SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM PHYSICS
QUANTUM INFORMATION

Received
9 April 2014

Accepted
20 May 2014

Published
10 June 2014

Correspondence and requests for materials should be addressed to A.M. (mizutani@qi.mp.es.osaka-u.ac.jp)

Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol

Akihiro Mizutani[1], Kiyoshi Tamaki[2], Rikizo Ikuta[1], Takashi Yamamoto[1] & Nobuyuki Imoto[1]

[1]Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan, [2]NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan.

The measurement-device-independent quantum key distribution (MDI QKD) was proposed to make BB84 completely free from any side-channel in detectors. Like in prepare & measure QKD, the use of other protocols in MDI setting would be advantageous in some practical situations. In this paper, we consider SARG04 protocol in MDI setting. The prepare & measure SARG04 is proven to be able to generate a key up to two-photon emission events. In MDI setting we show that the key generation is possible from the event with single or two-photon emission by a party and single-photon emission by the other party, but the two-photon emission event by both parties cannot contribute to the key generation. On the contrary to prepare & measure SARG04 protocol where the experimental setup is exactly the same as BB84, the measurement setup for SARG04 in MDI setting cannot be the same as that for BB84 since the measurement setup for BB84 in MDI setting induces too many bit errors. To overcome this problem, we propose two alternative experimental setups, and we simulate the resulting key rate. Our study highlights the requirements that MDI QKD poses on us regarding with the implementation of a variety of QKD protocols.

The security of quantum key distribution (QKD) can be guaranteed based on some mathematical models of the users' devices[1–3]. Unfortunately, the actual devices do not necessarily follow mathematical models, and we need to close the gap (side-channel) between the actual device and the mathematical model to implement secure QKD systems in practice. Among side-channels, the side-channel of a photon detector seems to be most easily exploited by an eavesdropper (Eve) since it accepts any input from Eve who can generate an arbitrary optical state such that it causes an unexpected behavior in the detector. In fact, the famous bright-pulse illumination attacks are based on side-channel in detectors[4]. In order to countermeasure such attacks, measurement-device-independent (MDI) QKD[5] was proposed to make BB84[6] free from any possible side-channel in a detector. We note that MDI QKD for continuous variable was proposed by[7,8]. In MDI QKD, Alice and Bob do not perform any measurement but only send quantum signals to be measured by Eve. Therefore, bit strings generated by Alice and Bob are free from side-channels in photon detectors since they do not employ photon detectors. Since its invention, MDI QKD has been actively studied both theoretically[9–12] and experimentally[13–16].

As is the case in prepare & measure scheme, implementation of protocols other than BB84 in MDI setting could be suitable for some practical situations. In fact, many experiments for non-BB84 type prepare & measure schemes, including B92[17], DPS QKD[18], coherent one-way protocol[19], SARG04[20], etc, have been reported[21]. Therefore, it is useful in practice to use non-BB84 type protocols in MDI setting, and in this paper we consider to use SARG04 protocol in MDI setting, which we refer to as MDI SARG04. SARG04 was originally proposed to make BB84 robust against photon number splitting (PNS) attacks[22,23] just by changing the classical post-processing part in BB84. It is proven that SARG04 can indeed generate a key from two-photon emission event by Alice in addition to single-photon emission event[24,25], showing robustness against PNS attack in some parameter regimes. Note in MDI setting is that both Alice and Bob are the sender of the signals, and as a result, the information leakage from the signals seems to be larger than the one in prepare & measure setting. Therefore, it is not trivial whether both single and two-photon emission events can contribute to the key generation or not. Our work answers this question, and we have found that the single-photon emission event by both Alice and Bob, or single-photon and two-photon emission by each of Alice and Bob can contribute to generating a key, but two-photon emission by the two parties cannot make the contribution when a probability of Eve's announcement of the successful measurement for the two-photon emission event is smaller than 1/16.

Another important issue to be addressed in MDI setting is what kind of measurement setup should be implemented experimentally at Eve's laboratory. Naively thinking, as SARG04 differs from BB84 only in the post-processing part, the same measurement setup for MDI BB84 should also work for MDI-SARG04 protocol. On the contrary, however, it turns out that the measurement setup for MDI BB84 results in high bit error rate when applied to MDI-SARG04 protocol, and consequently, no significant key can be generated. To generate a key in practice, we propose two alternative measurement schemes for the MDI-SARG04 protocol, and simulate the resulting key generation rate.

Results

MDI-SARG04 QKD protocol. In this section, we introduce the MDI-SARG04 QKD protocol. First, we summarize the assumptions and mathematical definitions made in this paper, and then we describe how the protocol runs.

Assumptions and definitions. We assume that each of Alice and Bob has a phase randomized photon source, *i.e.* the vacuum, a single photon, and multi photons are emitted probabilistically. The probabilities of the n-photon emission from Alice and Bob are p_n and $p_{n'}$, respectively, which satisfy $\sum_n p_n = \sum_{n'} p_{n'} = 1$. We encode the bit information in polarization of photons, and we assume that the preparation of the polarization is precise without any flaw. For simplicity, we consider the asymptotic case to neglect any statistical fluctuation, *i.e.*, the number of the signals sent by Alice and Bob is infinite. In our paper, horizontal and vertical polarization states of a single photon are represented by Z-basis qubit states, namely $|0_z\rangle$ and $|1_z\rangle$, respectively. We also define X (rectilinear)-basis states as $|i_x\rangle = \left(|0_z\rangle + (-1)^i|1_z\rangle\right)/\sqrt{2}$ for $i = 0, 1$. By using a creation operator $a_\theta^\dagger$ for a single photon in a polarization θ and the vacuum state $|\mathrm{vac}\rangle$, we denote an n-photon number state with polarization θ by $|n_\theta\rangle = \left(a_\theta^\dagger\right)^n |\mathrm{vac}\rangle/\sqrt{n!}$. (note that when the subscript θ is z or x, it refers to the qubit state rather than the photon number state). Other definitions we use are as follows: $|\varphi_i\rangle = \cos(\pi/8)|0_x\rangle + (-1)^i \sin(\pi/8)|1_x\rangle$ for $i = 0, 1$ and $|\varphi_i\rangle = \sin(\pi/8)|0_x\rangle + (-1)^{i-1}\cos(\pi/8)|1_x\rangle$ for $i = 2, 3$. $R = \exp(-\pi/2Y)$, where $Y = -i|0_z\rangle\langle 1_z| + i|1_z\rangle\langle 0_z|$, which satisfies $Ra_{\varphi i}^\dagger R^\dagger = a_{\varphi_{i+1(\mathrm{mod}4)}}^\dagger$ for all i. $|\psi^\pm\rangle = (|0_x 1_x\rangle \pm |1_x 0_x\rangle)/\sqrt{2}$ and $|\phi^+\rangle = (|0_x 0_x\rangle + |1_x 1_x\rangle)/\sqrt{2}$. We denote $P(\cdot) = (\cdot)(\cdot)^\dagger$.

The protocol of the MDI-SARG04 QKD. The protocol runs as follows:

(a1) Alice and Bob choose a bit value i and i' ($i, i' = 0, 1$), respectively, and they encode the bit value into the photonic states of their pulses as $\sum_n p_n |n_{\varphi_i}\rangle\langle n_{\varphi_i}|$ and $\sum_{n'} p_{n'} |n'_{\varphi_{i'}}\rangle\langle n'_{\varphi_{i'}}|$.

(a2) Alice and Bob rotate the polarization of their pulses by applying rotation R_k and $R_{k'}$ with randomly-chosen values of k(=0, 1, 2, 3) and k'(=0, 1, 2, 3), respectively, where R_k is defined by $R_k \equiv R^k$. After the rotation, Alice and Bob send the pulses to Eve's measurement unit (MU) through quantum channels.

(a3) Eve performs a measurement on the incoming pulses and announces to Alice and Bob over the authenticated public channel whether her measurement outcome is successful or not. When the outcome is successful, she also announces types of the successful events, either Type1 or Type2.

(a4) Alice and Bob broadcast k and k', over the authenticated public channel. If the measurement outcome in (a3) is successful with Type1 and $k = k' = 0, \ldots, 3$, they keep their bit values i and i' in (a1), and Alice flips her bit. If the measurement outcome in (a3) is successful with Type2 and $k = k' = 0, 2$, they keep their bit values i and i' in (a1). In all the other cases, they discard their bit values.

(a5) Alice and Bob repeat from (a1) to (a4) until the number of the successful events with rotation $k = k' = 0, \ldots, 3$ in Type1 becomes N_1 and $k = k' = 0, 2$ in Type2 becomes N_2. Let $N_i Q_i^{\mathrm{tot}}$ be the number of the successful detection event of Type i. Alice and Bob announce randomly-chosen $N_i Q_i^{\mathrm{tot}}\zeta$ bits over the authenticated public channel, where ζ is much smaller than 1, and estimate the error rate e_i^{tot} in the remaining code bits. The estimated number of the bit error in the code bits is denoted by $e_i^{\mathrm{tot}} N_i Q_i^{\mathrm{tot}}(1-\zeta)$.

