Experimental quantum key distribution without monitoring signal disturbance

Hiromi Takesue1*, Toshihiko Sasaki2*, Kiyoshi Tamaki1 and Masato Koashi2

Quantum key distribution (QKD) is a method of realizing private communication securely against an adversary with unlimited power. The QKD protocols proposed and demonstrated over the past 30 years relied on the monitoring of signal disturbance to set an upper limit to the amount of leaked information. Here, we report an experimental realization of the recently proposed round-robin differential-phase-shift protocol. We used a receiver set-up in which photons are randomly routed to one of four interferometers with different delays so that the phase difference is measured uniformly over all pair combinations among five pulses comprising the quantum signal. The amount of leak can be bounded from this randomness alone, and a secure key was extracted even when a finite communication time and the threshold nature of photon detectors were taken into account. This demonstrates the first QKD experiment without signal disturbance monitoring, thus opening up a new direction towards secure communication.

As the Internet becomes indispensable in our society, the importance of communication network security is increasing more rapidly than ever. Quantum key distribution (QKD) offers the ultimate way to distribute secret keys between distant parties based on the laws of quantum physics and thus may possibly change the way we ensure security in future communication networks1. Since the proposal of the Bennett–Brassard 1984 (BB84) protocol2, various QKD protocols have been proposed3–9. Many QKD experiments have been performed to demonstrate the feasibility of high-speed10–14 and long-distance15–17 secure key distribution, and QKD systems have been shown to operate even in field environments18,19. It was believed until recently that, to guarantee the security of any QKD protocol, the sender Alice and the receiver Bob had to monitor the statistics of the measurement outcomes to determine the amount of privacy amplification20. Surprisingly, with a recently proposed protocol called the ‘round-robin differential phase shift’ (RRDPS) protocol, we can ensure the privacy of the final key without monitoring any statistics of the measurement outcomes21. In this Article, we report a proof-of-principle QKD experiment based on the RRDPS protocol.

One may wonder what makes such a fundamentally big difference in the RRDPS protocol. To answer this question, let us briefly explain the crux of the RRDPS protocol. The RRDPS protocol is similar to the original differential phase shift (DPS) protocol22–24 in the sense that both protocols employ trains of L coherent pulses as an information carrier sent by Alice, and each of the pulses is phase-modulated to incur either a 0 or π optical phase shift according to Alice’s random choice. A crucial difference between the RRDPS protocol and the DPS protocol lies in Bob’s detection unit. In the DPS protocol, Bob’s set-up reads out the relative phase of two adjacent pulses, while that of the RRDPS protocol randomly picks up two pulses from among L pulses and reads out the relative phase of the two pulses. This random choice brings an additional difficulty on top of the DPS protocol in relation to eavesdropping and, roughly speaking, the amount of privacy amplification per sifted key bit is given by h(ν/(L − 1)), where \( h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x) \) is the binary entropy function and \( \nu \) is the total number of photons contained in L pulses. This means in particular that as L increases, the amount of privacy amplification decreases. Because the privacy amplification factor does not depend on the parameters related to signal disturbance, the RRDPS protocol is in principle highly robust against channel disturbance for large L and provides a new route towards QKD over long distances and under a much harsher environment.

The receiver’s set-up in the original proposal21 assumed a single interferometer with an active variable delay, which is not so easy to realize at high speed and with good stability. Here, as a first demonstration, we have realized a round-robin phase difference measurement for five-pulse time-bin states by passively choosing one of four interferometers.

