI-QKD. By connecting a storage line (SL), we can significantly minimize the effects of the Raleigh backscattering.[39,40] Moreover, in the real MDI-QKD system, it is usually used to reduce the adverse effect of intensity fluctuation on the system by combining the decoy state and intensity monitor scheme.[41] It can also overcome the Trojan horse attack[42] by using a light source monitor to control photon number distribution (PND) of the untrusted source. Furthermore, only one single untrusted source is used and the problem of multiple lasers can be removed.

The proposed scheme is shown in Fig. 1. There are an untrusted network server (Charlie) and two legitimate participants (Alice and Bob). Alice and Bob share beforehand a secret random bit string for authentication by using the classical channel which is used to transmit control information, and they negotiate parameters required by the protocol. Alice and Bob then perform a calibration measurement of their devices. Note that these previously shared secret bits must be discarded after use.



FM: Faraday mirror
DL: Delay Line
AOM: Acousto-optic modulator
VOA: Variable optical attenuator
ATT: Attenuator
Pol: Polarizer
BS: Beam splitter
SL: Storage line
IM: Intensity monitor
Pol-M: Polarization modulation
PR: Polarization randomization
SPD: Single photon detector
PBS: Polarization beam splitter
EPC: Electric polarization controller

Fig. 1. Schematic diagram of polarization encoding MDI-QKD with a single laser source.

The procedures of the protocol are as follows: (1) Preparing and transmitting: Untrusted server Charlie generates strong light pulses by laser. The pulses pass through a polarizer (Pol), and a circulator (CIRC$_c$), then are split into two parts by a beam splitter (BS). The strong light pulses propagate to Alice and to Bob through the optical fiber channel, respectively.

(2) Monitoring and encoding: When the pulses arrive at Alice (Bob), they first pass through a circulator CIRC$_{A1}$ (CIRC$_{B1}$) and enter into the upper branch and then pass through an optical filter (Filter), which removes the unexpected light signal. The phase of each individual pulse is actively randomized by a phase randomization (PR) in the range of $[0, 2\pi]$. The pulses are attenuated by an attenuator (ATT), and then pass through a monitoring unit which consists of a BS and an intensity monitor (IM). To implement the decoy-state method, intensities of pulses are randomly modulated by using an acousto-optic modulator (AOM) for generating the signal states and two decoy states. Then the polarization of each pulse is randomly encoded by a polarization modulator (Pol-M) in one of the four BB84 states (i.e., $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$). Finally, after passing through a CIRC$_{A2}$ (CIRC$_{B2}$) and delay line (DL), the pulses are reflected back by a Faraday mirror (FM), coupled into the other branch and again attenuated by a variable optical attenuator (VOA) to the light pulses with mean photon number μ, ν or ω (here μ denotes the mean photon number of signal state, ν and ω, respectively,

denote the mean photon number of the two decoy states). It is noteworthy that, as pulses travel back and forth in our scenario, the Rayleigh backscattering of the forward pulses can considerably increase the noise. To overcome this problem of the Rayleigh backscattering, we introduce a storage line (SL) behind the VOA in Alice's (Bob's) system.[39,40] Furthermore, we place a narrow bandpass filter with a single-mode fiber as the Filter in Fig. 1, which allows only a single mode in spectral and spatial domains to enter into the encoder.[36]

(3) The Bell state measurement (BSM): The polarization-encoding weak coherent pulses from Alice and Bob travel back through the two quantum channels, and arrive at Charlie's BS where they interfere. Then the photons are counted by four single-photon detectors (SPDs) after polarization beam splitters (PBS) which project the input photons onto either horizontal (H) or vertical (V) polarization states. Electrical polarization controllers (EPC) are used to compensate for the polarization rotations. Then the incoming photons may be projected into Bell states, $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$, or $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$.[22]