(a6) Alice and Bob perform error correction and privacy amplification on the remaining $N_i Q_i^{\mathrm{tot}}(1-\zeta)$ bits by their discussion over the public channel. As a result, they share a final key of length $G_1 N_1(1-\zeta) + G_2 N_2(1-\zeta)$.

At Eve's MU in (a3), honest Eve performs the Bell measurement in order to establish quantum correlations between Alice and Bob to generate the key. In Fig. 1, the experimental setup for the Bell measurement is depicted. It employs a half beam splitter (BS), two polarization BSs (PBSs), and the photon detectors. In the case where both Alice and Bob emit a single photon, the simultaneous photon detection events matching the pattern Type1 (Type2), listed in Table I, corresponds to the detection of $|\psi^-\rangle$ ($|\psi^+\rangle$). We emphasize that in the security proof we assume that Eve is malicious and has a control over the quantum channels, and all the bit errors are attributed to the consequence of the eavesdropping.

Limitation of the experimental setup. In prepare & measure setting, the SARG04 protocol is different from the BB84 protocol only in the post-processing part, *i.e.*, no modification is needed in the experimental setup. In the MDI setting, however, the experimental setup for the BB84 protocols[5] cannot be directly used in MDI-SARG04 as it induces a high bit error rate, and this is a significant qualitative difference of MDI setting from prepare & measure setting, implying that not all the prepare & measure QKD protocols cannot be directly converted to MDI setting. Therefore, we need to consider an alternative experimental scheme for MDI-SARG04. In this section, we first discuss why the setup for MDI-BB84 gives the high bit error rate, and then we propose alternative experimental schemes for MDI-SARG04.

For the explanation we denote by $F^{(n,m)}$ the joint probability that Eve receives n and m photons from Alice and Bob, respectively, and

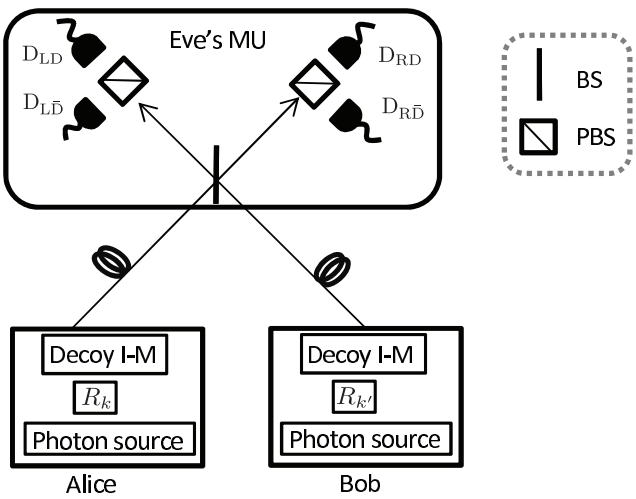

Figure 1 | Schematic of an experimental setup for the MDI-SARG04 QKD. The role of Eve's measurement unit (MU) is to perform entangling operation on the photons from Alice and Bob, which is implemented by using a half beamsplitter (BS) followed by polarization BSs (PBSs) and photon detectors. We note that the PBS passes the photons in 45° polarization and reflects the photons in −45° polarization.

Table I | Two types of the successful events announced by Eve's MU. Type1 is the coincidence detection events of D_{LD}&$D_{R\bar{D}}$ or D_{RD}&$D_{L\bar{D}}$ denoted in Fig. 1. Type2 is the coincidence events of D_{LD}&$D_{L\bar{D}}$ or D_{RD}&$D_{R\bar{D}}$. When the successful events are Type1 and Type2, Alice and Bob distill the states $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively, in the virtual protocol.

successful event	output
Type1 (D_{LD}&$D_{R\bar{D}}$ or D_{RD}&$D_{L\bar{D}}$)	$\|\psi^-\rangle$
Type2 (D_{LD}&$D_{L\bar{D}}$ or D_{RD}&$D_{R\bar{D}}$)	$\|\psi^+\rangle$

obtains the successful measurement outcome. Note that while we do not deal with the types of Eve's successful outcomes separately, the following discussion is valid for both types. For simplicity, we neglect all the losses, including those in the quantum channel and the photon detectors, and therefore we can also regard $F^{(n,m)}$ as $Q^{(n,m)}$, which is the joint probability that Alice and Bob respectively emit n and m photons and Eve obtains the successful measurement outcome. Like in the MDI-BB84 protocols, we assume that Alice and Bob use a phase randomized weak coherent light whose average photon number is much smaller than 1. Thus, we have $Q^{(1,1)}/2 \sim Q^{(2,0)} \sim Q^{(0,2)} \gg Q^{(n,m)}$ for $n + m \geq 3$. For simplicity, we assume Eve is honest, namely the bit error rate for $n = m = 1$ is zero, and all photon detectors have unit quantum efficiency and no dark counting. In the following, we show that even with this simplification favorable to Alice and Bob, no significant key is expected. To see this, we consider the bit error rate, and the total bit error rate e^{tot} is expected to be

$$e^{\mathrm{tot}} \sim \frac{Q^{(2,0)} e_{\mathrm{bit}}^{(2,0)} + Q^{(0,2)} e_{\mathrm{bit}}^{(0,2)}}{Q^{(1,1)} + Q^{(2,0)} + Q^{(0,2)}}, \qquad (1)$$

where $e_{\mathrm{bit}}^{(n,m)}$ is the bit error probability under the condition that Alice emits n photons and Bob emits m photons, and Eve announces the successful outcome. Note that equation (1) holds in both the MDI-BB84 and MDI-SARG04 protocols. It is clear from equation (1) that the bit error is caused by the case where one party emits two photons and the other party emits the vacuum. It is also clear that $e_{\mathrm{bit}}^{(2,0)}$ cannot be zero since the vacuum emission carries no bit information. In the case of MDI-BB84, this event is always discarded from the sifted key, and consequently the bit error rate in the key generation basis, *i.e.*, rectilinear basis, is zero. This is so because the two-photon states $|2_{45^\circ}\rangle$ and $|2_{-45^\circ}\rangle$, which contribute to the bit values, are orthogonal and they never produce the successful outcomes in Eve's projection measurement for the basis $\{|0_x\rangle, |1_x\rangle\}$. Therefore, in the experiment of MDI-BB84, the bit error rate is very small. In the case of MDI-SARG04, however, two states $|2_{\varphi 0}\rangle$ and $|2_{\varphi 1}\rangle$ consisting bit values are not orthogonal. This means that the two-photon emission contributes to the successful outcome. More precisely, $e^{\mathrm{tot}} \sim e_{\mathrm{bit}}^{(0,2)}/2 = 0.25$ holds from the direct calculation of $e_{\mathrm{bit}}^{(2,0)} = e_{\mathrm{bit}}^{(0,2)} = 0.5$ Note that $Q^{(1,1)}/2 \sim Q^{(2,0)} \sim Q^{(0,2)}$ and $e^{\mathrm{tot}} \sim 0.25$ hold for any linear loss transmittance channel. Therefore, we conclude that the use of the phase randomized coherent light source gives no significant key in MDI-SARG04. In order to generate a key in the MDI-SARG04 protocol, Eve's MU or the photon sources should be modified such that the probability of obtaining the successful outcome due to the two photons and the vacuum state is suppressed. In order to suppress the probability, we propose two experimental setups: (i) Eve performs quantum nondemolition (QND) measurement on the two incoming pulses from Alice and Bob just before mixing them as shown in Fig. 2(a). The QND measurement discriminates whether the photon number in the pulse is 0, 1 or more. Eve accepts only the case where $n \leq 1$ and $m \leq 1$ and discards the other cases with multiple photons. Thanks to the QND measurement, the total bit error rate is suppressed even if the phase randomized coherent light is used as a photon source. (ii) Without the modification of Eve's MU, Alice and Bob replace the phase randomized coherent light by a heralded single photon source based on a spontaneous parametric down-conversion (SPDC) and a threshold photon detector (see Fig. 2(b)). This dramatically reduces the probabilities of the events of $(n, m) = (2, 0)$ and $(0, 2)$. We will show that these setups enable us to generate the key later.

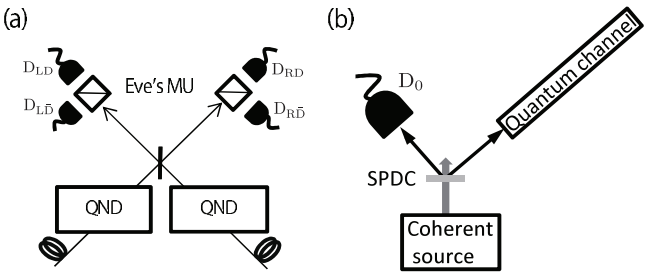

Figure 2 | Two experimental setups for generating the key in the MDI-SARG04 protocol. Both setups significantly eliminate the events caused by $(n, m) = (2, 0), (0, 2)$ and other problematic photon number configurations. (a) Eve performs the QND measurements on the pulses from Alice and Bob, and she does not perform the interference measurement for $n \geq 2$ or $m \geq 2$. Eve accepts only when $n \leq 1$ and $m \leq 1$ are satisfied. (b) A quasi single-photon source used by Alice and Bob, which is composed of the heralded SPDC process. When detector D_0 clicks, Alice/Bob sends her/his pulse at the remaining mode to Eve's MU.