RRDPS protocol

In the RRDPS protocol, Alice, using a laser source, prepares a packet of L coherent optical pulses and modulates each pulse with a phase shift of either 0 or π. The state of the whole packet is given by

\[
|\Psi\rangle = \bigotimes_{k=1}^{L} |\alpha e^{i\phi_k}\rangle_k
\]

where \( |\alpha e^{i\phi_k}\rangle_k \) denotes the coherent state of the kth pulse. Here, the amplitude \( \alpha \) is related to the average photon number \( \mu \) per pulse as \( |\alpha|^2 = \mu \) and the phase \( \phi_k = [0, \pi] \). Let \( \nu \) be the total photon number in a packet. Then, the probability of finding more than \( \nu_{th} \) photons in a packet is given by

\[
Pr(\nu > \nu_{th}) \leq e_{\text{att}} := 1 - \sum_{\nu=0}^{\nu_{th}} \frac{(L\mu)^\nu e^{-L\mu}}{\nu!}
\]

Here, \( \nu_{th} \) is an integer constant chosen in the protocol. The packet is transmitted over a quantum channel and sent to Bob. Bob inputs the packet into a delayed interferometer whose delay time was randomly chosen from \( \{T, 2T, \ldots, (L - 1)T\} \), where T is the temporal interval between adjacent pulses. When the MT-delay(\( M \in \{1, 2, \ldots, L - 1\} \)) is chosen, Bob observes photon interferences in \( L - M \) slots (Fig. 1, inset). At those time slots, a photon is output from port 0 (1) when the phase difference

---

1 NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan. 2 Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan. *e-mail: takesue.hiromi@lab.ntt.co.jp; sasaki@qi.t.u-tokyo.ac.jp
This is the bit error rate and $T'$ is the sifted key length and $N_{\text{ch}}/N_{\text{em}}$ the probability of error caused by an intercept-and-resend attack against the DPS protocol. In the passive configuration adopted by Bob, one might wonder how the security is achieved by simply repeating a fixed measurement. This can be understood as follows. Because a valid outcome in the RRDPS protocol is generated when a packet contains a single photon, the role of the optical splitter can be regarded as routing the packet randomly to one of the four interferometers. Hence, it amounts to choosing randomly among four different measurements.

The photons from two output ports of each interferometer are then received by superconducting single-photon detectors (SSPD) based on NbN nanowires (Sconstel). Although eight detectors are needed for the passive configuration with four interferometers, a temporal multiplexing technique is used to halve the required number of detectors. As shown in Fig. 1, a port from a $T$-delay (3T-delay) interferometer is delayed by 250 ps and combined with that from a 4T-delay (2T-delay) interferometer using a 3 dB coupler, and input into an SSPD. The drawback of this temporal multiplexing is the additional 3 dB loss induced by the coupler. The detection signals from each SSPD are input into a time interval analyser (Picoquant) for recording the detection time instances and which-detector information. The detection efficiencies of the SSPDs are $\sim$19% at a dark count rate of $\sim$2 c.p.s. The timing jitter and the recovery time of the SSPDs are $\sim$40 ps (FWHM) and $\sim$20 ns, respectively. Therefore, the condition for the successful detection of a single photon is satisfied.
Figure 2 | Example of packet configuration and interference pattern at each interferometer.

respectively. The overall system loss (including the detection efficiencies of the SSPDs) is 12.7 dB. We applied a 200 ps time window to the obtained data to reduce the contribution of dark counts. The inter-symbol interference error caused by the SSPD timing jitter is estimated to be 0.04% (Supplementary Section S4).

Figure 2 is an example of the interference pattern observed by Bob. Although we can observe interference in every time slot (as in the original DPS protocol), we only use detection events that are obtained from the interference between two pulses within the same packet, which are shown by the yellow cells in Fig. 2. When we observe only one detection event in the yellow cells for a packet, we record the event as a new bit of the sifted key. We can estimate the frequency of Bob receiving two or more photons in a packet by observing the 'double clicks' between the detection events at detectors 'Ch 1 or Ch 2' and 'Ch 3 or Ch 4' in yellow cells in a packet. Note that such an event does not produce a bit of the sifted key. When the number of double-click events is $N_d$, the fraction in the $N$-bit sifted key that originated from the multi-photon received packets is no larger than $q_d := 8N_d/N$. The modified secure key length in the asymptotic limit that takes account of $q_d$ is given by (see Methods for details)

$$G = N(1 - bh(c_{th}) - q_d - (1 - q_d)h(c_{ph}')) \tag{6}$$

$$c_{ph}' = \frac{c_{th}}{Q(1 - q_d)} + \left(1 - \frac{c_{th}}{Q(1 - q_d)}\right)\frac{v_{ph}}{L - 1} \tag{7}$$

Parameter $q_d$ was included in the calculation of the amount of privacy amplification in our experiments, but the effect was almost negligible because $q_d$ was less than $10^{-3}$ in all runs.