(4) Sifting: Charlie will use public channels to announce the events in which he obtained successful outputs. Alice and Bob keep the samples measured in the same bases for signal and decoy states after announcing their encoding bases, signal and decoy intensity levels by an authenticated public channel. Then they obtain the sifted key bits, while the rest will be discarded. For example, Alice and Bob encode their qubits in Z-basis or X-basis randomly. It is agreed that the two states $|H\rangle$ and$|+\rangle$ encode bit value '0', and the other two states $|V\rangle$ and $|-\rangle$ encode bit value '1'. Assume that a measured state by Charlie is $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$. If Alice and Bob picked the same basis, then they establish an anticorrelated key bit, that is, the two photons must have been in orthogonal states (e.g., the state of Alice is $|H\rangle$, then Bob $|V\rangle$). Therefore, to guarantee that their bit strings are correctly correlated, either Alice or Bob flips her or his bits, except for the cases where both of them select the X-basis and the obtained outputs a triplet state by Charlie.[22]

(5) Post-processing: After obtaining the sifted key, Alice and Bob use the classical channel to compare some part of their data and calculate the error rate. They can perform an error correction using the data reconciliation process. Finally, Alice and Bob apply the privacy amplification to extract the final unconditional secure key bits.

Now we analyze the security of our protocol. The security of the protocol is inspired by the security proof of a time-reversed Einstein–Podolsky–Rosen-(EPR-) based QKD protocol,[43,44] the plug-and-play QKD[37] and the decoy state method. We also use a virtual qubit idea. One can imagine that two EPR pairs are generated by any other party, with one particle of each pair being sent to the third party, Charlie, and the other to Alice and to Bob respectively as a virtual qubit. The virtual qubit is subsequently measured, and a BB84 state is thus prepared. In fact, in principle, each one could keep his or her virtual qubit in his or her quantum memory and delay his or her measurement on it. What we consider is the case where the measurement result is a singlet state, since the security of the EPR protocol relies on the fact that the singlet state is the only state in which the polarization states of the two particles are anticorrelated in both the rectilinear basis Z and the diagonal basis X. Only after Charlie has announced that he has obtained a successful outcome (that is, a singlet) will each perform a measurement on his or her virtual qubit to decide which state he or she is sending to Charlie. Thus in such a virtual qubit setting, our protocol is actually equivalent to an entanglement-based protocol. Alice and Bob share a pair of qubits in their quantum memories, and they can compute the quantum bit error rate (QBER) on their virtual qubits. Furthermore, by the analysis of gain and QBER of the untagged pulses in the plug-and-play MDI-QKD system, even if Charlie/Eve is given greater power since he can control the source, it is still possible to achieve the unconditional security, for he does not know whether the pulses are tagged or not.[36,37] Moreover, Alice and Bob can test the honesty of Charlie/Eve by comparing a random portion of their bits. Additionally, the results of BSM by Charlie/Eve are just used to check the parity of the two parties' bits, and thus Charlie/Eve cannot obtain any information on the bit values. Thus our protocol is practically secure and ready for implementation.

The key rate of the proposed scheme in the asymptotic case of infinite decoy states is given by[36]

$$R \geq (1-\Delta_{\rm a}-\varepsilon_{\rm a})(1-\Delta_{\rm b}-\varepsilon_{\rm b})Q_{11}^{Z}[1 - H_2(e_{11}^{X})] - Q_{e,\mu\mu}^{Z} f_{\rm e}(E_{e,\mu\mu}^{Z}) H_2(E_{e,\mu\mu}^{Z}), \quad (1)$$

where $\Delta_{\rm a}$ ($\Delta_{\rm b}$) is the average probability with which a sampling pulse at Alice (Bob) belongs to a tagged sampling pulse in the asymptotic case, $\varepsilon_{\rm a}$ ($\varepsilon_{\rm b}$) is the error probability due to statistical fluctuations, Q_{11}^{Z} and e_{11}^{X} are, respectively, the gain (the probability of a successful projection onto $|\psi^+\rangle$ or $|\psi^-\rangle$ per emitted pair of untagged pulse given that both Alice and Bob send single-photon states) in the Z-basis and the error rate (the ratio of erroneous to the total projections) in the X-basis, $Q_{e,\mu\mu}^{Z}$ and $E_{e,\mu\mu}^{Z}$ are, respectively, the overall gain and qubit error rate in the Z-basis when Alice and Bob send signal states, the subscript e denotes the experimentally measurable overall properties and μ is the intensity of the

signal state, H_2 is the binary entropy function given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, f_e is the error correction inefficiency function. The values of Δ_a, Δ_b, ε_a, ε_b, $Q^Z_{e,\mu\mu}$ and $E^Z_{e,\mu\mu}$ can be measured in the experiment, while Q^Z_{11} and e^X_{11} are estimated from the decoy states.[36] The numerical results of the key rate shown in Eq. (1) can be obtained in Ref. [36] since the analysis method and the result are the same.