Security proof. In this section, we discuss the unconditional security proof (*i.e.*, the security proof against most general attacks) of our scheme. The security proof is independent of the specific device models like in Fig. 2, namely it is valid for any Eve's MU and any photon sources of Alice and Bob. Our proof employs the security proof based on the entanglement distillation protocol (EDP)[3,26], where the distillation of $|\psi^-\rangle$ is considered for Type1 and that of $|\psi^+\rangle$ is considered for Type2. The proposed EDP-based virtual protocol, which is equivalent to the MDI-SARG04 QKD from Eve's viewpoint, runs as follows.

(V1) Alice and Bob prepare $|\Phi_{n(m),k(k')}\rangle_{A_1(B_1),A_2(B_2)}$, where $|\Phi_{n,k}\rangle_{\Gamma_1,\Gamma_2} = \left(|0_z\rangle_{\Gamma_1}|n_{\varphi_k}\rangle_{\Gamma_2} + |1_z\rangle_{\Gamma_1}|n_{\varphi_{1+k}}\rangle_{\Gamma_2}\right)/\sqrt{2}$ for Γ = A,B. Here $k(=0, 1, 2, 3)$ and $k'(=0, 1, 2, 3)$ are randomly chosen. The probability distribution of the photon number is equal to that of the photon source in the actual protocol. Alice and Bob send the n and m photon states in A_2 and B_2 to Eve's MU, respectively.

(V2) Eve performs a measurement on the photons coming from Alice and Bob, and announces to them whether the measurement is successful (including the type of the event) or not. If the measurement result is not successful, Alice and Bob discard their qubits.

(V3) Alice and Bob broadcast the labels k and k', respectively. In the cases of $k = k' = 1, 3$ with the announcement of Type2 or $k \neq k'$, Alice and Bob discard their qubits.

(V4) Alice and Bob repeat (v1) – (v3) many times until the number of the successful events for $k = k'$ becomes N_i for $i = 1, 2$, where i corresponds to the type of the events.

(V5) Let $N_i Q_i^{\mathrm{tot}}$ be the number of the successful detection event for Type i. Alice and Bob announce randomly chosen $N_i Q_i^{\mathrm{tot}} \zeta$-photon pairs over the authenticated public channel, where ζ is much smaller than 1, and then they perform Z-basis measurement on their qubits of the chosen pairs. By sharing their

measurement results over the authenticated public channel, they estimate the bit error rate on the code qubits denoted by e_i^{tot}. As a result, the number of the bit error is estimated to be $e_i^{\mathrm{tot}} N_i Q_i^{\mathrm{tot}}(1-\zeta)$.

(V6) They estimate the upper bound on the phase error rate $e_{i,\mathrm{ph}}^{(n,m)}$ for n and m photons from the bit error rate $e_{i,\mathrm{bit}}^{(n,m)}$ for n and m photons. Here the phase error is defined by the bit error that would have been obtained if they had measured the qubit pairs by X basis, which is the complementarity basis of the computational basis.

(V7) When the bit and the phase errors are smaller than a threshold value for entanglement distillation, they perform the distillation for $N_i Q_i^{\mathrm{tot}}(1-\zeta)$ qubit pairs. For the cases of Type1 and Type2, they distill the photon pairs in states $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively. We denote the number of the distilled maximally entangled qubit pairs as $G_i N_i(1-\zeta)$. Finally, by performing Z-measurements on the distilled photon pairs, they obtain the key.

The important quantities in the proof is the bit and phase errors, and the phase error rate determines the amount of privacy amplification. The bit error rate in the code bits of the virtual protocol, which is exactly the same as the one of the actual protocol, is directly estimated by test bits. On the other hand, the phase error rate is defined by the complementary basis X, which Alice and Bob never employ, and therefore this rate is not directly estimated in the protocols. Note that we are allowed to work on Alice's n-photon emission and Bob's m-photon emission separately, because Alice's and Bob's photon sources in the protocols are phase randomized. In the following subsections, we present the estimation of the phase error rates for the cases of Type1 and Type2 independently. We derive an upper bound on the phase error $e_{i,\mathrm{ph}}^{(1,1)}$ for $i = 1, 2$, where the superscript (1, 1) denotes $n = m = 1$ and the subscript represents the type of the successful outcome, and derive an upper bound on the phase error $e_{i,\mathrm{ph}}^{(1,2)}$. We show that in the case of $n = m = 2$, no key can be generated when the probability of Eve's successful outcome for the two-photon emission event is smaller than 1/16. We note that in the cases of either $n \geq 3$ or $m \geq 3$, Eve can perform an unambiguous state discrimination to one of the three-photon emission part[27,28], and thus we cannot extract the key from such events, given that the channel is lossy enough.

Finally, we note that given the phase error rates, $Q_i^{\mathrm{tot}} = \sum_{n,m} Q_i^{(n,m)}$ and $e_i^{\mathrm{tot}} = \sum_{n,m} Q_i^{(n,m)} e_{i,\mathrm{bit}}^{(n,m)} \Big/ Q_i^{\mathrm{tot}}$, the asymptotic key rate for Type i is written by[29]

$$\begin{aligned} G_i = {} & Q_i^{(1,1)}\left[1-h\left(e_{i,\mathrm{ph}}^{(1,1)}\right)\right] + Q_i^{(1,2)}\left[1-h\left(e_{i,\mathrm{ph}}^{(1,2)}\right)\right] \\ & + Q_i^{(2,1)}\left[1-h\left(e_{i,\mathrm{ph}}^{(2,1)}\right)\right] - f\left(e_i^{\mathrm{tot}}\right) Q_i^{\mathrm{tot}} h\left(e_i^{\mathrm{tot}}\right). \end{aligned} \tag{2}$$

Here $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary shannon entropy.

phase error estimation for (n, m) = (1, 1) and (1, 2). By the analysis based on the virtual protocol, we give the phase error estimation formula for $(n, m) = (1, 1)$ and $(n, m) = (1, 2)$. The estimation is performed for Type1 and Type2, separately, and we detail the derivation of the phase error estimation in Methods section.

In the case of Type 1, we have

$$e_{1,\mathrm{ph}}^{(1,1)} = \frac{3}{2} e_{1,\mathrm{bit}}^{(1,1)} \tag{3}$$

for $(n, m) = (1, 1)$ and

$$e_{1,\mathrm{ph}}^{(1,2)} = \min_{s_1}\left\{ s_1 e_{1,\mathrm{bit}}^{(1,2)} + f(s_1) \right\} \tag{4}$$

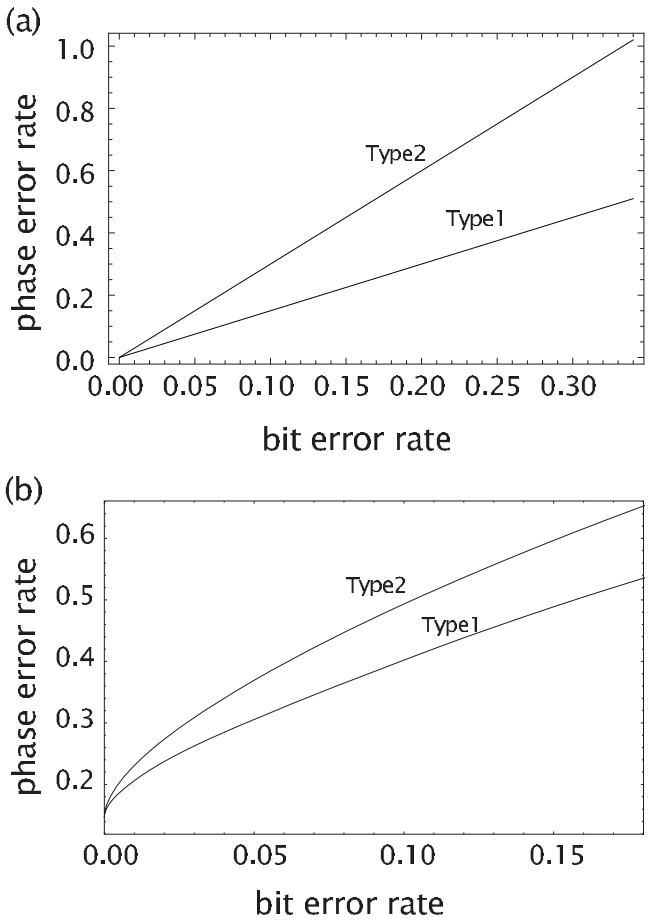

Figure 3 | The relations between the phase error rates and the bit error rates (a) for (*n*, *m*) = (1, 1) and (b) for (*n*, *m*) = (1, 2).