Experimental result

We undertook key generation experiments with various channel loss values. At each loss we performed sifted key generation for an effective data acquisition time of 260 s. We optimized the average photon number per pulse for each loss as in Fig. 3b to maximize the secure key length based on the calculation described in the Methods. Figure 3c shows the error rate as a function of channel loss. The error rate at 0 channel loss was 1.5%, which was dominantly limited by the imperfect extinction ratio of the delayed interferometers. The asymptotic secure key rate obtained in the experiment is plotted in Fig. 3a, where squares and circles denote fibre transmissions and optical attenuation, respectively. The secure key rates were calculated using equation (6) with experimentally obtained sifted key lengths, error rates and the numbers of double-click events, with the assumption of $f = 1.1$. The results indicate that, asymptotically, we can generate secure keys up to a channel loss of 8.7 dB, and we have realized secure key distribution over a 30 km fibre.

We next analysed the security that takes account of the effect arising from the finiteness of the sifted key length, with a choice of the security parameter $d = 2^{-50}$. The finite-key security analysis procedure is shown in detail in the Methods. The analysis was performed first on the data shown in Fig. 3. The obtained secure key length is shown in Fig. 4a. This shows that we successfully generated secure keys for up to 20 km of fibre (4.7 dB loss) with the finite-key effect considered. We also undertook measurements with various data acquisition times at 0 dB transmission loss and 20 km fibre transmission to assess the sifted key length dependence on the secure key. The result is shown in Fig. 4b, where the fraction of the secure key length obtained with finite-key security analysis relative to the asymptotic secure key length is plotted as a function of the sifted key length. When the fibre length was 0 (denoted by circles), the fraction was 50% and 93% for sifted key lengths of 420 kbits (effective data acquisition time of 26 s) and 21 Mbits (1,300 s), respectively. We also obtained a secure key fraction of 80% for a 20-km-long fibre with a sifted key length of 5.1 Mbits taken in a 2,600 s data acquisition time.

Figure 3 | Experimental results. a. Secure key rate per pulse in the limit of asymptotic key length as a function of transmission loss. b. Average photon number per pulse used in the experiments for each transmission loss. c. Bit error rate as a function of transmission loss. In a-c the squares and circles denote fibre transmissions and optical attenuation, respectively. The solid curves in a-c are calculated from equation (6) with the average photon number per pulse optimized to maximize the secure key rate at each transmission loss (see Methods).
The analysis in ref. 21 predicted that the performance of the RRDPS protocol can be superior to the decoy-state BB84 protocol at a large error rate. However, in our experiment with $L = 5$ and the baseline system error of 1.5%, the secure key rate per sifted key bit in the asymptotic limit is as small as $1 - \beta h(0) - h(\rho_{ph}) \approx 0.06$, even if $\rho_{ph}$ is assumed to be $1/4$ (that is, $\rho_{ph} = 1$ and no multiphotons are emitted in a packet). This means that our experiment was already close to the edge of secure key generation with a relatively small $L$. By using a larger $L$, we can improve the performance of an RRDPS system significantly. The use of optical waveguide technologies will facilitate the implementation of a larger number of delays. Silica-waveguide-based optical delay lines with lengths as long as 4 m and a footprint of only $63 \times 12$ mm$^2$ have already been reported\textsuperscript{27}. With a 10 GHz clock QKD system as reported in ref. 16, we can implement a ~$200 T$ delay line with a 4 m waveguide.

