W-state Analyzer and Multi-party Measurement-device-independent Quantum Key Distribution

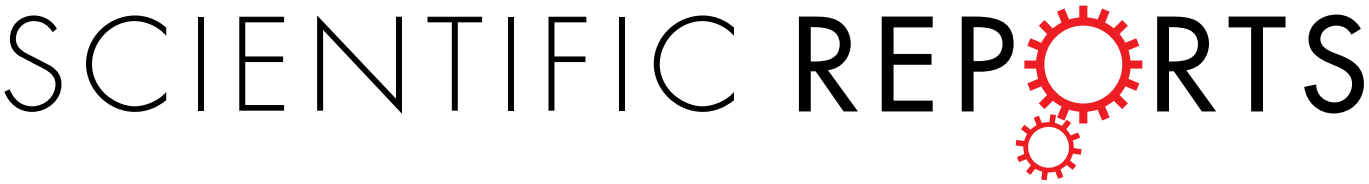
Citation: Zhu, Changhua, Feihu Xu, and Changxing Pei. "W-State Analyzer and Multi-Party Measurement-Device-Independent Quantum Key Distribution." Scientific Reports 5 (December 8, 2015): 17449.

As Published: http://dx.doi.org/10.1038/srep17449

Publisher: Nature Publishing Group

Persistent URL: http://hdl.handle.net/1721.1/100932

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context



OPEN

W-state Analyzer and Multi-party Measurement-device-independent Quantum Key Distribution

Received: 02 July 2015
Accepted: 29 October 2015
Published: 08 December 2015

Changhua Zhu[1,2], Feihu Xu[3] & Changxing Pei[1]

W-state is an important resource for many quantum information processing tasks. In this paper, we for the first time propose a multi-party measurement-device-independent quantum key distribution (MDI-QKD) protocol based on W-state. With linear optics, we design a W-state analyzer in order to distinguish the four-qubit W-state. This analyzer constructs the measurement device for four-party MDI-QKD. Moreover, we derived a complete security proof of the four-party MDI-QKD, and performed a numerical simulation to study its performance. The results show that four-party MDI-QKD is feasible over 150 km standard telecom fiber with off-the-shelf single photon detectors. This work takes an important step towards multi-party quantum communication and a quantum network.

The quantum key distribution (QKD) protocol, which is based on the principles of quantum mechanism, is unconditionally secure in theory[1,2]. For a review, see, e.g. Ref. 3. In practice, however, a QKD system still has security loopholes due to the gap between theory and practice. Various attacks have been successfully launched through the exploration of these loopholes, e.g. a time-shift attack[4,5], a phase-remapping attack[6], a blinding attack[7,8], and so forth[9–11]. To close this gap, the first method is to build precise mathematical models for all the devices and refine the security proofs to include these models[12]. However, this method is challenging to implement due to the complexity of QKD components. In addition, a device-independent QKD (DI-QKD) was proposed[13,14]. In DI-QKD, the legitimate participants during the process of communication, namely, Alice and Bob, do not need to obtain precise mathematical models for their devices, and all side-channels can be removed from QKD implementations if certain requirements can be satisfied. However, the implementation requires a loophole-free Bell test, which is still out the scope of current technology. Instead, a new protocol, measurement-device-independent QKD (MDI-QKD)[15] (for a review, see ref. 16), was proposed. This protocol is fully practicable with current technology. Unlike security patches[17,18], MDI-QKD can remove all detector side-channel attacks. This kind of attack is arguably the most important security loophole in conventional QKD implementations[7–11,19]. The measurement setup in MDI-QKD can be fully untrusted and even manufactured by Eve. The experimental feasibility of MDI-QKD has been demonstrated in both the laboratory and field tests[20–23]. MDI-QKD has also attracted a lot of scientific attention from theoretical side[24–31]. In addition to the application in QKD, MDI technique can also be used in other quantum information processing tasks, such as MDI entanglement-witness[32].

In addition to the two-party QKD protocol, researchers have also proposed various multi-party QKD protocols. Generally, there are three types of multi-party QKD schemes. The first one is based on a trusted center (TC)[33], in which each user shares a secret key with the TC and builds a common session key. The second one is an entanglement-based multi-party QKD protocol. Cabello proposed a multi-party QKD protocol that uses Greenberger-Horne-Zeilinger (GHZ) states[34] and that is an extension of a two-party entanglement-based QKD protocol[2]. Chen and Lo proposed a wide class of distillation schemes for multi-party entanglement, which have been applied to implement conference key agreement[35,36]. The third one is a multi-party QKD protocol without the use of entanglement and TC. Matsumoto proposed a QKD protocol in which Alice sends the same qubits sequence to Bob and Charlie respectively, and the qubits with coincident bases are used to build a secret key after post-processing[37]. In the first type of scheme, information may be leaked since pre-shared secret bits are used repeatedly. In the second type, a perfect GHZ state should be prepared. In the third type, two prepare-and-measure QKD processes are implemented. Nevertheless, up until now, a key weakness of all multi-party quantum cryptographic protocols is

[1]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, Shaanxi 710071, China. [2]Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada. [3]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA. Correspondence and requests for materials should be addressed to C.Z. (email: chhzhu@xidian.edu.cn)

the assumption that the measurement devices are trusted. As aforementioned, the occurrence of many quantum hacking attacks indicates that this is a highly unrealistic assumption.

In order to remove the demanding requirement for trusted measurement devices, we focus our attention on multi-party MDI-QKD. Appropriate entanglement states and their analyzers are the premises for the design of a multi-party MDI-QKD protocol. An elegant GHZ-type multi-party MDI-QKD protocol has been recently proposed in ref. 38, and this protocol shows that three-party MDI-QKD is highly feasible in practice. However, ref. 38 is primarily limited to three participants, and in a situation with more participants, the GHZ-type MDI-QKD is restricted to a very low key rate. Another potential candidate to build multi-party MDI-QKD is cluster state, but an efficient cluster-state analyzer based on linear optics remains unknown. Therefore, in a large-scale quantum Internet, a better analyzer and a different type of entanglement state are essential and required in order to design a multi-party MDI-QKD protocol and to obtain a high key rate.

W-state is a category of multi-particle entanglement state that can be used in a number of quantum information processing protocols[39]. *W*-state can be generated by type-II spontaneous parametric down-conversion (SPDC) and linear optical components[40,41]. In comparison with GHZ state, an important property of *W*-state is that, if one particle is traced out and projected into a specified state, the remaining particles are still entangled. That is, W-state is highly robust. Nonetheless, a *W*-state analyzer, which would enable the state of multiple particles to be projected into a *W*-state, still has to be constructed properly.