for $(n, m) = (1, 2)$, where

$$f(s_1) = \frac{3 - 2s_1 + \sqrt{6 - 6\sqrt{2}s_1 + 4s_1^2}}{6}. \tag{5}$$

In the case of Type 2, we have

$$e_{2,\mathrm{ph}}^{(1,1)} \leq 3 e_{2,\mathrm{bit}}^{(1,1)} \tag{6}$$

for $(n, m) = (1, 1)$ and

$$e_{2,\mathrm{ph}}^{(1,2)} = \min_{s_2}\left\{ s_2 e_{2,\mathrm{bit}}^{(1,2)} + g(s_2) \right\} \tag{7}$$

for $(n, m) = (1, 2)$, where $g(s_2)$ is the maximal solution of the following equation for x

$$\begin{aligned} & 4\sqrt{2}x^3 + 2\left(1 - 3\sqrt{2} + 3\sqrt{2}s_2\right)x^2 \\ & + 2\left(-1 + \sqrt{2} + \left(1 - 3\sqrt{2}\right)s_2 + \sqrt{2}s_2^2\right)x \\ & + \left(\sqrt{2} - 1\right)s_2 + \left(1 - \sqrt{2}\right)s_2^2 = 0. \end{aligned} \tag{8}$$

We depict the dependencies of the phase error rates on the bit error rates in Fig. 3.

Impossibility of generating a key from n = m = 2. For the case of $n = m = 2$, the key cannot be obtained for $n = m = 2$ in Type1 and Type2 by giving an explicit Eve's attack which give a phase error of 0.5, as long as the success probability of Eve's measurement conditioned that both Alice and Bob emit two photons is not larger than 1/16. We

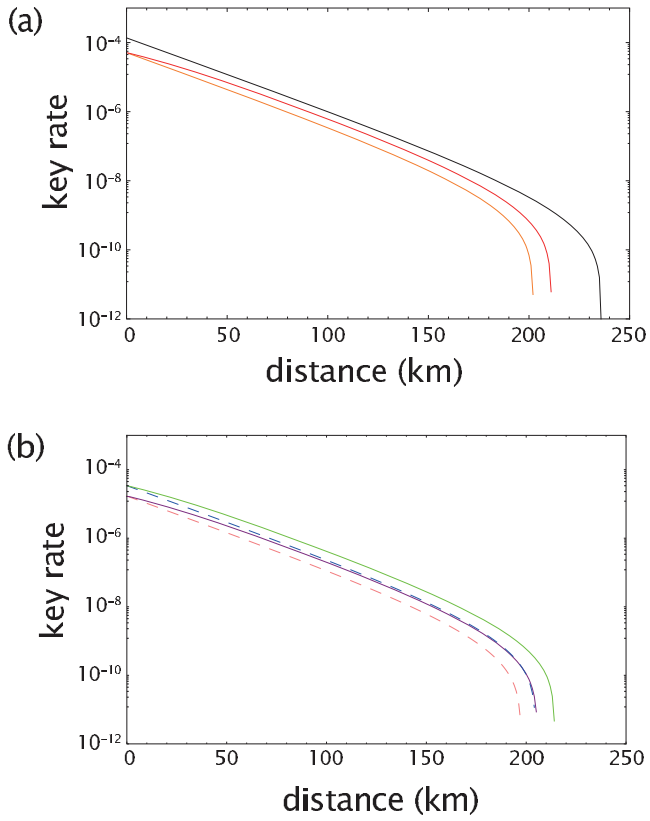

Figure 4 | The key rate when Alice and Bob use coherent pulses and Eve performs non-destructively exclusion of the multi-photons from Alice and Bob. (a) Bottom: the key rate of the MDI-SARG04 protocol from $(n, m) = (1, 1)$ only. Middle: the key rate of the MDI-SARG04 protocol from $(n, m) = (1, 1)$, $(1, 2)$ and $(2, 1)$. Top: the key rate of the MDI-BB84 protocol. (b) The upper and lower solid lines are the key rates from $(n, m) = (1, 1)$, $(1, 2)$ and $(2, 1)$ for Type1 and Type2, respectively. The upper and lower dashed lines are the key rates from $(n, m) = (1, 1)$ for Type1 and Type2, respectively.

show the proof in Methods section. We will prove that we cannot generate a key from $n = m = 2$ in the virtual protocol, and it follows that we cannot generate a key from $n = m = 2$ in the actual protocol either. To see this, note that the virtual protocol differs from the actual protocol only in the way to prepare the state, and the state prepared and post data-processing are exactly the same in both protocols. In other words, only the local operation needed in state-preparation process by the legitimated parties are different in the two protocols. By recalling that any local operation cannot convert a separable state into a non-separable state, we conclude that if we cannot generate a key from a virtual protocol, then we cannot generate a key from the actual protocol.

Simulation. Here we show the results of the key generation rate for the two experimental setups as shown in Figs. 2(a) and (b) by using typical experimental parameters taken from Gobby-Yuan-Shields (GYS) experiment[30], where the quantum efficiency and the dark counting of the all detectors in Eve's MU are $\eta = 0.045$ and $d = 8.5 \times 10^{-7}$, respectively, the loss coefficient of the quantum channel is $\xi = 0.21$ dB/km, and the inefficiency of the error correcting code is 1.22. In the simulation, we use infinite number of decoy states[31] in order to obtain $Q_i^{(1,1)}$, $e_{i,\mathrm{bit}}^{(1,1)}$, $Q_i^{(1,2)}$ and $e_{i,\mathrm{bit}}^{(1,2)}$. Assuming that the bit error is stemmed only from dark countings of the detectors, we ignore the other imperfections such as the misalignment of the devices. We also assume that the mean photon numbers of the signal pulses prepared by Alice and Bob are the same, and the MU

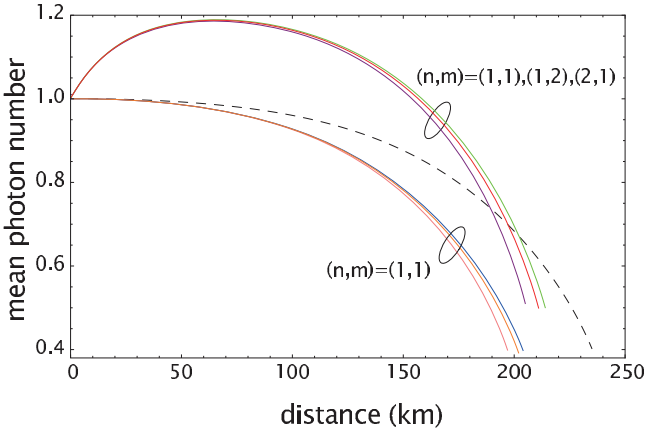

Figure 5 | The optimal mean photon number for the key rate in Fig. 4. For the key rates from $(n, m) = (1, 1)$, the three lines show the mean photon number when we consider only Type1, both types and only Type2 from the top. The mean photon numbers for the key rates from $(n, m) = (1, 1)$, $(1, 2)$ and $(2, 1)$ show a similar tendency. The dashed line is for the MDI-BB84 protocol.

in Eve is the middle of Alice and Bob. The mean photon number for the signal is optimized for maximizing the key generation rate at each distance. By using equation (2) with the above parameters and assumptions, we calculate the key generation rate as a function of the distance between Alice and Bob (i) when Eve postselects the events with $n \leq 1$ and $m \leq 1$ with the QND measurement as shown in Fig. 2(a) and Alice and Bob use the coherent pulses, and (ii) when Eve uses the MU in Fig. 1 and Alice and Bob use quasi single photon sources prepared by the SPDC in Fig. 2(b).

Case (i) – The simulation result of the key rate is shown in Fig. 4(a), and the mean photon number which maximizes the key rate is shown in Fig. 5. We also plot the key rates of Type1 and Type2 separately in Fig. 4(b). The details for obtaining these figures are shown in Supplementary. When the distance is zero, since there is no photon loss before the BS and the multi-photon emissions are excluded, the events of multi-photon input have no contribution to the key rate. In fact, in Fig. 4(a), the two key rates at zero distance obtained from only $(n, m) = (1, 1)$ and from both $(n, m) = (1, 1)$, $(1, 2)$ and $(2, 1)$ are exactly the same. When the distance becomes longer, we see from Fig. 5 that the contribution of the multi photons becomes larger. For the key rate from only $(n, m) = (1, 1)$, the mean photon number is monotonically decrease because the multi-photon emissions give only adverse effect. On the other hand, when we extract the key additionally from the multi photons, the mean photon number does not decrease monotonically, which shows an advantage in using multi-photon emission.