With such technologies, we can further increase the number of interferometers in the multi-interferometer configuration used in the present experiment. A drawback of such a multi-interferometer scheme is that we need $2(L - 1)$ detectors, which will result in an increase in the effective dark count rate with an $O(L)$ scaling and thus lead to a shorter secure key distribution distance. Another practical disadvantage is increased detector cost. However, we may be able to avoid this problem by using SSPD array technologies, which have been studied intensively in recent years with a view to realizing photonic quantum computation on chip\textsuperscript{28}. An alternative to this scheme is to use an actively controlled variable-delay interferometer based on a nested interferometer configuration (for details see Supplementary Section S1). We can implement this active interferometer using a silica waveguide. A drawback of this scheme is the slow response speed of the silica-waveguide switches (on the scale of milliseconds), which are based on the thermo-optic effect\textsuperscript{29}. As a result, the key rate of an RRDPS system implemented with this interferometer is limited by the response speed of the switch.

We numerically evaluated the performance of an RRDPS system with $L = 128$ based on the two implementations described above and compared the results with those obtained with a system based on the decoy-state BB84 protocol with an infinite number of decoys\textsuperscript{30}. The detailed conditions are provided in Supplementary Section S1 and the simulation result is shown in Supplementary Fig. S2. When the system error was 1.5%, the decoy-state system outperformed the RRDPS systems both in terms of secure key rate and distribution distance. However, the RRDPS system performed better when the system error rate was close to 10%. When the system error rate was 10.2%, the tolerable error of the decoy-state system decreased to 24 dB and no secure key was generated if the system error rate was 10.3% or more. On the other hand, the performance of the RRDPS system did not change greatly even when the system error rate was large.

For example, at a 10.2% system error rate we could send the secure key over a 35 dB loss with a much larger secure key rate than that of a decoy-state system using the passive multi-interferometer configuration. With the active interferometer, although the key rate was small at relatively short distances because of the slow response of the switches, the tolerable channel loss could be increased to as much as 55 dB. Moreover, with future technological advancements, we may be able to realize both fast and long-distance QKD based on the RRDPS protocol by implementing an active interferometer with fast optical switches whose bandwidth can be more than 10 GHz using silica–lithium niobate hybrid integration technology\textsuperscript{31}. Thus, the RRDPS protocol has a clear advantage over the decoy-state protocol in noisy transmission channels where it is difficult to keep the baseline system error small. We believe that the importance of the present experiments lies in the fact that they confirm the possibility of key generation with a fundamentally new QKD scheme, which paves a new route toward QKD systems under harsher environments.

**Methods**

Methods and any associated references are available in the online version of the paper.
Received 19 January 2015; accepted 7 August 2015; published online 14 September 2015