Here, we, for the first time, propose a multi-party QKD protocol based on W-state. We present the application of *W*-state in multi-party QKD, and construct a new *W*-state analyzer to distinguish the four-qubit *W*-state, based on linear optics only. With this analyzer, a four-party *W*-state MDI-QKD protocol is proposed. In this protocol, the four users, Alice, Bob, Charlie, and David, each send BB84 qubits to the central relay, Emma, with a *W*-state analyzer. The qubits with successful measurement outputs and coincident bases are used to build a secret key. The results show that the scheme is highly feasible for practically distributing the post-selected-state entanglement and for generating secure keys over a distance of more than 150 km standard telecom fiber for experimentally accessible parameter regimes. With state-of-the-art high-efficiency detectors, four-party MDI-QKD is feasible over 250 km fiber. We remark that, our protocol can be extended to the case with more participants and still remain a high key rate. All these features move an important step towards practical multi-party quantum communication.

Results

W-state and its analyzer. In this section, a group of four-particle entanglement *W* states is introduced, and a four-particle *W*-state analyzer based on linear optics is proposed.

W_4 state. The standard n-qubit *W*-state is defined by ($n \geq 3$)[42]

$$|W_n\rangle = 1/\sqrt{n}\,(|10\cdots0\rangle + |01\cdots0\rangle + \cdots + |00\cdots1\rangle) \tag{1}$$

If $n = 4$, the four-qubit *W*-state is given by

$$|W_4\rangle = 1/2(|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle) \tag{2}$$

There are nine families of states that correspond to nine different ways of entangling four qubits[43]. For *W*-state, the widely used state is the standard one, given by equation (2). Here, based on the W_4 state, 16 four-qubit W states can be constructed, and these states appear in Supplementary I. All these W_4 states form a group of orthogonal bases in a 16-dimensional Hilbert space. Any four-qubit state can be expressed as a linear combination of these 16 W_4 states. The protocol proposed in this paper is based on these states.

A four-photon W_4 state analyzer. The tomography of *W*-states has been a hot topic in recent years[44–46]. However, the method for designing an analyzer to verify a *W*-state is still an open question.

In fact, a four-qubit W_4 state can be expressed by Bell states, which is presented as below.

$$|W_{4,0}\rangle = 1/2\Big[\Big(|\phi^+\rangle_{12} + |\phi^-\rangle_{12}\Big)|\psi^+\rangle_{34} + |\psi^+\rangle_{12}\Big(|\phi^+\rangle_{34} + |\phi^-\rangle_{34}\Big)\Big], \tag{3}$$

where $|\phi^+\rangle$, $|\phi^-\rangle$, and $|\psi^+\rangle$ are three Bell states. From equation (3), we find that it is possible to design a W_4 state analyzer based on a Bell-state analyzer. Indeed, this is our method to construct the W_4 state analyzer.

Generally, with an optimal linear optics-based scheme and without the use of auxiliary photons, only two out of four Bell states can be distinguished[47]. However, an important time-bin-based Bell-state analyzer can distinguish three out of four Bell states[48]. Its schematic representation is shown in Fig. 1. In this scheme, the qubit is encoded with time bins[49]. The qubit $|0\rangle$ ($|1\rangle$) corresponds to a photon in state $\hat{a}^\dagger_{t_0}|0\rangle$ ($\hat{a}^\dagger_{t_1}|0\rangle$) under Z-basis, or in state $1/\sqrt{2}\,(\hat{a}^\dagger_{t_0} + \hat{a}^\dagger_{t_1})|0\rangle$ ($1/\sqrt{2}\,(\hat{a}^\dagger_{t_0} - \hat{a}^\dagger_{t_1})|0\rangle$) under X-basis, where $t_1 = t_0 + \tau$ and τ is a constant time. The device consists of two beam splitters, BS_1 and BS_2, two fibers with time delay τ, and two single photon detectors, D_1 and D_2, all of which build a time-bin interferometer.

In Fig. 1, let $\hat{a}^\dagger_{p,t}$ denote the creation operators in spatial mode p($p = a, b, c, d, e, f$) and temporal mode t ($t = t_0$ *or* t_1 for modes a, b, c, d; $t = t_0$, t_1 *or* t_2 for modes e and f). After passing through BS_1, let the relative phase between the transmitted light field and the reflected light field be π., then the operators evolve as follows[50]

$$\hat{a}^\dagger_{a,t} \to 1/\sqrt{2}\,(-i\hat{a}^\dagger_{c,t} + \hat{a}^\dagger_{d,t}), \tag{4}$$

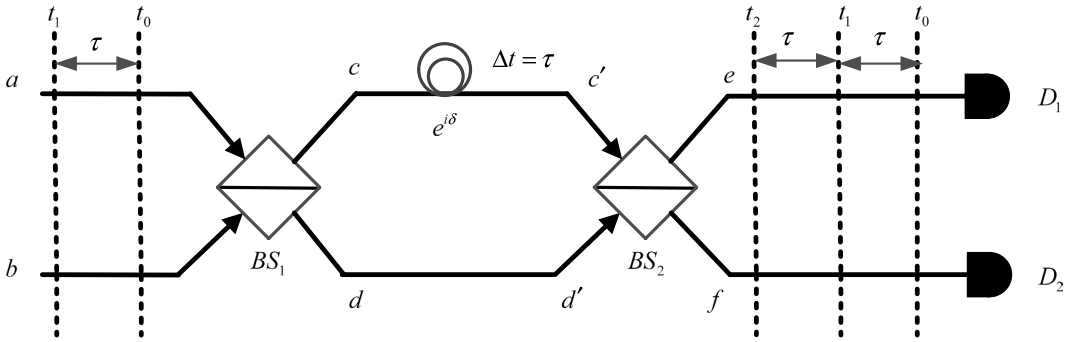


Figure 1. A schematic diagram of Bell-state measurement[48]. BS_1 and BS_2 are ideal 50/50 optical beam splitters that have equal reflection and transmission coefficients and no absorption loss. The delay Δt derived from the path length difference of the interferometer equals τ. When two qubits enter the interferometer, the output state is a mixture of photons in two spatial modes (e and f) and three temporal modes (t_0, t_1 and t_2). Three Bell states can be distinguished through an analysis of different combinations of these modes of photons.