Case (ii) – Alice and Bob use quasi single photon sources by SPDC as shown in Fig. 2(b). Detector D_0 is the same as that used in Eve's MU, namely it is the threshold detector with the quantum efficiency of $\eta = 0.045$ and the dark counting of $d = 8.5 \times 10^{-7}$. Eve's MU is the same as that shown in Fig. 1. The key rate is shown in Fig. 6. The details for calculating the key rates are shown in Supplementary. The mean photon number which maximizes the key rate is shown in Fig. 7. From Fig. 6, we see that the key rate only from Type1 and that both from Type1 and Type2 intersect. For the distribution distance longer than the cross point, Type2 has no contribution of the key, which is shown by the blue line in the figure, and therefore it is better to generate a key from Type1 only. From Fig. 7, we see that the mean photon number is very small. This is so because the use of larger mean photon numbers results in two-photon emission, which increases the bit error rate. From all the figures of the key rate, one sees that the key rates of MDI-SARG04 are lower than those of MDI-BB84. This tendency holds also for prepare & measure SARG04[24,32],

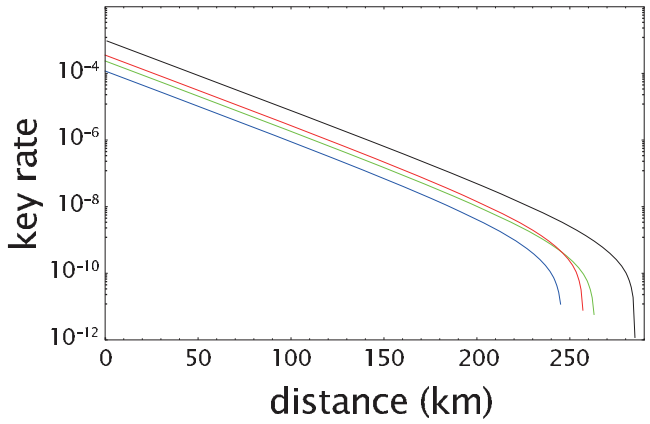

Figure 6 | The key rate when Alice and Bob use quasi single-photon sources prepared by the SPDC and Eve's MU is the same as the circuit used in the MDI-BB84 protocols. In this case, the total the key is approximately obtained from only the case of $(n, m) = (1, 1)$, and the successful events of $(n, m) = (1, 2)$ and $(n, m) = (2, 1)$ give little contribution to the key rate. This is so because the probability of the two-photon component in the heralded photon source is negligibly small compared with the probability of the single-photon component. The lines are for MDI-BB84 (black), for both types (red), Type1 (green) and Type2 (blue) of the MDI-SARG04.

and the higher phase error rates of SARG04 protocol than that of BB84 is the main reason of this tendency.

Discussion

As shown in Figs. 4(a) and 6, the key rates of the MDI-SARG04 protocol are smaller than those of the MDI-BB84 protocol for any distance. This is because the phase error rate of MDI-SARG04 is larger than that of MDI-BB84 and the scaling of all key rates for both protocols linearly depend on the total channel transmittance $T_{AB} = T_A T_B$ between Alice and Bob thanks to an infinite number of decoy states[31], where $T_{A(B)}$ is the transmittance between Alice (Bob) and Eve. On the other hand, the scaling of the key rate of MDI-SARG04 can be better than that of MDI-BB84 in a high loss and small error regime when we do not employ the decoy states in the experimental setup in Fig. 2(a), which one can see as follows. For the positive key rate, the joint probability that both of Alice and Bob emit single photons and those photons are detected must be higher than the probability of the emission of the photons satisfying $n + m \geq 4$ since

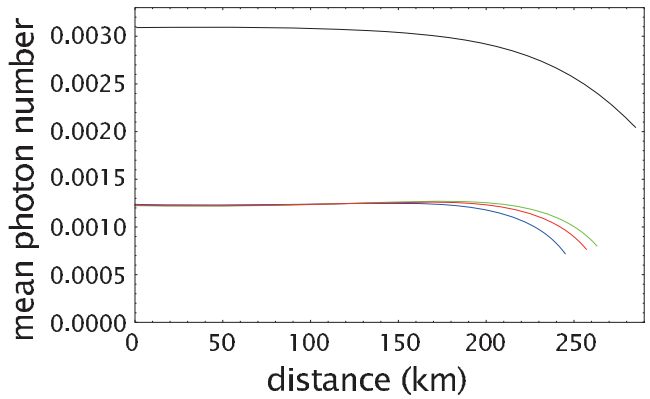

Figure 7 | The optimal mean photon number for the key rate in Fig. 6. The upper line (black) is the mean photon number for the MDI-BB84 protocol. The lower three lines are for the key rates of the MDI-SARG04 protocol obtained from Type1 (green), both types (red) and Type2 (blue) from the top.

Eve causes the detection event preferentially from the multi-photon events such as $n + m \geq 4$. Noting that the joint probablity is given by $\mathcal{O}(\mu_A \mu_B T_A T_B)$, where $\mu_{A(B)}$ is the mean photon number of Alice (Bob)'s coherent source, we have $\mathcal{O}(\mu_A \mu_B T_A T_B) \gg \mathcal{O}(\mu_A^2 \mu_B^2)$, $\mathcal{O}(\mu_A \mu_B T_A T_B) \gg \mathcal{O}(\mu_A \mu_B^3)$ and $\mathcal{O}(\mu_A \mu_B T_A T_B) \gg \mathcal{O}(\mu_A^3 \mu_B)$. These lead to $\mu_{A(B)} \sim \mathcal{O}\left(\sqrt{T_A T_B}\right)$, and we see that the scaling of the key rates of MDI-SARG04 is in the order of $\mathcal{O}(T_{AB}^2)$. By using a similar argument for MDI-BB84, $\mathcal{O}(\mu_A \mu_B T_A T_B) \gg \mathcal{O}(\mu_A \mu_B^2)$ and $\mathcal{O}(\mu_A \mu_B T_A T_B) \gg \mathcal{O}(\mu_A^2 \mu_B)$ must hold for the positive key rate, leading to $\mu_{A(B)} \sim \mathcal{O}(T_A T_B)$ and the scaling of the key rate of $\mathcal{O}(T_{AB}^3)$. As a result, the key rates of MDI-SARG04 is larger than those of MDI-BB84 in a high loss and small error regime, and this is one of the advantage of MDI-SARG04 over MDI-BB84. This tendency is similarly seen in the prepare & measure setting, where the key rates of SARG04 and BB84 scale $\mathcal{O}\left(T_{AB}^{3/2}\right)$ and $\mathcal{O}(T_{AB}^2)$, respectively[25]. Note that implementation of the decoy state method makes the QKD system complicated as it requires the additional amplitude modulation, it increases the amount of classical communications, and the software must be modified such that it processes the data depending on whether the pulse is the decoy state or the signal state. Therefore, in some practical situations where simple implementation is preferable, MDI-SARG04 is advantageous over MDI-BB84.

In our analysis, we have considered the asymptotic length of the key. It is interesting to consider the security with finite resources[12,33,34]. Regarding with the analysis of the decoy state method with finite number of signals, we can directly apply the technique developed for MDI-BB84[12] to MDI-SARG04 since the estimation of the yields and the bit error rates of the single/two-photon part in a particular signal/decoy state is totally independent of the protocol that we run, and it is solely independent on the intensities of the signal/decoy states. On the other hand, however, the phase error estimation of MDI-SARG04 is essentially different from that of MDI-BB84. In the case of BB84-type protocol, Alice and Bob directly measure both the bit and phase errors in the test bits, which enables them to apply the random sampling theory for the phase error estimation in the code bits. In the case of MDI-SARG04, on the other hand, the phase error is not directly measured, and it is estimated via symmetry, *i.e.*, the random rotations and the filtering operation, as well as Azuma's inequality[35]. Therefore, the phase error estimation is essentially different from the one in BB84-type protocol, and we leave it for future works.

In the conclusion, we first proved the unconditional security of the MDI QKD based on the SARG04 protocol. In our security proof, we gave the upper bounds on the phase error rate when Alice and Bob emit single photons and when one party emit one photon and the other half emit two photons. For the case of the two photon emissions from both parties, we proved that a key cannot be generated as long as the probability of success in her measurement conditioned that both Alice and Bob emit two photons is not larger than 1/16. Another important issue to be addressed in MDI setting is what kind of measurement should be implemented experimentally at Eve's laboratory. We have shown that the measurement setup for BB84 in MDI setting cannot be used in SARG04 in MDI setting, and we proposed two measurement schemes for MDI SARG04. In the first one, Alice and Bob use heralded single photon sources prepared by SPDC. In the second one, Eve performs QND measurement on the two pulses coming from Alice and Bob individually. In our simulation based on these experimental setups, it was confirmed that these setup can generate a key.