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002).
2. Bennett, C. H. & Brassard, G. in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175–179 (IEEE Press, 1984).
3. Ekert, A. K. Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67, 661–663 (1991).
4. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121–3124 (1992).
5. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. Phys. Rev. A 51, 1863–1869 (1995).
6. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photon. 14, 378–381 (2013).
7. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. Phys. Rev. Lett. 89, 037902 (2002).
8. Scarani, V., Acín, 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).
9. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. Appl. Phys. Lett. 87, 194108 (2005).
10. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. I. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Opt. Express 16, 18790–18797 (2008).
11. Zhang, Q. et al. Megabits secure key rate quantum key distribution. New J. Phys. 11, 045010 (2009).
12. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Continuous operation of high bit rate quantum key distribution. Appl. Phys. Lett. 96, 161102 (2010).
13. Tanaka, A. et al. High-speed quantum key distribution system for 1-Mbps real-time key generation. IEEE J. Quantum Electron. 48, 542–550 (2012).
14. Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. Opt. Express 21, 24550–24565 (2013).
15. Gobyy, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. 84, 3762–3764 (2004).
16. Takesue, H. et al. Quantum key distribution over 40 dB channel loss using superconducting single-photon detectors. Nature Photon. 1, 343–348 (2007).
17. Korzh, B. et al. Provably secure and practical quantum key distribution over 307 km of optical fiber. Nature Photon. 9, 163–168 (2015).
18. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. New J. Phys. 11, 075001 (2009).
19. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. Opt. Express 19, 10387–10409 (2011).
20. Scarani, V. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301–1350 (2009).
21. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature 509, 475–478 (2014).
22. Waks, E., Takesue, H. & Yamamoto, Y. Security of differential-phase-shift quantum key distribution against individual attacks. Phys. Rev. A 73, 012344 (2006).
23. Wen, K., Tamaki, K. & Yamamoto, Y. Unconditional security of single-photon differential phase shift quantum key distribution. Phys. Rev. Lett. 103, 170503 (2009).
24. Tamaki, K., Koashi, M. & Kato, G. Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization. Preprint at http://arxiv.org/abs/1208.1995 (2012).
25. Honjo, T., Inoue, K. & Takahashi, H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer. Opt. Lett. 29, 2797–2799 (2004).
26. Honjo, T. & Inoue, K. Differential-phase-shift quantum key distribution with an extended degree of freedom. Opt. Lett. 31, 522–524 (2006).
27. Kwack, M. J. et al. Compact optical buffer module for intra-packet synchronization based on InP 1×8 switch and silica-based delay line circuit. IEEE Trans. Electron. E96–C, 738–743 (2013).
28. Najafi, F. et al. On-chip detection of non-classical light by scalable integration of single-photon detectors. Nature Commun. 6, 5873 (2015).
29. Goh, T. et al. Low-loss and high-extinction ratio silica-based strictly nonblocking 16×16 thermooptic matrix switch. IEEE Photon. Technol. Lett. 10, 810–812 (1998).
30. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. Phys. Rev. Lett. 94, 230504 (2005).
31. Yamazaki, H., Yamada, T., Goh, T., Sakamaki, Y. & Kaneko, A. 64QAM modulator with a hybrid configuration of silica PLCs and LiNbO3 phase modulators. IEEE Photon. Technol. Lett. 22, 344–346 (2010).

Acknowledgements

The authors thank Y. Yamamoto, T. Yamada and M. Oguma for discussions. This work was funded in part by the ImPACT Program of the Council for Science, Technology and Innovation (Cabinet Office, Government of Japan) and the Photon Frontier Network Program (MEXT).

Author contributions

H.T. designed and constructed the experimental set-up and performed the QKD experiments. T.S. and M.K. designed the detailed procedure for secure key generation. H.T., T.S. and K.T. undertook the data analysis. M.K. led the project. All authors discussed the results and wrote the paper.

Additional information

Supplementary information is available in the online version of the paper. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to H.T. and T.S.

Competing financial interests

The authors declare no competing financial interests.
Methods

Security proof outline. We outline a security proof against general attacks for the implementation used in the present experiment. This experiment can be distinguished in two ways from that proposed in ref. 21. First, Bob does not use an interferometer with an actively controlled variable-delay line, but employs a passive optical splitter followed by several interferometers with various temporal delays. As long as the number of photons received in a packet is one, this change does not make any difference in security proof because the positive operator-valued measure (POVM) characterizing this measurement is the same as that using the variable-delay line.

Second, Bob cannot measure the number of photons directly because he uses threshold detectors, whereas the proof in ref. 21 assumes the use of detectors that can discriminate a single photon from two or more photons. This is the point where extra consideration is needed, as we need to estimate the number of received packets containing one photon using threshold detectors.

We define a double-click event as a coincidence between a detection event at ‘Ch1 or Ch2‘ and one at ‘Ch3 or Ch4‘, both in the interference slots (yellow cells in Fig. 2) of the same packet. We assume that all four detectors have the same detection efficiency. This can be modelled by detectors with unit efficiency and a common linear absorber in front of Bob’s apparatus. In Supplementary Table S2, we show the probability that a photon in one pulse goes to each interferometer and is detected in the interference slots. We see that the probability that a photon in a packet is detected at ‘Ch1 or Ch2‘ is 1/4 regardless of which pulse the photon is in. The same is true for ‘Ch3 or Ch4‘. In calculating Supplementary Table S2, we have used the fact that the 1 × 4 splitter in Fig. 1 randomly routes the incident photon to one of the four output ports. When multiple photons are incident, each photon is independently and randomly distributed to the four output ports, regardless of the quantum state of the incident multiple photons. This means that the lower bound of the probability of a double-click event is 1/8 when there are two or more photons received in a packet.