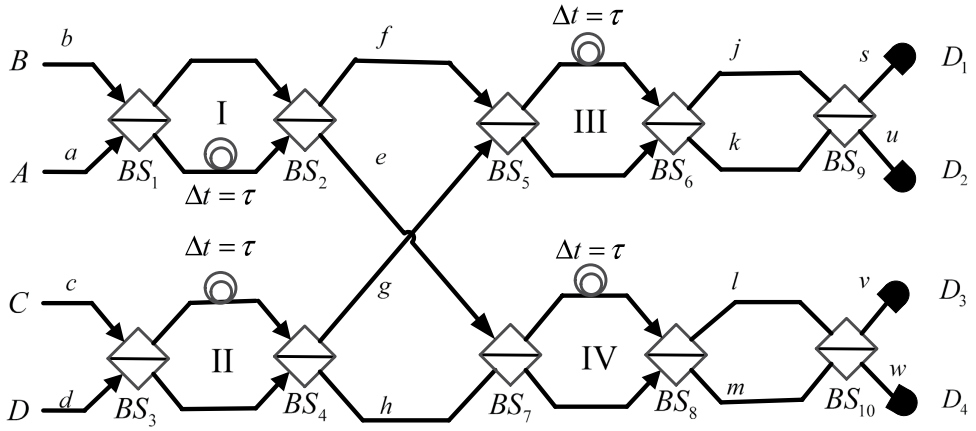


Figure 2. A schematic diagram of a *W*-state analyzer. The analyzer consists of four time-bin interferometers. Each interferometer is the same as the one shown in Fig. 1. Two photons from port A and B enter into the interferometer I. The photon in spatial mode e enters into interferometer IV, and the photon in spatial mode f enters into interferometer III. Another two photons from port C and D enter into interferometer II. The photon in spatial mode g enters into interferometer III, and the photon in spatial mode h enters into interferometer IV. The state of photons at the output is in a superposition state of four spatial modes (s, u, v, w) and four temporal modes (t_0, t_1, $t_2$and t_3). By analysis of different combinations of these modes, four out of sixteen W -states can be distinguished.

$$\hat{a}^{\dagger}_{b,t} \rightarrow 1/\sqrt{2}\,(\hat{a}^{\dagger}_{c,t} - i\hat{a}^{\dagger}_{d,t}). \tag{5}$$

Next, after the time-bin interferometer, the creation operators evolve into

$$\hat{a}^{\dagger}_{a,t} \rightarrow 1/2\left(-\hat{a}^{\dagger}_{e,t} + e^{i\delta}\hat{a}^{\dagger}_{e,t+\tau} + i\hat{a}^{\dagger}_{f,t} + ie^{i\delta}\hat{a}^{\dagger}_{f,t+\tau}\right), \tag{6}$$

$$\hat{a}^{\dagger}_{b,t} \rightarrow 1/2\left(\hat{a}^{\dagger}_{f,t} - e^{i\delta}\hat{a}^{\dagger}_{f,t+\tau} + i\hat{a}^{\dagger}_{e,t} + ie^{i\delta}\hat{a}^{\dagger}_{e,t+\tau}\right), \tag{7}$$

where δ is the phase derived from the path length difference in the interferometer[48]. Equations (6) and (7) indicate that the photons may arrive at D_1 or D_2 at different time instants, t_0, t_1, or t_2, according to input states, as shown in Fig. 1. From the output coincidence, in principle, Bell-states $|\psi^+\rangle_{ab}$ can be detected with 100% probability, and $|\psi^-\rangle_{ab}$ and $|\phi^+\rangle_{ab}$ can be detected with 50% probability, respectively[48].

The W-state analyzer shown in Fig. 2 is proposed. The qubits $|0\rangle$ and $|1\rangle$ are also encoded with the time-bin. At the first stage, the states of the photons in spatial modes a and b evolve into the states at modes e and f, according to equations (6) and (7). In ways that are also similar to equations (6) and (7), the states of the photons in spatial modes c and d evolve into the ones in modes g and h; the ones in modes f and g evolve into the ones in modes j and k; the ones in modes e and h evolve into the ones in modes l and m.

After BS_9 and BS_{10}, the states of photons evolve into

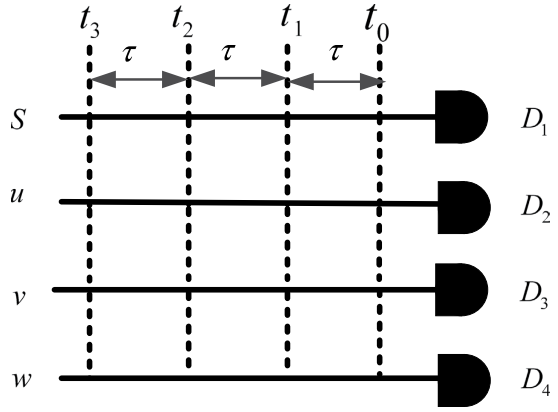


Figure 3. The spatial and temporal modes at the output of the *W*-state analyzer. There are four spatial modes (i.e., s, u, v, and w) and four temporal modes (i.e., t_0, t_1, t_2, and t_3). The time separation between time-bins is τ. The output state is a superposition of spatial modes and temporal modes.

$$\hat{a}^{\dagger}_{j,t} \rightarrow 1/\sqrt{2}\,(-i\hat{a}^{\dagger}_{s,t} + \hat{a}^{\dagger}_{u,t}) \tag{8}$$

$$\hat{a}^{\dagger}_{k,t} \rightarrow 1/\sqrt{2}\,(\hat{a}^{\dagger}_{s,t} - i\hat{a}^{\dagger}_{u,t}) \tag{9}$$

$$\hat{a}^{\dagger}_{l,t} \rightarrow 1/\sqrt{2}\,(-i\hat{a}^{\dagger}_{v,t} + \hat{a}^{\dagger}_{w,t}) \tag{10}$$

$$\hat{a}^{\dagger}_{m,t} \rightarrow 1/\sqrt{2}\,(\hat{a}^{\dagger}_{v,t} - i\hat{a}^{\dagger}_{w,t}) \tag{11}$$

