SCIENTIFIC REPORTS

OPEN

Detector-device-independent quantum secret sharing with source flaws

Received: 10 August 2017
Accepted: 22 March 2018
Published online: 10 April 2018

Xiuqing Yang[1], Kejin Wei[2], Haiqiang Ma[3], Hongwei Liu[3], Zhenqiang Yin[4], Zhu Cao[5] & Lingan Wu[6]

Measurement-device-independent entanglement witness (MDI-EW) plays an important role for detecting entanglement with untrusted measurement device. We present a double blinding-attack on a quantum secret sharing (QSS) protocol based on GHZ state. Using the MDI-EW method, we propose a QSS protocol against all detector side-channels. We allow source flaws in practical QSS system, so that Charlie can securely distribute a key between the two agents Alice and Bob over long distances. Our protocol provides condition on the extracted key rate for the secret against both external eavesdropper and arbitrary dishonest participants. A tight bound for collective attacks can provide good bounds on the practical QSS with source flaws. Then we show through numerical simulations that using single-photon source a secure QSS over 136 km can be achieved.

Quantum secret sharing (QSS) is a multiparty protocol[1–4] to distribute a secret to a network of players, each of whom is allowed to access a share of the secret. It is possible for them to obtain the final key only if they all say yes. Secret sharing has many useful applications in network-based scenario, ranging from online auctioning, remote voting, master key of nuclear missile to multiparty secure computation. One of the desirable protocols for QSS is that three parties Alice, Bob and Charlie share the GHZ state $|\Phi_0^{\pm}\rangle=(|000\rangle\pm|111\rangle)/\sqrt{2}$. Each of them randomly perform a projection measurement on their own photons either along X basis or along Y basis. The results of the three members in some measurement basis have perfect correlation and therefore can be used for QSS. As Charlie will obtain a deterministic outcome, e.g., $X_c=X_a\oplus X_b$, she can force Alice and Bob to share the secret key with her only after performing a cooperative operation.

Compared with quantum key distribution (QKD), the security analysis of the multiparty protocol is complicated and its security has been challenged over time. The deviations between the components used for experimental realizations and the models in the security proof have led to information leaking to the eavesdropper. For example, Although it was claimed that a QSS procedure can be securely implemented using GHZ state[3], we find out it is potentially vulnerable to a double blinding-attack by exploiting controllability of single-photon avalanche-photodiode-based detectors of both Alice and Bob instead of one[5]. That is, Eve intercepts the photon sent by Charlie and then performs measurements in random basis, as Alice (Bob) would have done it. In order to hide her presence, Eve blinds Alice's (Bob's) detectors so that the detector click only when the signal with peak power above a threshold P_{th} is reaching. After each detection, Eve forwards to Alice (Bob) a bright pulse corresponding to her measurement result, which deterministically gives Eve the same result as Alice's (Bob's) if their bases are identical, and no result at all if not. After Eve discards the few faked state in the reconciliation between Alice and Bob, she has the same bit value as theirs.

For practical QKD, the most general threats seem to be introduced by exploiting controllability of measurement devices including basis-choice apparatuses and single photon detector (SPD). Security threats like this are more implementation-friendly, of which time-shift attack[6], after-gate attack[7], blinding attack[5] and laser damage[8]

[1]College of Science, Inner Mongolia University of Technology, Hohhot, 010051, China. [2]Guangxi Key Laboratory for Relativistic Astrophysics, School of Physics Science and Technology, Guangxi University, Nanning, 530004, China. [3]School of Science, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [4]Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China. [5]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084, China. [6]Laboratory of Optical Physics, Institute of Physics, Chinese Academy of Sciences, Beijing, 100080, China. Correspondence and requests for materials should be addressed to K.W. (email: kjwei@gxu.edu.cn) or Z.Y. (email: yinzheqi@mail.ustc.edu.cn)