Methods

Proof of the phase error estimation for $n = m = 1$. Here, we give the phase error estimation for $n = m = 1$. For this, it is convenient to recall a mathematical property of the maximally entangled state that $(I_1 \otimes M_2)|\phi^+\rangle_{12} = (M_1^T \otimes I_2)|\phi^+\rangle_{12}$ is satisfied

Figure 8 | Schematic that is equivalent to the EDP for $n = m = 1$. While Eve accesses only the photons in modes A_2 and B_2 in the actual protocol, we pessimistically suppose that she can prepare any state in A'_1 and B'_1 for simplicity of the proof.

for any operator M. Therefore $|\Phi_{1,k}\rangle_{A_1A_2}$ in (v1) is expressed as $|\Phi_{1,k}\rangle_{A_1A_2} \propto F_{1,A'_1} R^T_{k,A'_1} |\phi^+\rangle_{A'_1A_2}$, where $F_{1,A'_1} = \cos(\Pi/8)|0_x\rangle_{A_1}\langle 0_x|_{A'_1} + \sin(\Pi/8)|1_x\rangle_{A_1}\langle 1_x|_{A'_1}$. Physically, this identification can be interpreted as the situation where $|\phi^+\rangle$ is prepared by each of the parties, the filtering operation, of which successful case is described by F_1, is applied, and then each party sends the photons to Eve only when the filtering operation succeeds (also see Fig. 8). For the simplicity of the security proof, we make an overestimation of Eve's ability in terms of the accessibility of the photons, namely, we imagine Eve who has a direct access to photons of A'_1 and B'_1 rather than A_2 and B_2, and she can prepare any joint state of the photons of A'_1 and B'_1. For later convenience, we denote by $\rho^{(1,1)}_{A'_1B'_1|suc}$ the state prepared by Eve.

In the following, we first discuss the case of Type1. We define $\tilde{e}^{(1,1)}_{1,bit/ph} = \mathrm{tr}\left(\Pi^{(1,1)}_{1,bit/ph}\rho^{(1,1)}_{A'_1B'_1|suc}\right)$ as the joint probability that the photons in $\rho^{(1,1)}_{A'_1B'_1|suc}$ pass through the filtering operation and induces a bit/phase error to the state $|\psi^-\rangle$ after the rotation. Here $\Pi^{(1,1)}_{1,bit}$ and $\Pi^{(1,1)}_{1,ph}$ are POVM elements of the bit and phase error measurements on $\rho^{(1,1)}_{A'_1B'_1|suc}$, respectively. The probability that the two photons in $\rho^{(1,1)}_{A'_1B'_1|suc}$ pass through the successful filtering operation is described by $p^{(1,1)}_{1,fil} = \mathrm{tr}\left(\Pi^{(1,1)}_{1,fil}\rho^{(1,1)}_{A'_1B'_1|suc}\right)$, where the POVM element of the successful filtering operation on the two photons is

$$\Pi^{(1,1)}_{1,fil} = \frac{1}{4}\sum_{k=0}^{3} P\left(R_{k,A'_1}F^T_{1,A'_1}R_{k,B'_1}F^T_{1,B'_1}\right), \tag{9}$$

where $P(\cdot) = (\cdot)(\cdot)^\dagger$. The POVMs for the bit and the phase errors are written as

$$\Pi^{(1,1)}_{1,bit/ph} = \frac{1}{4}\sum_{i=0}^{1}\sum_{k=0}^{3} P\left(R_{k,A'_1}F^T_{1,A'_1}|i_{z/x}\rangle_{A_1}R_{k,B'_1}F^T_{1,B'_1}|i_{z/x}\rangle_{B_1}\right). \tag{10}$$

Applying the Bayes' rule, the bit error rate $e^{(1,1)}_{1,bit}$ and the phase error rate $e^{(1,1)}_{1,ph}$ in the final state in modes A_1 and B_1 are described by

$$e^{(1,1)}_{1,bit/ph} = \frac{\tilde{e}^{(1,1)}_{1,bit/ph}}{p^{(1,1)}_{1,fil}}. \tag{11}$$

The phase error estimation can be established by directly writing down the explicit form of equation (10) comparing each matrix element, and one can conclude that

$$\Pi^{(1,1)}_{1,ph} = \frac{3}{2}\Pi^{(1,1)}_{1,bit}. \tag{12}$$

Thus from equations (9) and (11), the phase error rate is precisely estimated, by using the bit error rate, as shown in equation (3). Thanks to Azuma's inequality[35], equation (3) holds for any eavesdropping including coherent attacks.

Next, we estimate the phase error rate for Type2. Because only the cases of $k = k' = 0, 2$ are accepted for Type2, the definition of the POVM element of the successful filtering operation is changed to

$$\Pi^{(1,1)}_{2,fil} = \frac{1}{2}\sum_{k=0,2} P\left(R_{k,A'_1}F^T_{1,A'_1}R_{k,B'_1}F^T_{1,B'_1}\right), \tag{13}$$

and the probability that the two photons in $\rho^{(1,1)}_{A'_1B'_1|suc}$ pass through the successful filtering operation is expressed by $p^{(1,1)}_{2,fil} = \mathrm{tr}\left(\Pi^{(1,1)}_{2,fil}\rho^{(1,1)}_{A'_1B'_1|suc}\right)$. We describe a joint probability that the two photons in $\rho^{(1,1)}_{A'_1B'_1|suc}$ pass through the successful filtering operation after the rotation and then the photons in modes A_1 and B_1 have a bit/phase error to the state $|\psi^+\rangle$ by $\tilde{e}^{(1,1)}_{2,bit/ph} = \mathrm{tr}\left(\Pi^{(1,1)}_{2,bit/ph}\rho^{(1,1)}_{A'_1B'_1|suc}\right)$. Like in the case of Type1, the POVM elements of $\Pi^{(1,1)}_{2,bit}$ and $\Pi^{(1,1)}_{2,ph}$ are written by

$$\Pi^{(1,1)}_{2,bit} = \frac{1}{2}\sum_{i=0}^{1}\sum_{k=0,2} P\left(R_{k,A'_1}F^T_{1,A'_1}|i_z\rangle_{A_1}R_{k,B'_1}F^T_{1,B'_1}|i\oplus 1_z\rangle_{B_1}\right) \tag{14}$$

and

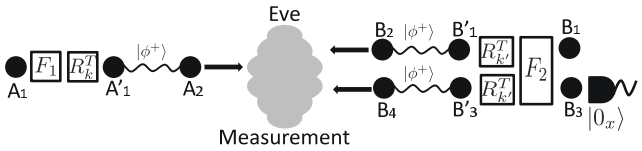

Figure 9 | Schematic which is equivalent to the EDP for $n = 1$ and $m = 2$. By Eve's announcement for the successful measurement on the photons in A_2, B_2 and B_4, the three-photon state $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$ is prepared.

$$\Pi^{(1,1)}_{2,ph} = \frac{1}{2}\sum_{i=0}^{1}\sum_{k=0,2} P\left(R_{k,A'_1}F^T_{1,A'_1}|i_x\rangle_{A_1}R_{k,B'_1}F^T_{1,B'_1}|i_x\rangle_{B_1}\right). \tag{15}$$

By using the Bayes' rule, the bit/phase error rate of $e^{(1,1)}_{2,bit/ph}$ in the final state is expressed by

$$e^{(1,1)}_{2,bit/ph} = \frac{\tilde{e}^{(1,1)}_{2,bit/ph}}{p^{(1,1)}_{2,fil}}. \tag{16}$$

In order to see the relation between the bit and phase error rates, we consider an inequality to bound the phase error as $se^{(1,1)}_{2,bit} - e^{(1,1)}_{2,ph} \geq 0$, where s is a real number, which is equivalent to $s\Pi^{(1,1)}_{2,bit} - \Pi^{(1,1)}_{2,ph} \geq 0$ for $p^{(1,1)}_{2,fil} > 0$. By considering a non-negativity condition of $s\Pi^{(1,1)}_{2,bit} - \Pi^{(1,1)}_{2,ph} \geq 0$, we see that this inequality always holds when $s \geq 3$, and therefore, we have the relation between the phase error rate and the bit error as shown in equation (6).

Proof of the phase error estimation for $n = 1$ and $m = 2$. Below, we give the phase error estimation for $n = 1$ and $m = 2$. By using the similar argument as $n = m = 1$, $|\Phi_{2,k}\rangle_{B_1,B_2}$ at Bob's side in (v1) is defined by $\langle 0_x|_{B_3}F_{2,B'_1B'_3}R^T_{k,B'_1}R^T_{k,B'_3}|\phi^+\rangle_{B'_1B_2}|\phi^+\rangle_{B'_3B'_4}$ as in Fig. 9, where $F_{2,B'_1B'_3} = \cos^2(\Pi/8)|0_x0_x\rangle_{B_1B_3}\langle 0_x0_x|_{B'_1B'_3} + \sin^2(\Pi/8)|0_x0_x\rangle_{B_1B_3}\langle 1_x1_x|_{B'_1B'_3} + \sqrt{2}\cos(\Pi/8)\sin(\Pi/8)|1_x0_x\rangle_{B_1B_3}\langle\psi^+|_{B'_1B'_3}$. Here we note that two-photon emission part is simulated by preparing two pairs of $|\phi^+\rangle$ followed by the rotation and the filtering operation on two qubits (see also Fig. 9). In this virtual protocol, while we consider two photons in different modes, this never underestimates Eve's ability. This is so because two photons in the different modes and two photons in a single mode can be converted just by an unitary transformation as $|\varphi_i\rangle_{B_2}|\varphi_i\rangle_{B_4} \to |2_{\varphi_i}\rangle_{B_2}$. We note that because the photon in mode B_3 is in $|0_x\rangle$ after the filtering operation, and it is decoupled from all the other systems, the component is not related to the security proof. Again, we employ the overestimation that Eve has the control over the state of the systems of A'_1, B'_1 and B'_3, and we denote the three-photon state by $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$, which is prepared by Eve after her announcement of the success. Like in the case for $n = m = 1$, we estimate a phase error for each case of Type1 and Type2 separately.