Although the actual measurement device cannot discriminate the photon number, it is in principle possible to measure the total photon number in each packet in front of Bob’s apparatus without affecting any procedure in the protocol. Hence, we may, in principle, tag every packet that includes two or more photons. Let $N_{m}$ be the number of tagged packets among the $N_{m}$ packets received by Bob and $N_{j}$ be the observed number of double-click events. In the asymptotic limit of large $N_{m}$, we may assume that $N_{m}$ is no larger than $N_{m}$. The secure key is obtained by subtracting the same number of bits in the privacy amplification, leading to a modified formula for the secure key length given by equations (6) and (7).

Performance estimation with experimental parameters. To estimate the performance, we need to assume a channel model to determine the expected asymptotic values of $Q_{t}, e_{m}$, and $p_{z} = N_{m}/N_{m}$. We denote $d_{i}$ and $c_{m}$ as the dark count rate of the SSPD (per channel) and the baseline system error rate, respectively. We then assume that the sifted key rate per packet and the bit error rate are approximated with the following equations:

$$Q \approx \frac{\mu_{n}}{2} + (L - 1)d_{i}$$

$$e_{m} = \frac{(\mu_{n} + 2) c_{m}}{Q}$$

$$p_{z} \approx \frac{(\mu_{n})^{2}}{16}$$

Using these assumptions, we optimize $\mu$ to obtain a secure key rate.

Finite-key security analysis. We will obtain a secure key length $G_{f}$ and a security parameter $d$ from six protocol parameters $N_{m}\cdot N_{m}\cdot N_{m}\cdot N_{m}\cdot t_{i}$, and $s_{j}$. As the security parameter $d$, we adopt half the trace distance between the actual state $\rho_{\text{tag}}$ and an ideal state $\rho_{\text{ideal}}$. We define a function for the tail distribution for finding no fewer than $K$ successes in a binomial distribution as

$$f(k,n,p) = \sum_{j=0}^{n} p^{j}(1-p)^{n-j}$$

If $k/n > p$, it is bounded by $f(k,n,p) \leq 2^{-K(n)dp}$, where $D(q||p) = -\log_{2}(q/p) + (1-q) \log_{2}(1-q)/(1-p)$. A similar function for no more than $K$ successes is

$$g(k,n,p) = \sum_{j=0}^{k} p^{j}(1-p)^{n-j}$$

which is bounded by $g(k,n,p) \geq 2^{-K(n)dp}$ if $k/n < p$.

After a sifted-key generation session has finished, Bob first examines the number of double-click events $N_{c}$. If it is larger than a predefined threshold $N_{c}$, Alice and Bob discard the key.

We analyse two cases separately according to the number $N_{m}$ of multi-photon packets (tagged packets) received by Bob’s apparatus. If $N_{m}$ is larger than a predefined threshold $N_{m}$, Alice and Bob should discard the sifted key at least with a probability $1 - \epsilon_{1}$, where $\epsilon_{1}$ is defined as

$$\epsilon_{1} := \mathbb{E} \left( N_{m} \cdot N_{m} / \theta \right)$$

(13)

Given that producing no key is regarded as an ideal state, the security parameter is bounded as $d \leq \epsilon_{1}$.