attack have been demonstrated successfully. Scientists have put much effort towards building loophole-free QKD systems with untrusted devices. One important approach is to develop device independent protocols. Among them, the measurement-device-independent quantum key distribution (MDI-QKD)[9] is automatically immune to all side-channel attacks by allowing Eve to fully control the measurement device. Recently, a detector-device-independent quantum key distribution (DDI-QKD)[10] has been to proposed to exhibit a connection between the MDI-QKD and conventional BB84-like protocol. Although DDI-QKD is not precisely as secure as MDI-QKD, it may possess a high key rate of conventional QKD and exceed the performance and practicality of MDI-QKD in circumventing detector side channels. One crucial assumption behind DDI-QKD is that the linear optical elements of Bell-state measurement (BSM) must be trusted or some trustworthiness to the untrusted BSM device is required[11].

Compared with QKD, both theoretical and experimental works on real applications in secure multiparty communication, such as QSS[12,13], are rare. Following a similar spirit to DDI-QKD, we propose a detector-device-independent quantum secret sharing (DDI-QSS) protocol against all detector side-channels. The DDI-QSS protocol is designed to distribute a secret only when a separable state will never be wrongly identified as an entangled one based on measurement-device-independent entanglement witness (MDI-EW)[14,15]. We remark that source flaws are a serious concern in practical communication, not only in decoy-state QKD implementation but also in multiparty tasks including the fascinating MDI-QSS. For this reason, until now, the practicality of long-distance multiparty communication tasks has remains unknown. What we propose here is an entirely new approach to distributing a secret to the two authorized parties over long distances despite the source flaws. We obtain a condition on secure key against general attacks of an eavesdropper and cheating methods of dishonest players, and we prove that its security is independent of source error.

Measurement-device-independent entanglement witness

It is known that there always exist an MDI-EW for any entangled state with untrusted measurement, even if the measurement devices are controlled by Eve. There are two situations in the so-called semiquantum nonlocal games. One would be a case where Alice and Bob want to verify their entanglement themselves. They prepare some ancillary state pairs (τ_s, ω_t), and send them along with the bipartite state ρ_{AB} to Eve. Eve performs two Bell-state measurement(BSMs) on $\rho_A(\rho_B)$ and $\tau_s(\omega_t)$, and gets some classical output a and b. For a bipartite entangled state ρ_{AB}, we always find a conventional entanglement witness W decomposed in the form

$$W=\sum_{s,t}\beta_{s,t}\tau_s^T\otimes\omega_t^T, \tag{1}$$

with real coefficients $\beta_{s,t}$ such that $tr(W\rho_{AB})<0$, while $tr(W\sigma_{AB})\geq 0$ for all separable states σ_{AB}. In the MDI-EW design, an witness detecting the entanglement of ρ_{AB} can be obtained by

$$I(\rho_{AB}^{v})=\sum_{s,t}\beta_{s,t}^{+,+}p(+,+|\tau_s,\omega_t), \tag{2}$$

where $\beta_{s,t}^{+,+}=\beta_{s,t}$ and the probability distribution $p(+,+|\tau_s,\omega_t)$ is obtained by projecting onto the maximally entangle state $|\Phi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$. Mathematically, $I(\rho_{AB}^{v})$ is always positive for all separable states, but is negative for certain entangled states. We show that Alice and Bob can obtain secure key in a MDI-EW scenario. We prove the security of practical QKD system is independent of source flaws.

Another situation would be a case where the third party wants to be convinced two untrusted members share entanglement. For example, Charlie who is in the parent company wants to identify whether an bipartite state ρ_{AB} is entangled in an untrused scenario. Similar to the above case, Charlie sends quantum state (τ_s, ω_t) to Alice and Bob, who perform BSMs on $\rho_A(\rho_B)$ and $\tau_s(\omega_t)$. Note that in both cases, it requires that the input states must be perfect. When using imperfect states, the MDI-EW could wrongly conclude a separable state to be entangled due to imperfect input state and thus indeed leads to an erroneous estimation of $I(\rho_{AB}^{v})$.