Based on equations (6–11), the output detection modes of each of 16 W_4 states can be obtained. As an example, the state $|W_{4,0}\rangle$ is discussed. Its operator form is

$$|W_{4,0}\rangle = 1/2(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$$

$$=1/2\left[\hat{a}^{\dagger}_{a,t_0}\hat{a}^{\dagger}_{b,t_0}\hat{a}^{\dagger}_{c,t_0}\hat{a}^{\dagger}_{d,t_1} + \hat{a}^{\dagger}_{a,t_0}\hat{a}^{\dagger}_{b,t_0}\hat{a}^{\dagger}_{c,t_1}\hat{a}^{\dagger}_{d,t_0} + \hat{a}^{\dagger}_{a,t_0}\hat{a}^{\dagger}_{b,t_1}\hat{a}^{\dagger}_{c,t_0}\hat{a}^{\dagger}_{d,t_0} + \hat{a}^{\dagger}_{a,t_1}\hat{a}^{\dagger}_{b,t_0}\hat{a}^{\dagger}_{c,t_0}\hat{a}^{\dagger}_{d,t_0}\right]|0\rangle \tag{12}$$

Then, by using equations (6–11), $|W_{4,0}\rangle$ evolves into

$$\begin{aligned}|W_{4,0}\rangle \;\rightarrow\; & 1/2048\{64e^{i2\delta}\hat{a}^{\dagger}_{s,t_0}(\hat{a}^{\dagger}_{s,t_1})^3 - 192e^{i6\delta}a^{\dagger}_{s,t_1}a^{\dagger}_{s,t_2}(\hat{a}^{\dagger}_{w,t_2})^2 - 64e^{i3\delta}a^{\dagger}_{s,t_1}(\hat{a}^{\dagger}_{u,t_1})^2a^{\dagger}_{w,t_1} \\ & + \cdots + 128e^{i2\delta}\hat{a}^{\dagger}_{s,t_0}\hat{a}^{\dagger}_{u,t_1}\hat{a}^{\dagger}_{v,t_0}\hat{a}^{\dagger}_{w,t_2} + 128e^{i2\delta}\hat{a}^{\dagger}_{s,t_0}\hat{a}^{\dagger}_{u,t_1}\hat{a}^{\dagger}_{v,t_1}\hat{a}^{\dagger}_{w,t_1} + 128e^{i2\delta}\hat{a}^{\dagger}_{s,t_0}\hat{a}^{\dagger}_{u,t_2}\hat{a}^{\dagger}_{v,t_0}\hat{a}^{\dagger}_{w,t_1} \\ & + \cdots + 128e^{i4\delta}\hat{a}^{\dagger}_{v,t_0}\hat{a}^{\dagger}_{v,t_1}\hat{a}^{\dagger}_{w,t_1}\hat{a}^{\dagger}_{w,t_3} + 128e^{i4\delta}\hat{a}^{\dagger}_{v,t_0}\hat{a}^{\dagger}_{v,t_2}\hat{a}^{\dagger}_{w,t_1}\hat{a}^{\dagger}_{w,t_2}\}|0\rangle\end{aligned} \tag{13}$$

There are 200 terms in equation (13). That means that the output state is a superposition of 200 states. Each of the states is called a detection mode. Here, detection mode means SPD clicks at some spatial modes and time-bins; e.g., $\hat{a}^{\dagger}_{s,t_i}\hat{a}^{\dagger}_{u,t_j}\hat{a}^{\dagger}_{v,t_k}\hat{a}^{\dagger}_{w,t_l}$ means that photons clicks occur in spatial modes s, u, v, and w at the time instant t_i, t_j, t_k, and $t_l (i, j, k, l = 0, 1, 2, 3)$, respectively. $(\hat{a}^{\dagger}_{s,t_i})^2\hat{a}^{\dagger}_{u,t_j}\hat{a}^{\dagger}_{v,t_k}$ means that two photons arrive in s mode at t_i. One photon occurs in u mode at t_j, and one photon occurs in v mode at time t_k, respectively. The spatial and temporal modes are shown in Fig. 3.

All detection modes of 16 W_4 states have been obtained. By comparing the detection modes among different states, the unique modes belonging to one specific state are obtained. These modes make one state distinguishable from the others. Here, only the modes in which the SPD click derives from one photon are taken into account; i.e., all four SPDs in each mode have a click. There are four W_4 states, i.e., $|W_{4,0}\rangle$, $|W_{4,1}\rangle$, $|W_{4,c}\rangle$, and $|W_{4,d}\rangle$, that can be identified with the proposed analyzer. Their detection modes are shown in Table 1. The success rate is determined by the corresponding coefficients of output states. For states $|W_{4,0}\rangle$ and $|W_{4,c}\rangle$, the probability of successful detection is $D_{p0} = [128/2048]^2 \times 12 = 0.0469$. For states $|W_{4,1}\rangle$ and $|W_{4,d}\rangle$, the probability of successful detection is $D_{p1} = [128/2048]^2 \times 4 = 0.0156$. Therefor the total success probability is $D_p = 1/16(2 \times D_{p0} + 2D_{p1}) = 0.78\%$ These four states can be applied to build keys among four users, a process that will be discussed in the next section.

It is worth mentioning that four other states, i.e., $|W_{4,2}\rangle$, $|W_{4,3}\rangle$, $|W_{4,e}\rangle$ and $|W_{4,f}\rangle$, can also be distinguished if photon-number-resolving detectors can be used. In addition, the detection probabilities of states $|W_{4,0}\rangle$, $|W_{4,1}\rangle$, $|W_{4,c}\rangle$, and $|W_{4,d}\rangle$ can also be increased with this type of detector.

No	Distinguished states	Detection modes	Success probability
I	$\|W_{4,0}\rangle$	$s_0u_1v_0w_2$, $s_0u_1v_1w_1$, $s_0u_1v_1w_3$, $s_0u_1v_2w_2$,	0.0469
		$s_0u_2v_0w_1$, $s_0u_2v_0w_3$,$s_0u_3v_0w_2$, $s_1u_1v_0w_1$,	
		$s_1u_1v_2w_1$, $s_1u_3v_0w_1$,$s_2u_1v_1w_1$, $s_2u_2v_0w_1$	
II	$\|W_{4,1}\rangle$	$s_0u_1v_0w_3$,$s_0u_1v_2w_1$,$s_0u_3v_0w_1$,$s_2u_1v_0w_1$	0.0156
III	$\|W_{4,c}\rangle$	$s_0u_2v_2w_3$,$s_0u_3v_1w_3$,$s_1u_1v_2w_3$,$s_1u_3v_0w_3$	0.0469
		$s_1u_3v_2w_3$, $s_2u_1v_2w_2$,$s_2u_2v_2w_1$, $s_2u_2v_2w_3$,	
		$s_2u_3v_0w_2$, $s_2u_3v_1w_1$, ,$s_2u_3v_1w_3$,$s_2u_3v_2w_2$	
IV	$\|W_{4,d}\rangle$	$s_0u_3v_2w_3$, $s_2u_1v_2w_3$,$s_2u_3v_0w_3$, $s_2u_3v_2w_1$	0.0156

Table 1. Distinguishable W_4 states and their detection modes. Four W_4 states, i.e., $|W_{4,0}\rangle$, $|W_{4,1}\rangle$, $|W_{4,c}\rangle$, and $|W_{4,d}\rangle$, can be identified by the proposed analyzer. Detection modes $s_iu_jv_kw_l$ mean that photons clicks occur in the spatial modes s, u, v, and w, and at the temporal modes t_i, t_j, t_k, and t_l ($i, j, k, l = 0,1,2,3$), respectively.