When $N_{m} \leq N_{m}$, we can choose $N := N - N_{m}$ untagged packets from the $N$ packets, resulting in an $N$-bit sifted key. We then apply the security argument in ref. 21 to these $N$ packets, which is summarized as follows. For each of the $N_{m}$ packets emitted from Alice, we may assume that Alice is left with $L$ qubits such that the phase errors in the qubits in the standard basis $\{0,1\}$ would reveal the corresponding phase shift $\theta(n)$. On the other hand, the statistics of the $L$ qubits measured in the $\{0,1\}$ basis, where $|z| = 1/2$, are related to the property of the light source. Let $n_{z}$ be the number of qubits found in state $|z\rangle$. We then have $P(n_{z} \leq N_{m} / \theta) \leq e^{-\lambda n_{z}}$. Whenever Bob succeeds in detection, Alice may convert the $L$ qubits into a single qubit (we call it a sifted qubit) and then measures it in the standard basis to determine her sifted key bit. To prove the security, we ask what happens if Alice measures the sifted qubit in the $|z\rangle$ basis instead. We call this outcome for state $|z\rangle$ a phase error. It was shown20 that the probability of obtaining a phase error is no larger than $n_{z} = (k - 1)$. The security of the final key generated from the $N_{m}$ sifted key bits can then be related to the failure probability $\rho_{\text{fail}}$ of correcting the phase errors in the corresponding $N_{m}$ sifted qubits.

The total number of phase errors in the $N_{m}$ sifted qubits is estimated as follows. For each of the $N_{m}$ packets emitted from Alice, $n_{z}$ exceeds $\nu_{0}$ at most with probability $e^{-\lambda n_{z}}$. Therefore, the number $N_{m}$ of packets with $n_{z} \leq \nu_{0}$ is no larger than a predefined threshold value $N_{m}$ except for a small probability defined by

$$\epsilon_{2} := \mathbb{E} \left( N_{m} \cdot N_{m} / \eta \right)$$

(14)

This means that, except for the probability $\epsilon_{2}$, at least $N := N - N_{m}$ packets from the $N_{m}$ sifted qubits satisfy $n_{z} \leq \nu_{0}$. We define $N_{m}$ as the number of phase errors in the $N_{m}$ packets. The number $N_{m}$ should be no larger than a predefined threshold $N_{m}$ with a probability no smaller than $1 - \epsilon_{1} - \epsilon_{2}$, where $\epsilon_{1}$ is defined as

$$\epsilon_{1} := \mathbb{E} \left( N_{m} \cdot N_{m} / \theta \right)$$

(15)

As it makes the total number of phase errors in the $N_{m}$ sifted qubits no larger than $N_{m} + N_{m}$, a virtual phase error correction with a syndrome length $N_{m} + N_{m}$ will succeed at least with $1 - \rho_{\text{fail}}$, where $\rho_{\text{fail}} := \epsilon_{2} + \epsilon_{1} + \eta$. We define $\eta := 2^{-s}$. As a result, when $N_{m} \leq N_{m}$, the secure key length with the finite-length effect taken into account is given by

$$G_{f} = N - \rho N_{m}(c_{m}) - s_j - N_{m} \left( \frac{N_{m} + N_{m}}{N} \right) - s_j$$

(17)

where $s_j = -\log_{2} \eta$ bits are used for a verification of the bit error correction. The security parameter is bounded as $d \leq \eta \leq \sqrt{2} \rho_{\text{fail}}$ (ref. 20).

Because any attack by Eve can be regarded as a mixture of the two cases analysed above, $d$ is always bounded as

$$d \leq \max \left( \epsilon_{1}, \epsilon_{2}, \epsilon_{1} + \sqrt{2} \rho_{\text{fail}} \right)$$

(18)

To obtain the numerical results in this Article, we set $N_{m} = N_{m} / N_{m} / 3 / \sqrt{\rho_{\text{fail}}} / N_{m}$, which makes the probability of discarding the protocol negligibly small. We fixed $\epsilon_{1}, \epsilon_{2}, \epsilon_{1} + \eta$, and $\eta$ at $2^{-50}, 2^{-50}, 2^{-50}, 2^{-50}$, and $2^{-50}$, respectively. We then determined the values of $N_{m}, N_{m}, N_{m}$, and $s$ and $s_{j}$ to satisfy equations (13) to (15) and the definitions of $\eta$ and $\eta$. This achieves the condition $d \leq 2^{-50}$.

References

32. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect device. Quant. Inf. Comp. 4, 325–360 (2004).