Protocol

The task of secret of sharing is as follows. Charlie, the president of a bank, wants to give access to a vault to two vice presidents, Alice and Bob. Instead of giving the combination to anyone individual, Charlie transmit a qubit string to Alice and Bob. It may be desirable to distribute information in such a way that using the MDI-EW Charlie detects an entangled state ρ_{AB} and perfect correlations among Alice, Bob and Charlie are obtained for QSS. There exists an equivalence between the security of the QSS and the success of the EW because it is crucial for Charlie to prove that a given state is entangled or not. Originating from this analogy, we propose a practical QSS protocol with untrusted detectors used in an EW process. However, a crucial assumption for the present protocol is that the linear optical elements of BSM inside the receivers' laboratories must be trusted. That is measurement device is assumed to be a well-defined projective measurement acting on the two photons. This is indeed similar to the case in the concept of DDI-QKD, which requres perfect linear optical elements of BSM.

In the following, we design DDI-QSS scheme in a MDI-EW process. As shown in Fig. 1, Charlie prepares single-photon input state pairs $(\tau_s, \omega_t)\in\{|H,H\rangle, |H,V\rangle, |V,H\rangle, |V,V\rangle, |D,D\rangle, |D,\widetilde{D}\rangle, |\widetilde{D},D\rangle, |\widetilde{D},\widetilde{D}\rangle, |L,L\rangle, |L,R\rangle, |R,L\rangle, |R,R\rangle\}$, from spontaneous parametric down-conversion (SPDC) processes. Charlie sends quantum states pairs, τ_s to Alice and ω_t to Bob, who in this scenario do share some certain quantum states. More precisely, we consider the two-qubit Werner state

$$\rho_{AB}^{v}=v|\Psi^-\rangle\langle\Psi^-|+(1-v)I/4, \tag{3}$$

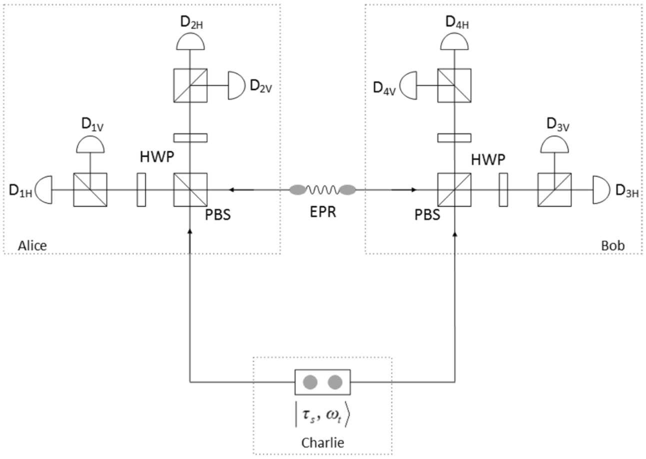

Figure 1. The schematics of the experimental setup for the DDI-QSS. Charlie prepare single-photon state pairs $|\tau_s, \omega_t\rangle$ as the signal states. The Werner state preparation setup consist of photon pairs generation by spontaneous parametric down conversion (SPDC). The experimental setup for Bell analysers consist of polarizing beam splitter (PBS) and half-wave plate (HWP) at 22.5°. All the photons are detected by sing-photon detector D.

Alice	Bob	Charlie
$\lvert\Phi^+\rangle$	$\lvert\Phi^+\rangle$	$\lvert D, \widetilde{D}\rangle$ or $\lvert\widetilde{D}, D\rangle$
$\lvert\Phi^+\rangle$	$\lvert\Phi^-\rangle$	$\lvert D, D\rangle$ or $\lvert\widetilde{D}, \widetilde{D}\rangle$
$\lvert\Phi^-\rangle$	$\lvert\Phi^+\rangle$	$\lvert D, D\rangle$ or $\lvert\widetilde{D}, \widetilde{D}\rangle$
$\lvert\Phi^-\rangle$	$\lvert\Phi^-\rangle$	$\lvert D, \widetilde{D}\rangle$ or $\lvert\widetilde{D}, D\rangle$

Table 1. Correlations among Alice, Bob and Charlie in the *X* Basis.