Measurement-device-independent quantum key distribution based on W-state. In this section, we propose a four-party MDI-QKD protocol based on W_4 state and the analyzer presented in the previous section. The security of the protocol is also proved.

The protocol. Conceptually, the four-party MDI-QKD can be implemented based on a time-reversal W_4 state protocol. In this protocol, each of the four users can prepare an entangled EPR photon pairs, keep one photon from each pair, and send the other photon to the central relay. Then projective measurement on the state of the photons can be performed by the relay. If the state is projected into a W_4 state by the relay, the state of the remaining four photons in the users is projected to the same W_4 state. Through the use of the idea of a virtual qubit[16], a four-party MDI-QKD scheme can be constructed.

The proposed setup of four-party MDI-QKD protocol is shown in Fig. 4. There are four participants, i.e., Alice, Bob, Charlie, and David. Photons from single photon sources (SPS) are encoded with time-bin. Generally, weak coherent pulse (WCP) sources combined with decoy state technology[51–53] can also be used to replace the SPS. Here, SPS is used to simplify the discussion.

The procedures of the protocol are as follows:

(1) **Preparing**: Each one of the participants, i.e., Alice, Bob, Charlie, and David, prepares single photons, which are in the four possible BB84 time-bin states (i.e., $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$) and sends them to an untrusted relay, Emma, with an analyzer in the middle. The preparation processes are implemented by single photon sources and a time-bin encoder.
(2) **Measuring**: Emma performs W_4 state measurement by using the analyzer in Fig. 2. Then the incoming signals are projected into a W_4 state.
(3) **Sifting**: Emma uses public channels to announce the events in which she obtained successful outputs; i.e., some of the states in Table 1 are identified. When all participants use the rectilinear (Z) basis, two of them announce their bits, and the other two perform operations according to the scenarios shown in Table 2. In addition to the case that all participants encode their qubits in Z basis, another case is that they encode their qubits in X basis. For the latter, the W-states can be described as states $|+\rangle$ and $|-\rangle$, e.g.,

$$\begin{aligned}|W_{4,\ 0}\rangle \quad &= 1/4[|{+}{+}\rangle(2|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle) + (|{+}{-}\rangle + |{-}{+}\rangle)(|{+}{+}\rangle - |{-}{-}\rangle)\\ &\quad - |{-}{-}\rangle(|{+}{-}\rangle + |{-}{+}\rangle + 2|{-}{-}\rangle)]\end{aligned} \tag{14}$$

and

$$\begin{aligned}|W_{4,\ c}\rangle = 1/4[&|{+}{+}\rangle(2|{+}{+}\rangle - |{+}{-}\rangle - |{-}{+}\rangle) - (|{+}{-}\rangle + |{-}{+}\rangle)(|{+}{+}\rangle - |{-}{-}\rangle)\\ &+ |{-}{-}\rangle(|{+}{-}\rangle + |{-}{+}\rangle - 2|{-}{-}\rangle)]\end{aligned} \tag{15}$$

In this case, the first two announce the values of the qubits ($|+-\rangle$ or $|-+\rangle$), and the other two perform phase error rate estimation.
(4) **Post-processing**: After obtaining the sifted key, the two participants perform information reconciliation and privacy amplification. The suggestion is that an error correction code-based reconciliation protocol be used, since the interactive protocol, e.g., Cascade[54], requires many communications. A low-density parity-check (LDPC) code-based reconciliation scheme[55] can be used.

Security analysis. The security of the four-party W-state-based MDI-QKD protocol is inspired by the security of a time reversed W-state-based QKD protocol.

First, we briefly introduce the W-state-based QKD protocol. In a three-party W-state-based QKD protocol, three particles in W_3 state are distributed to three participants respectively. The announcement of the measurement bases and the measurement results of one participant enables the other two to perform key distribution or security verification. The protocol can be extended to the one with four participants. Compared with a three-party QKD

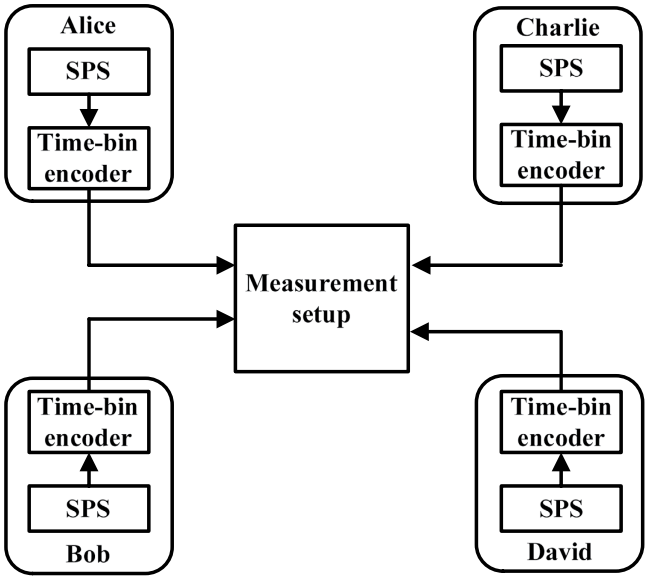


Figure 4. Basic setup of a W_4-based four-party MDI-QKD protocol. Alice, Bob, Charlie, and David prepare single photon pulses in a different BB84 time-bin coded state, which is selected independently and at random for each signal. The time-bin encoder can follow the design proposed in ref. 20. Inside the measurement setup, signals from Alice, Bob, Charlie, and David are sent into a W-state analyzer (see Fig. 2). Successful output corresponds to the observation of one of four W_4 states shown in Table 1. The four participants' laboratories are well shielded from the eavesdropper, and the measurement setup can be untrusted.