In summary, we have proposed a novel scheme of polarization-encoding-based decoy state MDI-QKD with a single untrusted source. By this scheme high-fidelity interference among photons can be implemented, the complexity of synchronization system can be reduced, and the success rate of the Bell state measurement (BSM) can be improved. Furthermore, the decoy state technology can solve the risk that weak coherent pulses (WCPs) occasionally give out more than one photon and can open the door for a practical quantum secure communication. Therefore, combining the plug-and-play structure and the decoy state MDI protocol for QKD, our proposal suggests an important avenue for a wide-area QKD network with both practical performance and security. In addition, the experimental work on MDI-QKD implementation with polarization encoding has been presented recently,[34] while our scheme is also practical and feasible technology for secure communication, including technology from different vendors, which is important in view of open quantum networks.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* (Bangalore India) p 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[5] Vernam G S 1926 *J. A. I.E.E.* **45** 109
[6] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[7] Zou X F, Qiu D W, Li L Z et al 2009 *Phys. Rev.* A **79** 052312
[8] Zou X F and Qiu D W 2014 *Chin.-Phys. Mech. Astron.* **57** 1696
[9] Zou X F and Qiu D W 2010 *Phys. Rev.* A **82** 042325
[10] Zou X F, Qiu D W and Mateus P 2013 *Int. J. Theor. Phys.* **52** 3295
[11] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
[12] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[13] Brassard G, Lutkenhaus N, Mor T et al 2000 *Phys. Rev. Lett.* **85** 1330
[14] Qi B, Fred Fung C H, Lo H K et al 2006 *Quantum Inf. Comput.* **7** 73
[15] Zhao Y, Fred Fung C H, Qi B et al 2008 *Phys. Rev.* A **78** 042333
[16] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
[17] Fred Fung C H, Qi B, Tamaki K et al 2007 *Phys. Rev.* A **75** 032314
[18] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[19] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[20] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[21] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[22] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[23] Ma X F and Razavi M 2012 *Phys. Rev.* A **86** 062319
[24] Wang X B 2013 *Phys. Rev.* A **87** 012320
[25] Dong C, Zhao S H, Zhao W H et al 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese)
[26] Xu F H, Xu H and Lo H K 2014 *Phys. Rev.* A **89** 052333
[27] Fu Y, Yin H L, Chen T Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[28] Yu Z W, Zhou Y H and Wang X B 2015 *Phys. Rev.* A **91** 032318
[29] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys.* B **24** 120307
[30] Rubenok A, Slater J A, Chan P et al 2013 *Phys. Rev. Lett.* **111** 130501
[31] Liu Y, Chen T Y, Wang L J et al 2013 *Phys. Rev. Lett.* **111** 130502
[32] Ferreira da Silva T, Vitoreti D, Xavier G B et al 2013 *Phys. Rev.* A **88** 052303
[33] Tang Z Y, Liao Z F, Xu F H et al 2014 *Phys. Rev. Lett.* **112** 190503
[34] Choi Y, Kwon O, Woo M et al 2016 *Phys. Rev.* A **93** 032319
[35] Tang Y L, Yin H L, Zhao Q et al 2016 *Phys. Rev.* X **6** 011024
[36] Xu F H 2015 *Phys. Rev.* A **92** 012333
[37] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev.* A **77** 052327
[38] Liu W T, Wu W, Liang L M, Li C Z and Yuan J M 2006 *Chin. Phys. Lett.* **23** 287
[39] Ribordy G, Gautier J D, Gisin N et al 2000 *J. Mod. Opt.* **47** 517
[40] Gui Y Z, Han Z F, Mo X F and Guo G C 2003 *Chin. Phys. Lett.* **20** 608
[41] Xu F X, Zhang Y, Zhou Z et al 2009 *Phys. Rev.* A **80** 062309
[42] Gisin N, Fasel S, Kraus B et al 2006 *Phys. Rev.* A **73** 022320
[43] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651
[44] Inamori H 2002 *Algorithmica* **34** 340