with the visibility $v \in [0, 1]$ and the singlet state $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Alice and Bob project their part of shared state together with these input states onto the maximally entangle state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ or $|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$. To implicitly express MDI-EW in the form of Eq. (2), we define a possible decomposition for an EW

$$W = \frac{1}{2}\mathbb{1} - |\Psi^-\rangle\langle\Psi^-|, \tag{4}$$

on the basis of three Pauli matrices. Then we get

$$\begin{aligned} I \;=\; & \frac{2}{6}P(+,+|H,H) - \frac{1}{6}P(+,+|H,V) \\ & -\frac{1}{6}P(+,+|V,H) + \frac{2}{6}P(+,+|V,V) \\ & +\frac{2}{6}P(+,+|D,D) - \frac{1}{6}P(+,+|D,\widetilde{D}) \\ & -\frac{1}{6}P(+,+|\widetilde{D},D) + \frac{2}{6}P(+,+|\widetilde{D},\widetilde{D}) \\ & +\frac{2}{6}P(+,+|L,L) - \frac{1}{6}P(+,+|L,R) \\ & -\frac{1}{6}P(+,+|R,L) + \frac{2}{6}P(+,+|R,R). \end{aligned} \tag{5}$$

With the MDI-EW method, Charlie will allow two legitimate users, Alice and Bob, to jointly share the secret key with her. Entanglement witness is estimated with three different bases, but the secret key is extracted in the *X* basis. Charlie encodes $|\Phi^+\rangle$ as 1 and $|\Phi^-\rangle$ as 0, while Alice and Bob encodes $|D, D\rangle$ ($|\widetilde{D}, \widetilde{D}\rangle$) as 0 and $|D, \widetilde{D}\rangle$ ($|\widetilde{D}, D\rangle$) as 1. In each quantum transmission, Charlie prepares state pairs in a basis which makes it easy to detect entanglement and distribute a secret with high efficiency. Compared to similar protocols, it does not require announcing basis choice and discarding those data in different basis. When quantum state they share is entangled, we can obtain the perfect correlation among Alice, Bob and Charlie in some successful outcomes. As illustrated in Table 1, the key is extracted from the data of *X* basis except for those data used to identify entanglement. It is clear that after Charlie split a message into two parts, neither Alice nor Bob can it but they together can.

In our scenario, based on the MDI-EW perfect correlations among Alice, Bob and Charlie are obtained, and therefore can be used for QSS without trusting their detectors. Considering some attacks on QKD based on the detection efficiency loophole, the detectors used by Bob will report no detection, or have a low detection efficiency when Eve's and Bob's setting differ. Similarly, Eve wants to determine a Bell state projection $|\Phi^{+}\rangle$ by remotely influencing the influencing the detectors, so that Bob is only to allowed to produce a specified output, maybe double-click D_{3H} and D_{4H}. As a result, in this run the other possible output D_{3V} and D_{4V} for $|\Phi^{+}\rangle$ can not be observed. This attack is simialr to time-shift attack on QKD, however, it could not break the QSS system. We emphasize that the MDI-EW is not prone to any detection loophole, contrary to standard EW, and the present protocol is naturately immune to attacks by exploiting detection efficiency loophole, including the overwhelming blinding attack. Importantly, Alice, Bob and Charlie can obtain an information-theoretically secure key in an entanglement witness process.