For Type1, define a POVM element of the successful filtering operations on $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$ as

$$\Pi^{(1,2)}_{1,fil} = \frac{1}{4}\sum_{k=0}^{3} P\left(R_{k,A'_1}F^T_{1,A'_1}R_{k,B'_1}R_{k,B'_3}F^T_{2,B'_1B'_3}\right). \tag{17}$$

Here the probability of the successful filtering operation is written by $p^{(1,2)}_{1,fil} = \mathrm{tr}\left(\Pi^{(1,2)}_{1,fil}\rho^{(1,2)}_{A'_1B'_1B'_3|suc}\right)$. We define $\tilde{e}^{(1,2)}_{1,bit/ph} = \mathrm{tr}\left(\Pi^{(1,2)}_{1,bit/ph}\rho^{(1,2)}_{A'_1B'_1B'_3|suc}\right)$ as a joint probability that the photons in $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$ pass through the filtering operation and induces a bit/phase error to the state $|\psi^-\rangle$ after the rotation. the successful filtering operation after the rotation is performed on the two photons in $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$ and then the photons in modes A_1 and B_1 have a bit/phase error to the state $|\psi^-\rangle$. Here, POVM elements of $\Pi^{(1,2)}_{1,bit/ph}$ are written by

$$\Pi^{(1,2)}_{1,bit/ph} = \frac{1}{4}\sum_{i=0}^{1}\sum_{k=0}^{3} P\Big(R_{k,A'_1}F^T_{1,A'_1}|i_{z/x}\rangle_{A_1} R_{k,B'_1}R_{k,B'_3}F^T_{2,B'_1B'_3}|i_{z/x}\rangle_{B_1}|0_x\rangle_{B_3}\Big). \tag{18}$$

The actual bit error rate $e^{(1,2)}_{1,bit}$ and phase error rate $e^{(1,2)}_{1,ph}$ for $n = 1$ and $m = 2$ are obtained by accommodating the normalization by $p^{(1,2)}_{1,fil}$, and they are expressed as

$$e^{(1,2)}_{1,bit/ph} = \frac{\tilde{e}^{(1,2)}_{1,bit/ph}}{p^{(1,2)}_{1,fil}}. \tag{19}$$

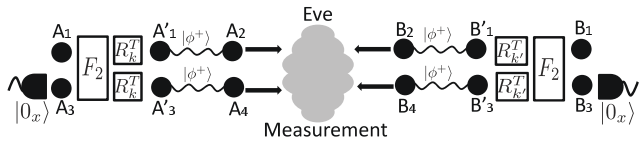

Figure 10 | Schematic which is equivalent to the EDP for $n = m = 2$. By Eve's announcement for the successful measurement on the photons in A_2, A_4, B_2 and B_4, the four-photon state $\rho^{(2,2)}_{A'_1A'_3B'_1B'_3|suc}$ is prepared.

In order to see the relation between the bit and phase error rates, we consider an inequality to bound the phase error as $e^{(1,2)}_{1,ph} \le s_1 e^{(1,2)}_{1,bit} + t_1$, where s_1 and t_1 are real numbers. By using equations (17) – (19), and the linearity of the trace, we obtain an inequality as $s_1\Pi^{(1,2)}_{1,bit} + t_1\Pi^{(1,2)}_{1,fil} - \Pi^{(1,2)}_{1,ph} \ge 0$, which is satisfied when

$$t_1 \ge f(s_1) = \frac{3 - 2s_1 + \sqrt{6 - 6\sqrt{2}s_1 + 4s_1^2}}{6}. \quad (20)$$

Therefore the phase error rate is given by using the bit error as shown in equation (4).

For Type2, we define a POVM element $\Pi^{(1,2)}_{2,fil}$ of the successful filtering operation by limiting the summation only to $k = 0, 2$ and by replacing 1/4 with 1/2 in equation (17). The probability of the successful filtering operation is described by $p^{(1,2)}_{2,fil} = \mathrm{tr}\left(\Pi^{(1,2)}_{2,fil}\rho^{(1,2)}_{A'_1B'_1B'_3|suc}\right)$. We also define joint probabilities of $\rho^{(1,2)}_{A'_1B'_1B'_3|suc}$ passing through the filtering and presenting bit and phase errors to the state $|\psi^+\rangle$ by $\tilde{e}^{(1,2)}_{2,bit} = \mathrm{tr}\left(\Pi^{(1,2)}_{2,bit}\rho^{(1,2)}_{A'_1B'_1B'_3|suc}\right)$ and $\tilde{e}^{(1,2)}_{2,ph} = \mathrm{tr}\left(\Pi^{(1,2)}_{2,ph}\rho^{(1,2)}_{A'_1B'_1B'_3|suc}\right)$. We define the POVM element of $\Pi^{(1,2)}_{2,ph}$ by limiting the summation only to $k = 0, 2$ and replacing 1/4 with 1/2 in equation (18), and that of $\Pi^{(1,2)}_{2,bit}$ is defined by limiting the summation only to $k = 0, 2$, replacing 1/4 with 1/2, and $|i_z\rangle$ with $|i \oplus 1_z\rangle$ for mode B_1. In a similar manner as the case of Type1 for $n = 1$ and $m = 2$, by using the bit error rate defined by $e^{(1,2)}_{2,bit} = \tilde{e}^{(1,2)}_{2,bit} \Big/ p^{(1,2)}_{2,fil}$, the phase error rate as $e^{(1,2)}_{2,ph} = \tilde{e}^{(1,2)}_{2,ph} \Big/ p^{(1,2)}_{2,fil}$ and real numbers s_2 and t_2, we consider an inequality as $e^{(1,2)}_{2,ph} \le s_2 e^{(1,2)}_{2,bit} + t_2$, which leads to $s_2\Pi^{(1,2)}_{2,bit} + t_2\Pi^{(1,2)}_{2,fil} - \Pi^{(1,2)}_{2,ph} \ge 0$. From this inequality, we obtain $t_2 \ge g(s_2)$, where $g(s_2)$ is the maximal solution of equation (8). Using $g(s_2)$, we have the relation between the phase error rate and the bit error as shown in equation (7).

Proof of the impossibility of generating a key from $n = m = 2$. For the case of $n = m = 2$, like in the previous subsection, $|\Phi_{2,k}\rangle_{A_1,A_2}$ at Alice's side in (v1) is obtained by $\langle 0_x|_{A_3} F_{2,A'_1A'_3} R^T_{k,A'_1} R^T_{k,A'_3} |\phi^+\rangle_{A'_1A_2} |\phi^+\rangle_{A'_3A_4}$, and $|\Phi_{2,k}\rangle_{B_1,B_2}$ at Bob's side is prepared by the same manner. As a result, the virtual protocol for $n = m = 2$ is equivalent to the successful situation of the filtering operations, which we depict in Fig. 10. We denote the state of Alice's and Bob's four qubits after Eve's successful announcement by $\rho^{(2,2)}_{A'_1A'_3B'_1B'_3|suc}$. In the following, we prove that the key cannot be obtained for $n = m = 2$ by giving an explicit Eve's attack, namely we give explicit states of A'_1, A'_3, B'_1 and B'_3 which give a phase error of 0.5. The key ingredient is that while Eve cannot manipulate these four qubits, she conclusively prepare such a state on their qubits by announcing the success of her measurement only when she succeeds an eavesdropping measurement on Eve's photons A_2, A_4, B_2 and B_4. This attack gives Eve the perfect information on the bit values when her measurement succeeds.