Announced bits				Participants who obtain the key bits and their operation
Alice	Bob	Charlie	David	
0 (1)	0 (1)	–	–	Charlie & David, one of their bits flips.
0 (1)	–	0 (1)	–	Bob & David, one of their bits flips.
0 (1)	–	–	0 (1)	Bob & Charlie, one of their bits flips.
–	0 (1)	0 (1)	–	Alice & David, one of their bits flips
–	0 (1)	–	0 (1)	Alice & Charlie, one of their bits flips.
–	–	0 (1)	0 (1)	Alice & Bob, one of their bits flips.

Table 2. Four participants' post-selection after Emma announces a successful output of states $|W_{4,0}\rangle$ or $|W_{4,1}\rangle$ ($|W_{4,c}\rangle$ or $|W_{4,d}\rangle$). Any two participants announce their classic bits. If the bits are "00" ("11"), the other two participants can obtain the raw key bits; i.e., one of them flips his or her bits. For example, when Alice and Bob announce classic bits "00" ("11"), one of the pair Charlie and David flips his bits. This way, any two participants can perform QKD. The optical quantum channel need not be changed.

protocol, in the one with four participants, two participants announce their measurement bases and results, and the other two are in a maximally entangled Bell state and can obtain a secret key.

Secondly, it can be demonstrated that a time reversed W-state-based QKD protocol exists as the same as the time reversed EPR protocol[56]. With reference to the two-party MDI-QKD protocol[15], the idea of a virtual qubit is also used. One can imagine that each of four participants prepares an EPR entanglement state, sends one qubit to Emma, and retains the other qubit as a virtual qubit. The virtual qubit is subsequently measured, and a BB84 state is thus prepared. In principle, each one could keep his or her virtual qubit in his or her memory and delay his or her measurement of it. Only after Emma has announced that she has obtained a successful outcome will each perform a measurement on his or her virtual qubit in order to decide which state he or she is sending to Emma. Furthermore, it is shown that W-state can be prepared among four participants by entanglement swapping, while each participant prepares an EPR pair initially. So, in such a virtual qubit setting, the protocol is equivalent to an entanglement-based protocol. Alice, Bob, Charlie, and David share quadruple qubits in their quantum memories, and they can compute the quantum bit error rate (QBER) on their virtual qubits on a special basis.

Key rate of the four-party MDI-QKD protocol. The key rate of the W-state-based MDI-QKD protocol is evaluated with SPS. According to the procedures described in the previous section, any two participants can build a secret key after Emma announces successful outputs, and the other two participants' classic bits are 00 or 11. So the key rate can be obtained by referring to the case of two-party MDI-QKD[15] and to the basic work of Shor and Preskill[57]. The difference between the four-party and the two-party MDI-QKD is that the gain in the four-party

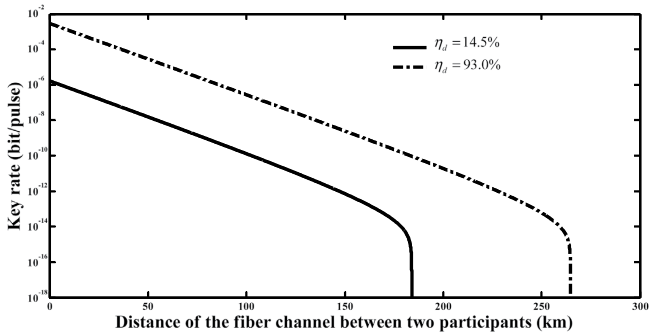


Figure 5. Key rates with different detection efficiencies. Both curves are key rates with single photon sources (SPSs). The solid curve is the one with a detection efficiency of 14.5%. The dash-and-dot is the one with the higher detection efficiency of 93%.

one refers to the joint probability that Emma announces successful output and two of participants' classic bits are 00 (or 11), according to Table 2. Since any two participants can build a secret key, the maximum information loss value in data reconciliation and the privacy amplification processes of each pair are considered. So the key rate can be given as

$$R_0 = qQ_1\{1 - Max[H_2(e_{cd}^X), H_2(e_{bd}^X), H_2(e_{bc}^X), H_2(e_{ad}^X), H_2(e_{ac}^X), H_2(e_{ab}^X)] - Max[H_2(e_{cd}^Z), H_2(e_{bd}^Z), H_2(e_{bc}^Z), H_2(e_{ad}^Z), H_2(e_{ac}^Z), H_2(e_{ab}^Z)]\} \quad (16)$$

where e_{jk}^X (e_{jk}^Z) denotes the QBER between participants j and k under X (Z) basis, given that each of Alice (a), Bob (b), Charlie (c), and David (d) sends single photon states, $j, k = a, b, c, d$; Q_1 denotes the gain (the joint probability of Emma's announcement of a successful detection in the Z basis, and also of the announced classic bits being 00 or 11, according to Table 2). q means the basis reconciliation factor; $H_2(x)$ is the binary entropy function with parameter x given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

In this protocol, the QBER in Z basis equals the one in X-basis under SPS, i.e. $e_{jk}^X = e_{jk}^Z$. The assumption is that there is no misalignment error, that the data size is infinite, and that the ideal reconciliation algorithm is applied. There is also an assumption that the quantum channels between the participants and Emma are identical. For the sake of simplicity, if we assume e_1 to be e_{jk}^Z, then equation (16) can be reduced to

$$R_0 = qQ_1\{1 - 2H_2(e_1)\} \quad (17)$$

Let the probability of Z basis be nearly one, i.e., $q \approx 1$. Q_1 can be estimated as (the detailed for obtaining Q_1 and e_1 are shown in Methods and Supplementary III)

$$Q_1 = (1 - Y_0)^{12}[1024(1-\eta)^4 Y_0^4 + 1440\eta(1-\eta)^3 Y_0^3 + 496\eta^2(1-\eta)^2 Y_0^2 + 49\eta^3(1-\eta)Y_0 + 8(D_{p0} + D_{p1})\eta^4]/128 \quad (18)$$

and the QBER $e_1$as

$$e_1 = \frac{1}{16Q_1}(1 - Y_0)^{12}[64(1-\eta)^4 Y_0^4 + 90\eta(1-\eta)^3 Y_0^3 + 31\eta^2(1-\eta)^2 Y_0^2 + 3\eta^3(1-\eta)Y_0] \quad (19)$$

where η is the channel transmittance between the participant and the analyzer, $\eta = 10^{-\alpha\cdot l/10}\cdot\eta_d$; α and l are the attenuation coefficient and fiber length between the participant and analyzer, and η_d is the detection efficiency of a single photon detector. Here, it is assumed that each SPD at each time instant has the same detection efficiency.