Security analysis

Collective attacks. For charlie the purpose of QSS protocol can be recognized as an equivalent one to verify entanglement, which is also the purpose of entanglement witness. We note that there are two parameters, the value of entanglement witness I and the error rate in the X basis e_x that used to quantify Eve's information. Without loss of generality, we can suppose the bipartite state for Alice and Bob is two-qubit Bell-diagonal state[16–18] $\rho_{AB} = \lambda_1|\Phi^{+}\rangle\langle\Phi^{+}| + \lambda_2|\Phi^{-}\rangle\langle\Phi^{-}| + \lambda_3|\Psi^{+}\rangle\langle\Psi^{+}| + \lambda_4|\Psi^{-}\rangle\langle\Psi^{-}|$, with $\sum_i \lambda_i = 1$. The reason is as follows. Due to symmetry, we should have obtained the correlations $P(1, 1) = P(0, 0)$ and $P(0, 1) = P(1, 0)$, where P is the probability to get a pair of $a, b \in \{0, 1\}$ with respect to three basis. Were this not the above symmetric scenario, we can apply a similar idea to the DDI-QSS and agree on permuting and flipping randomly a chosen half of their bit pairs[19,20]. The bit flip procedure would not change the above parameters, and would be public in classical communication. The symmetry of this protocol implies they can bound Eve's information by restricting to collective attacks such that the initial quantum state ρ_{AB}^{v} can be transformed into a Bell-diagonal state[21]. Following the QKD protocol[16], for collective attacks Eve's information is given by the Holevo quantity $\chi(A|E) = \chi(B|E) \le h\left(4I + \frac{1}{2}\right)$. With the observed parameters I and e_x, the key rate is

$$r \ge 1 - h(e_x) - h\left(4I + \frac{1}{2}\right), \tag{6}$$

where h is the binary entropy.

It is worth noting that dut to the imperfect states, the MDI-EW may consider some biseparable states as an entangled one. In the same manner, we repeat an argument for the DDI-QSS: the security in practical system is source-error-independent. To quantify the quantum states, the states to Alice can be written as $|\alpha_1\rangle$, $|90° + \alpha_2\rangle$, $|45° + \alpha_3\rangle$, $|-45° + \alpha_4\rangle$, $|e^{i(45\circ + \alpha_5)}\rangle$ and $|e^{i(-45\circ + \alpha_6)}\rangle$, with modulation error α_1, α_2, α_3, α_4, α_5 and α_6. Meanwhile, the situation is similar for Bob's states. For a Bell-diagonal state, we thus obtain $I' > I$. This implies the perfect sources witness entangled states in the worst case compared to the flawed sources. The secret key rate in practical QSS system thus can be give by Eq. 6. Compared with the postselected GHZ states scheme[12], we obtain a long distribution distance among Alice, Bob and Charlie for practical QSS with the source flaws.

Participant attacks. We point out here using the MDI-EW method, we provide condition on the secure key against both external eavesdropper and dishonest participants. The main idea in our approach, to deal with arbitrary cheating strategies is that Charlie wants to identify whether the two untrusted parties, Alice and Bob, share entanglement according to input and output of the BSM. It is a natural assumption that the dealer Charlie is considered to be trusted party with trusted device.

Suppose that Bob is a dishonest player, he expects to access Alice's secret by himself entirely bypassing the aforementioned collaboration with Alice. A most general cheating strategy for Bob would be the below attack. First, he performs the BSM using his local measurement ω_t, b. Meanwhile, he also intercepts the signal sent from Charlie to Alice and performs Bell state measurement τ_s, a. Second, according to detection outcome a he tells Alice's device to produce specified value as outputs so that the procedure for secret sharing deviates from the protocol. Bob can therefore determine Alice's value based on the following rules: If Bob obtain $|\Phi^{+}\rangle$ or $|\Phi^{-}\rangle$, he will send the corresponding single-photon state pairs $|D, D\rangle$ or $|D, \widetilde{D}\rangle$ to Alice. In other cases, he will send state pairs $|H, H\rangle$, $|V, V\rangle$ or no detection to Alice. Receiving the state pairs, Alice's detection probability is only 50% for $|\Phi^{+}\rangle$ and $|\Phi^{-}\rangle$. For this reason, Bob's BSM probability is twice as big as Alice's. However, Bob can carefully control the announcement rate to make it compatible with Alice's results so that Bob can conceal his cheating in a postselection process.

The cheating strategy discussed above can be partly prevented by a modified protocol so that Bob hardly simulate a entanglement witness based on three bases. The DDI-QSS protocol uses the data in the X basis to extract secure key and the Z, Y basis to test entanglement. Hence, Alice can choose a small fraction of Z, Y basis so that it is sufficient to evaluate the entanglement witness. After Alice and Bob announce the measurement results, Charlie calculates the BSM probability corresponding to three basis. When the statistical result deviates a desired range, they will abort it. As a result, Bob's cheating strategy is inefficient to generate a key by himself.