For Type1, the probability of the successful filtering operation is expressed by $p^{(2,2)}_{1,fil} = \mathrm{tr}\left(\Pi^{(2,2)}_{1,fil}\rho^{(2,2)}_{A'_1A'_3B'_1B'_3|suc}\right)$, where

$$\Pi^{(2,2)}_{1,fil} = \frac{1}{4}\sum_{k=0}^{3} P\left(R_{k,A'_1} R_{k,A'_3} F^T_{2,A'_1A'_3} R_{k,B'_1} R_{k,B'_3} F^T_{2,B'_1B'_3}\right). \quad (21)$$

The joint probability, that the filtering operation succeeds and the bit/phase error to the state $|\psi^-\rangle$ is detected, is expressed by $\tilde{e}^{(2,2)}_{1,bit/ph} = \mathrm{tr}\left(\Pi^{(2,2)}_{1,bit/ph}\rho^{(2,2)}_{A'_1A'_3B'_1B'_3|suc}\right)$, where

$$\Pi^{(2,2)}_{1,bit/ph} = \frac{1}{4}\sum_{i=0}^{1}\sum_{k=0}^{3} P\left(R_{k,A'_1} R_{k,A'_3} F^T_{2,A'_1A'_3} |i_{z/x}\rangle_{A_1} |0_x\rangle_{A_3} R_{k,B'_1} R_{k,B'_3} F^T_{2,B'_1B'_3} |i_{z/x}\rangle_{B_1} |0_x\rangle_{B_3}\right). \quad (22)$$

The bit/phase error rate is expressed as $e^{(2,2)}_{1,bit/ph} = \tilde{e}^{(2,2)}_{1,bit/ph} \Big/ p^{(2,2)}_{1,fil}$. One can confirm by direct calculation that a four-photon state of $|\mu_1\rangle_{A'_1B'_1A'_3B'_3} = |\psi^-\rangle_{A'_1B'_3} |0_x 1_x\rangle_{A'_3B'_1}$ gives $e^{(2,2)}_{1,bit} = 0$ and $e^{(2,2)}_{1,ph} = 0.5$, and another four-photon state $|\mu_2\rangle_{A'_1B'_1A'_3B'_3} = \left(|0_z 0_z 1_z 0_z\rangle_{A'_1A'_3B'_1B'_3} + |1_z 0_z 0_z 1_z\rangle_{A'_1A'_3B'_1B'_3}\right) \Big/ \sqrt{2}$, which is orthogonal to $|\mu_1\rangle_{A'_1B'_1A'_3B'_3}$, gives $e^{(2,2)}_{1,bit} = 0.5$ and $e^{(2,2)}_{1,ph} = 0.5$. Therefore, although Eve cannot touch the four modes A'_1, B'_1, A'_3 and B'_3, Eve can prepare the two states by a projective measurement on the four photons in A_2, B_2, A_4 and B_4 as $\left\{P(|\mu_1\rangle), P(|\mu_2\rangle), I - \sum_{i=1}^{2} P(|\mu_i\rangle)\right\}$. One sees this fact from the equation ${}_{A_2B_2A_4B_4}\langle\mu_i|\phi^+\rangle_{A'_1A_2} |\phi^+\rangle_{B'_1B_2} |\phi^+\rangle_{A'_3A_4} |\phi^+\rangle_{B'_3B_4} = |\mu_i\rangle_{A'_1B'_1A'_3B'_3} \Big/ \sqrt{16}$, which also implies that the preparation succeeds with a probability of 1/16. Thus a malicious Eve achieves the phase error rate of 0.5 for any bit error rate by distributing these states with a relevant probability. This means that the state in A_1 and B_1 is separable, and it follows that no key can be generated for $q^{(2,2)}_1 \le 1/16$, where $q^{(2,2)}_i$ is the probability of Eve's successful detection of Type i conditioned that both Alice and Bob emit two photons.

For Type2, with the same fashion as the case of $n = 1$ and $m = 2$, POVM elements $\Pi^{(2,2)}_{2,fil}$ for the successful filtering operation and $\Pi^{(2,2)}_{2,bit/ph}$ for the bit/phase error are defined by replacing the summation range of k, the prefactor and the proper inversion of the bit value of the projection in equations (21) and (22). We consider the following four orthogonal four-photon states for systems A'_1, B'_1, A'_3 and B'_3 $|v_1\rangle_{A'_1B'_1A'_3B'_3} = |\psi^+\rangle_{A'_1B'_1} |0_x 0_x\rangle_{A'_3B'_3}$, $|v_2\rangle_{A'_1B'_1A'_3B'_3} = |\psi^+\rangle_{A'_1B'_1} |0_x 1_x\rangle_{A'_3B'_3}$, $|v_3\rangle_{A'_1B'_1A'_3B'_3} = |\psi^+\rangle_{A'_1B'_1} |1_x 0_x\rangle_{A'_3B'_3}$ and $|v_4\rangle_{A'_1B'_1A'_3B'_3} = |\psi^-\rangle_{A'_1B'_1} |0_x 0_x\rangle_{A'_3B'_3}$. Each state can be prepared by Eve's projective measurement $\{P(|v_1\rangle), P(|v_2\rangle), P(|v_3\rangle), P(|v_4\rangle), I - \sum_{i=1}^{4} P(|v_i\rangle)\}$ on the four photons in A_2, B_2, A_4 and B_4 with a probability of 1/16. By calculating the error probabilities, we see that mixed states $0.25|v_1\rangle\langle v_1| + 0.75|v_2\rangle\langle v_2|$ and $0.75|v_3\rangle\langle v_3| + 0.25|v_4\rangle\langle v_4|$ give $\left(e^{(2,2)}_{2,bit}, e^{(2,2)}_{2,ph}\right) = (0, 0.5)$ and $\left(e^{(2,2)}_{2,bit}, e^{(2,2)}_{2,ph}\right) = (0.5, 0.5)$, respectively. Therefore Eve achieves any bit error rate below 0.5 while keeping $e^{(2,2)}_{2,ph} = 0.5$ by distributing the above two mixed states with an appropriate probability. As a result, we conclude that for $q^{(2,2)}_2 \le 1/16$, the key cannot be obtained.

1. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48**, 351–406 (2001).
2. Lo, H. K. & Chau, H. F. Unconditional Security Of Quantum Key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
4. Lydersen, L. *et al.* Hacking commercial quantuk cryptography systems by tailored blight illumination. *Nat. Photonics* **4**, 686–689 (2010).
5. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
6. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* 175–179 (IEEE Press, New York, 1984).
7. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
8. Li, Z., Zhang, Y. C., Xu, F., Peng, X. & Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052301 (2014).
9. Tamaki, K., Lo, H. K., Fung, C. H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
10. Xiongfeng, M. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
11. Xu, F., Curty, M., Qi, B. & Lo, H. K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007 (2013).
12. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *arXiv*:1307.1081.
13. Rubenok, A., Slater, J. A., Chan, P., Lucio-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).
14. 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).
15. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *arXiv*:1306.6134.
16. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
17. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124 (1992).
18. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002).
19. Gisin, N. Towards practical and fast quantum cryptography. *arXiv:quant-ph/*0411022.
20. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
21. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011).
22. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863–1869 (1995).
23. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).

24. Tamaki, K. & Lo, H. K. Unconditionally secure key distillation from multi-photons. *Phys. Rev. A* **73**, 010302(R) (2006).
25. Koashi, M. Security of quantum key distribution with discrete rotational symmetry. *arXiv:quant-ph*/0507154.
26. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed State Entanglement and Quantum Error Correction. *Phys. Rev. A* **54**, 3824–3851 (1996).
27. Chefles, A. Unambiguous discrimination between linearly independent quantum states. *Phys. Lett. A* **239**, 339–347 (1998).
28. Chefles, A. Unambiguous discrimination between linearly dependent states with multiple copies. *Phys. Rev. A* **64**, 062305 (2001).
29. Gottesman, D., Lo, H. K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **5**, 325–360 (2004).
30. Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84**, 3762–3764 (2004).
31. Lo, H. K., Ma, X. & Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
32. Fung, C. H. F., Tamaki, K. & Lo, H. K. On the performance of two protocols: SARG04 and BB84. *Phys. Rev. A* **73**, 012337 (2006).
33. Tomamichel, T., Lim, C. C. W., Gisin, N. & Renner, R. Continuous Variable Quatnum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. *arXiv*:1103.4130v1.
34. Hayashi, M. & Tsurumaru, T. Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *arXiv*:1107.0589v2.
35. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J.* **19**, 357 (1967).

Acknowledgments

This work was supported by the Funding Program for World-Leading Innovative R & D on Science and Technology (FIRST), MEXT Grant-in-Aid for Scientific Research on Innovative Areas 21102008, MEXT Grant-in-Aid for Young scientists(A) 23684035, JSPS Grant-in-Aid for Scientific Research(A) 25247068 and (B) 25286077. KT acknowledges support from the National Institute of Information and Communications Technology (NICT) of Japan (project "Secure photonic network technology" as part of "The project UQCC").

Author contributions

The main ideas were developed by A.M., K.T. and R.I. All results are obtained through the discussion among A.M., K.T., R.I., T.Y. and N.I. A.M., K.T. and R.I. prepared the main manuscript text and all authors contributed to the editing.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

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

How to cite this article: 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; DOI:10.1038/srep05236 (2014).

SCIENTIFIC REPORTS

DOI: 10.1038/srep06498

SUBJECT AREAS:
QUANTUM PHYSICS
QUANTUM INFORMATION

SCIENTIFIC REPORTS:
4 : 5236
DOI: 10.1038/srep05236

Published:
10 June 2014

Updated:
29 September 2014

CORRIGENDUM: Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol

Akihiro Mizutani, Kiyoshi Tamaki, Rikizo Ikuta, Takashi Yamamoto & Nobuyuki Imoto

The Supplementary Information that accompanies this study was omitted from the original version of this Article.