In numerical simulation, the parameters include the detection efficiency η_d, the background count rate Y_0 and the attenuation coefficient α. Let η_d be 14.5% and Y_0 be 6.02×10^{-6}. These values are chosen from the 144-Km QKD experiment reported in ref. 58. A superconducting nanowire single-photon detector (SNSPD) with a detection efficiency of 93%, as reported by Marsili *et al.*[59], is also used. Parameter α is set by a typical value, 0.2. The simulation results of the asymptotic key rate are shown in Fig. 5. The secure transmission distance between two participants is about 180 km for a detection efficiency of 14.5%, and is about 260 km for a detection efficiency of 93%. The distance is 100 km and 180 km for two detectors when the key rate is about 10^{-10}.

Discussion

In practice, the SPS may still be challenging with current technology. However, based on the so-called decoy state method[51–53], one can simply replace the SPS with weak coherent pulses (WCP) or parametric down- conversion (PDC) sources. As noted already in ref. 38 regarding the three-party MDI-QKD, the decoy state analysis and the

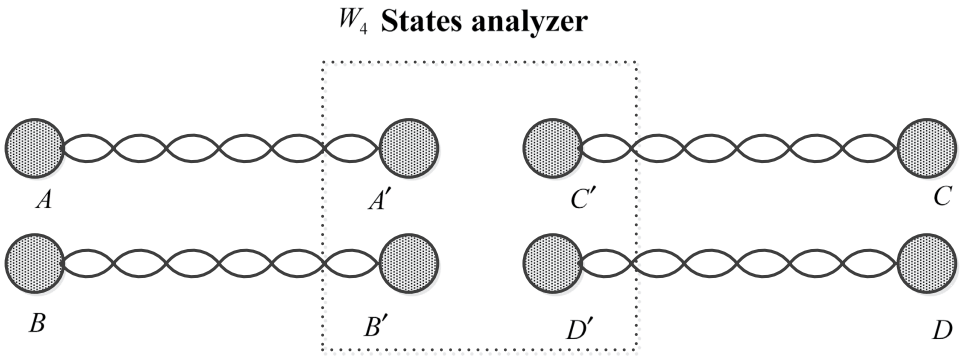


Figure 6. A schematic diagram of entanglement swapping for generating W_4 state. Each of Alice, Bob, Charlie and David prepares an EPR pair and sends half of them to Emma with a W_4 State analyzer.

finite-key analysis are similar to the initial two-party MDI-QKD protocol[24–28]. Therefore, the expectation is that, with decoy states, the results here can be easily extended to the cases with WCP and PDC sources.

In our proposal, any two of four parties can share a secure key bit. This is compatible to the usual network scenario, in which any two parties in the network can perform secure communications. There are several advantages as compared to the initial two-party MDI-QKD protocol. First, our proposal is faster in sharing key bits when the parties are reassigned. This is because the quantum channel is not required to be initialized. Second, the group key can also be built if one party serves as a controller. Finally, the initial MDI-QKD requires a clever design of fast and low-loss optical switches for a network setting, which might be challenging in a large-scale network. In contrast, our scheme does not have such requirement.

In the conclusion, we proposed a four-party W-state-based MDI-QKD protocol, in which any two of four participants can build secret keys, when the W-state analyzer announces a successful output, and the other two participants' classic bits sent are 00 (the distinguished states are $|W_{4,0}\rangle$ or $|W_{4,1}\rangle$) or 11 (the distinguished states are $|W_{4,c}\rangle$ or $|W_{4,d}\rangle$). Since the time-bin coded MDI-QKD protocol was verified to be feasible[20,22,29], and several schemes of SPS (e.g. quantum dot SPS)[60] have been presented, the proposed W-state analyzer can be implemented with current technology. The work presented here puts forward an important avenue for practical multi-party quantum communication.

Methods

W-state preparation based on entanglement swapping. A process of entanglement swapping for generating W_4-state is shown in Fig. 6.

In Fig. 6, all the photon pairs A and A', B and B', C and C', D and D' are in Einstein-Podolsky-Rosen (EPR) entangled states. When the state of 4 photons, A', B', C' and D', are projected into to any W_4 state, the state of remaining four photons , A, B, C and D, is projected into the corresponding W_4 sate. The detailed processes are shown in Supplementary II.

Estimation of Q_1 and e_1. We assume that there is no misalignment error (i.e. all mismatches in quantum channels are perfectly compensated), the four optical channels are identical, and ideal single photon sources are used. Therefore, the qubit error derives from dark counts of SPDs. As mentioned in Results, we only take into account the case in which SPD count in each spatial-temporal mode derives from no more than one photon.

For Emma, a successful output can be obtained from five cases: (1) all four counts of SPDs derive from background noise (dark counts); (2) one count derives from photon detection and the other three counts derive from background noise; (3) two counts derive from photon detections and the other two counts derive from background noise; (4) three counts derive from photon detections and the other one derives from background noise; (5) all four counts derive from photons. We assume that Alice (a) and Bob (b) announce their classical bits, while, Charlie (c) and David (d) try to generate secret key bits. In cases (2)–(5) we compute the output states of photons successfully passing through the analyzer and their probabilities. Then, we obtain the gain at each case according to the modes in Table 1. The details for obtaining Q_1 and e_1 are shown in Supplementary III.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing* [175–179] (IEEE, New York, 1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
3. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photon*. **8,** 595–604 (2014).
4. Qi, B., Fung, C.–H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7,** 73–82 (2007).
5. 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).
6. Xu, F., Qi, B. & Lo, H.–K. Experimental demonstration of phase remapping attack in a practical quantum key distribution system. *New J. of Phys.* **12,** 113026 (2010).
7. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photon*. **4,** 686–689 (2010).

8. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Commun*. **2,** 349 (2011).
9. Weier, H. *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13,** 073024 (2011).
10. Jain, N. *et al.* Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107,** 110501 (2011).
11. Bugge, A. N. *et al.* Laser damage helps the eavesdropper in quantum cryptography *Phys. Rev. Lett.* **112,** 070503 (2014).
12. Fung, C.-H., Tamaki, F. K., Qi, B., Lo, H.-K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quant. Info. Comp*. **9,** 0131 (2009).
13. Mayers, D. & Yao, A. C.-C. Quantum cryptography with imperfect apparatus. *Proc. of the 39th Annual Symp. on Foundations of Computer Science* [503–509] (IEEE, Washington DC, 1998).
14. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
15. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
16. Xu, F., Curty, M., Qi, B. & Lo, H.–K. Measurement-device-independent quantum cryptography. *IEEE J. of Selected Topics in Quantum Electron.* **21,** 6601111 (2015).
17. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography *Appl. Phys. Let*. **98,** 231104 (2011).
18. Ferreira da Silva, T., Xavier, G. B., Temporão, G. P. & von der Weid, J. P. Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems. *Opt. express* **20,** 18911–18924 (2012).
19. Yuan, Z. L., Dynes, J. F. & Shields, A. J. Avoiding the blinding attack in QKD. *Nature Photon*. **4,** 800–801 (2010).
20. Rubenok, A., Slater, J. A., Chan, P., Lucia-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
21. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88,** 052303 (2013).
22. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett*. **111,** 130502 (2013).
23. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112,** 190503 (2014).
24. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87,** 012320 (2013).
25. Ma, X., Fung C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 052305 (2012).
26. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New J. of Phys.* **15,** 113007 (2013).
27. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89,** 052333 (2014).
28. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution, *Nature commun*. **5,** 3732 (2014).
29. Ma X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 062319 (2012).
30. Wang, Q. & Wang, X.-B. Simulating of the measurement-device-independent quantum key distribution with phase randomized general sources. *Sci. Rep*. **4,** 4612 (2014).
31. Mizutani, A., Tamaki, K., Ikuta, R., Yamamoto, T. & Imoto N. Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol. *Sci. Rep*. **4,** 5236 (2014).
32. Xu, P. *et al.* Implementation of a Measurement-Device-Independent Entanglement Witness. *Phys. Rev. Lett.* **112,** 140506 (2014).
33. Hwang, T., Lee, K. C. & Li, C. M. Provably secure three-party authenticated quantum key distribution protocols. *IEEE Trans. on Dependable and Secure Computing* **4,** 71–80 (2007).
34. Cabello, A. Multiparty key distribution and secret sharing based on engtanglement swapping. *arXiv*: quant-ph/0009025.
35. Chen, K. & Lo, H.-K. Conference key agreement and quantum sharing of classical secrets with noisy GHZ states. *Proc. of Int. Symp. on Inform. Theory* [1607–1611] (IEEE, 2005).
36. Chen, K. & Lo, H.-K. Multi-partite quantum cryptographic protocols with noisy GHZ states. *Quantum Inf. Comput.* **7,** 689–715 (2007).
37. Matsumoto, R. Multiparty quantum-key-distribution protocol without use of entanglement. *Phys. Rev. A*. **76,** 062316 (2007).
38. 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).
39. Gorbachev V. N. & Trubilko, A. I. On multiparticle W states, their implementations and application in the quantum informational problems. *Laser Phys. Lett.* **3,** 59–70 (2006).
40. Yamamoto, T., Tamaki, K., Koashi, M. & Imoto, N. Polarization-entangled W state using parametric down-conversion. *Phys. Rev. A* **66,** 064301 (2002).
41. Eibl, M., Kiesel, N., Bourennane, M., Kurtsiefer, C. & Weinfurter, H. Experimental realization of a three-qubit entangled W state. *Phys. Rev. Lett.* **92,** 077901 (2004).
42. Dür, W., Vidal, G. & Cirac, J. I. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*. **62,** 062314 (2000).
43. Verstraete, F., Dehaene, J., De Moor, B. & Verschelde, H. Four qubits can be entangled in nine different ways. *Phys. Rev. A* **65,** 052112 (2002).
44. Zhao, M.-J., Zhang, T.-G., Li-Jost, X. & Fei, S.-M. Identification of three-qubit entanglement. *Phys. Rev. A* **87,** 012316 (2013).
45. Pál, K. F., Vertesi, T. & Navascues, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90,** 042340 (2014).
46. Wu, X. *et al.* Robust self-testing of the three-qubit W state. *Phys. Rev. A* **90,** 042339 (2014).
47. Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. Bell measurements for teleportation. *Phys. Rev. A* **59,** 3295 (1999).
48. Houwelingen, J. A. W., Van, Brunner, N., Beveratos, A., Zbinden, H. & Gisin, N. Quantum teleportation with a three-Bell-state analyzer. *Phys. Rev. Lett.* **96,** 130502 (2006).
49. Brendel, J., Gisin, N., Tittel, W. & Zbinden, H. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82,** 2594–2597 (1999).
50. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys*. **79,** 135–175 (2007).
51. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
52. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
53. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
54. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. Proceedings of Workshop on the theory and application of cryptographic techniques on Advances in cryptology (Eurocrypt'93), *Lect. Notes Comput. Sci*. **765,** 410–423 (1994).
55. Elkouss, D., Martinez-Mateo, J. & Martin, V. Information reconciliation for quantum key distribution. *Quantum Inf. Compu*. **11,** 226–238 (2011).
56. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54,** 2651 (1996).
57. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
58. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nature Phys*. **3,** 481–486 (2007).
59. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nature Photon*. **7,** 210–214 (2013).

60. Michler, P. *et al.* A quantum dot single-photon turnstile device. *Science* **290,** 2282–2285 (2000).

Acknowledgements
The authors would like to thank Zhiyuan Tang and Kejin Wei for helpful discussions, and thank Hoi-Kwong Lo for his inspiring proposal and brilliant comments. The authors also acknowledge the financial support from the Office of Naval Research (ONR), the Air Force Office of Scientific Research (AFOSR), the National Natural Science Foundation of China No. 61372076 and No. 61301171, the 111 Project (No. B08038), and China Scholarship Council (No. 201308615037). This work was done when the first author was a visiting scholar at University of Toronto.

Author Contributions
C.Z. and F.X. designed the new protocol, did the security analysis and key rate calculation. C.P. supervised the project. All authors wrote and reviewed the manuscript.

Additional Information
Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Zhu, C. *et al.* W-state Analyzer and Multi-party Measurement-device-independent Quantum Key Distribution. *Sci. Rep.* **5**, 17449; doi: 10.1038/srep17449 (2015).