Simulation. We give a numerical simulation using an ideal single-photon source prepared by Charlie and one EPR state (singlet) prepared by an eavesdropper. We consider the conditions of detection from the paper[22] with a detection efficiency of $\eta = 0.1$ and a dark count rate $d = 10^{-5}$, whereas here we consider a fiber-based channel. Then the probability for a detector to record a photon through transmission distance l is $p_\rho = \eta 10^{-\alpha l/10}$, with a loss coefficient $\alpha = 0.2$ dB/km. The polarization misalignments and losses of the transmissions of the four quantum channels (i.e., Charlie to Alice and Bob, EPR source to Alice and Bob) are assumed to be identical.

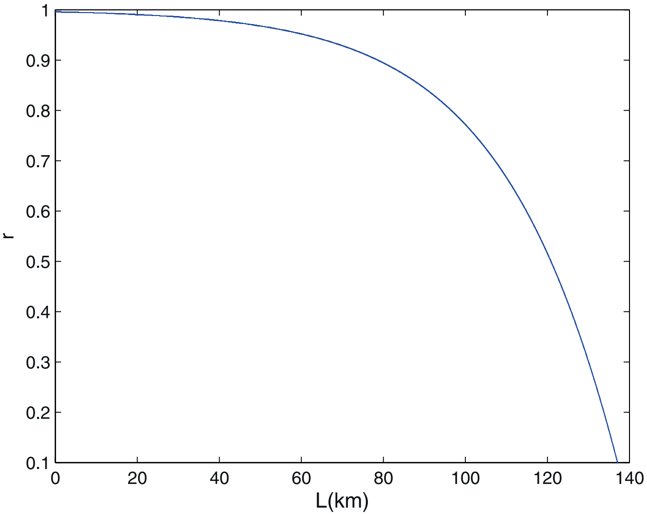

Figure 2. Lower bound on the key rate (per sifted key bit) versus fiber channel transmission from Charlie (EPR source) to Alice (Bob). A secret key rate with perfect single-photon states is illustrated. We show the simulation result of four identical quantum channels for the given parameters.

For post-processing, Charlie evaluates the data of I and the data of e_x separately. We consider actual detection condition, in which the probability corresponding to two successful Bell-state measurement in three bases is $p_d = p_\rho^3(1-p_\rho)d(1-d)^4 + 6p_\rho^2(1-p_\rho)^2 d^2(1-d)^4 + 8p_\rho(1-p_\rho)^3 d^3(1-d)^4 + 16(1-p_\rho)^4 d^4(1-d)^4$. Here, the first item represents three-photons click and a dark count, the second describes two-photons and two dark counts, the third denotes one photon and three dark counts, and the fourth is four dark counts. Otherwise, the probability to obtain two BSM results accounting for four photons in the X basis is $p = \frac{1}{4}p_\rho^4(1-d)^4$. In the X basis, an error corresponds to a projection into $|\Phi^-\Phi^-\rangle$ or $|\Phi^+\Phi^+\rangle$ when Charlie prepare the same states, or, into $|\Phi^+\Phi^-\rangle$ or $|\Phi^-\Phi^+\rangle$ with orthogonal states. The QBER in the X basis can be written as $e_x = \frac{1}{2}\frac{p_d}{p_d + p}$. Likewise, for Alice and Bob the probability to obtain a successful projection into $|\Phi^+\Phi^+\rangle$ in three bases is $p(H, H) = p(V, V) = p(D, D) = p(\widetilde{D}, \widetilde{D}) = p(L, L) = p(R, R) = \frac{1}{4}p_d$, and $p(H, V) = p(V, H) = p(D, \widetilde{D}) = p(\widetilde{D}, D)\, p(L, R) = p(R, L) = \frac{1}{8}p_\rho^4(1-d)^4 + p(H, H)$. Given these, one can calculate the value of I in Eq. (6). The resulting numerical simulation of the secret key rate are shown in Fig. 2. We would like to mention that the realization of our idea requires expanding the distance between entangled particles. On the basis of present fiber and detector technology, it has shown that the distance for distributing entanglement is limited to the order of 100 km[23]. Our result demonstrates the feasibility of quantum communication using entangled pairs with standard optical components.

What we take into consideration here is the signal state Charlie prepares must be single-photon state. A secure key can finnally be distilled with some practical sources only if we know the lower bound of the fraction of those raw bits contributed solely by the single-photon state components. We know that with the help of decoy-state method, one can perform QSS with weak coherent state sources using phase postselection technique or quantum nondemolition measurement technique[12]. Here in a model with one PDC source in the middle, it would be interesting to explore whether the decoy-state method will accurately and efficiently verify such a bound.

Discussion

To conclude, We propose a double blinding-attack on a QSS protocol based on GHZ state. we have shown that using the MDI-EW method one can securely distribute a key between the two agents against all detector side channels. We extend the trusted device boundary in both sides to include the linear optical elements of BSM, except that the single-photon detectors are untrusted. We show that it is unconditionally secure against both an eavesdropper and dishonest players. For collective attacks, we obtain a bound on the key rate with source flaws. With the chosen parameters, we realize a DDI-QSS using single-photon sources over a distance of about 136 km from Charlie to Alice (Bob). It is expected that by following our proposal, a long-distance quantum secret sharing can be achieved experimentally.

References

1. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
2. Cleve, R., Gottesman, D. & Lo, H.-K. How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648 (1999).
3. Chen, Y.-A. *et al.* Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95**, 200502 (2005).
4. Bell, B. *et al.* Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
5. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. photonics* **4**, 686–689 (2010).
6. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
7. Wiechers, C. *et al.* After-gate attack on a quantum cryptosystem. *New J. Phys.* **13**, 013043 (2011).
8. Bugge, A. N. *et al.* Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **112**, 070503 (2014).

9. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
10. Lim, C. C. W. *et al.* Detector-device-independent quantum key distribution. *Appl. Phys. Lett.* **105**, 221112 (2014).
11. Qi, B. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Phys. Rev. A* **91** (2015).
12. Fu, Y., Yin, H.-L., Chen, T.-Y. & Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
13. Kogias, I., Xiang, Y., He, Q. & Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **95**, 012315 (2017).
14. Branciard, C., Rosset, D., Liang, Y.-C. & Gisin, N. Measurement-device-independent entanglement witnesses for all entangled quantum states. *Phys. Rev. Lett.* **110**, 060405 (2013).
15. Xu, P. *et al.* Implementation of a measurement-device-independent entanglement witness. *Phys. Rev. Lett.* **112**, 140506 (2014).
16. Yang, X. *et al.* Measurement-device-independent entanglement-based quantum key distribution. *Phys. Rev. A* **93**, 052303 (2016).
17. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
18. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
19. Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **95**, 080501 (2005).
20. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005).
21. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
22. Xu, F., Qi, B., Liao, Z. & Lo, H.-K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Appl. Phys. Lett.* **103**, 061101 (2013).
23. Erven, C. *et al.* Experimental three-photon quantum nonlocality under strict locality conditions. *Nat. Photon.* **8**, 292–296, https://doi.org/10.1038/nphoton.2014.50 (2014).

Acknowledgements

This work was supported by the Key Science Research Project of Inner Mongolia University of Technology Grant No. ZS201123, the National Natural Science Foundation of China Grant No. 61475148, the National Key Research And Development Program of China Grant No. 2016YFA0302600, the Guangxi Science Foundation (Grant No. 2017GXNSFBA198231).

Author Contributions

X.Y. and K.W. conceived the idea; H.M., H.L., Z.C., and L.W. performed the theoretical analysis. K.W., and Z.Y. supervised the project. X.Y. wrote the manuscript with input from all the authors. All the authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.