doi:10.1038/nature13303

Practical quantum key distribution protocol without monitoring signal disturbance

Toshihiko Sasaki[1], Yoshihisa Yamamoto[2,3] & Masato Koashi[1]

Quantum cryptography[1–8] exploits the fundamental laws of quantum mechanics to provide a secure way to exchange private information. Such an exchange requires a common random bit sequence, called a key, to be shared secretly between the sender and the receiver. The basic idea behind quantum key distribution (QKD) has widely been understood as the property that any attempt to distinguish encoded quantum states causes a disturbance in the signal. As a result, implementation of a QKD protocol involves an estimation of the experimental parameters influenced by the eavesdropper's intervention, which is achieved by randomly sampling the signal. If the estimation of many parameters with high precision is required, the portion of the signal that is sacrificed increases, thus decreasing the efficiency of the protocol[9,10]. Here we propose a QKD protocol based on an entirely different principle. The sender encodes a bit sequence onto non-orthogonal quantum states and the receiver randomly dictates how a single bit should be calculated from the sequence. The eavesdropper, who is unable to learn the whole of the sequence, cannot guess the bit value correctly. An achievable rate of secure key distribution is calculated by considering complementary choices between quantum measurements of two conjugate observables[11]. We found that a practical implementation using a laser pulse train achieves a key rate comparable to a decoy-state QKD protocol[12–14], an often-used technique for lasers. It also has a better tolerance of bit errors and of finite-sized-key effects. We anticipate that this finding will give new insight into how the probabilistic nature of quantum mechanics can be related to secure communication, and will facilitate the simple and efficient use of conventional lasers for QKD.

In a QKD protocol, the sender Alice and the receiver Bob repeat transmission of quantum signals and accumulate raw bits of data through quantum measurements. Using public communication, each of them discards the apparently useless portion of the raw data to form a bit sequence called a sifted key. The sifted key of length N is then processed into the final key of a shorter length through error reconciliation and privacy amplification. Denoting the costs of the two procedures as H_{ER} and H_{PA}, the net production length G of the secure final key is given by

$$G = N(1 - H_{\mathrm{ER}} - H_{\mathrm{PA}}) \qquad (1)$$

When the bit errors between Alice's and Bob's sifted key occur at a rate e_{bit}, the ideal cost of error reconciliation in the asymptotic limit of large N is given by $H_{\mathrm{ER}} = h(e_{\mathrm{bit}})$ as Shannon entropy, with $h(x) := -x\log_2 x - (1-x)\log_2(1-x)$. The cost H_{PA} depends on how much information on the sifted key has leaked to an eavesdropper Eve. For example, it is given by $H_{\mathrm{PA}} = h(e_{\mathrm{bit}})$ in a simple proof[15] for the Bennett–Brassard 1984 (BB84) protocol[1]. In general, the formula varies depending on protocols and security proofs, and parameters other than e_{bit} are often monitored in the protocol and enter into the formula of H_{PA}. Nevertheless, so far H_{PA} has always been an increasing function of the amount of disturbance. This implies that the conventional QKD protocols[1–8,12–14] inherently rely on the original version of Heisenberg's uncertainty principle, which dictates that the more information Eve has obtained, the more disturbance she should have caused on the signal.

What we propose here is an entirely new approach to establishing private correlations between Alice and Bob under the presence of an eavesdropper Eve, in which the leaked information to Eve is bounded regardless of the disturbance that she causes on the quantum signal. The main idea is to encode many raw key bits on quantum systems coherently such that only a few bits can be read out at the same time, which enables Bob to specify randomly how the sifted key bit is calculated from the raw key bits. This randomness makes it hard for Eve to guess the calculated bit from what little knowledge on the raw key bits she has acquired.

Let us explain our QKD protocol in more detail using the schematics shown in Fig. 1a. The protocol proceeds as follows. (I) Alice encodes a random L-bit sequence $s_1 s_2 \cdots s_L$ on a weak signal. For the understanding of the basic idea, here we assume that the encoded signal is a single-photon state of L optical pulses

$$|\Psi_1\rangle := \frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{s_k} |k\rangle \qquad (2)$$

where the photon is in the kth pulse for state $|k\rangle$. (II) After possible intervention by Eve, Bob receives the signal. (III) An independent random

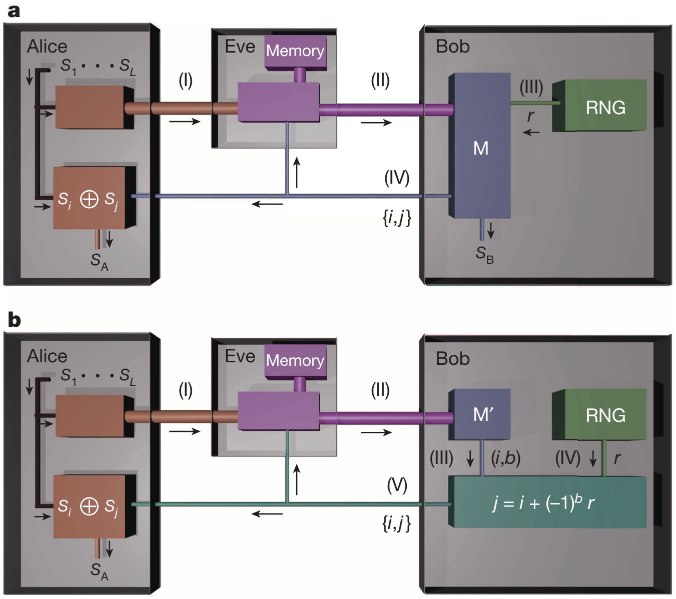

Figure 1 | Basic idea behind the proposed QKD scheme. a, **b**, Quantum signals flow through thick lines and classical ones through thin lines, in the order indicated by the Roman numerals. Eve tries to guess Alice's bit $s_A = s_i \oplus s_j$ in both figures, where indices $\{i, j\}$ are announced by Bob. In **a**, Bob conducts measurement M following random number generator RNG to guess s_A. In **b**, Bob conducts measurement M' prior to RNG, making it hard for anyone to guess s_A. As the procedures to generate indices $\{i, j\}$ in both figures are identical, every strategy used by Eve in **a** should work equally well in **b**.

[1] Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan. [2] E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA. [3] National Institute of Informatics, Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan.

number generator (RNG) announces a random value $r \in \{1, \cdots, L-1\}$. (IV) Through an optical interference measurement M, Bob tries to determine the value of $s_i \oplus s_j$ for a pair of indices $\{i, j\} \subset \{1, \cdots, L\}$ satisfying $j - i = \pm r (\mathrm{mod}\, L)$. Here the symbol $\oplus$ denotes summation modulo 2. In measurement M, Bob splits each pulse by a half beam-splitter and then superposes the kth and the k'th half pulses ($k' = k + r (\mathrm{mod}\, L)$, $k = 1, \ldots, L$) to measure the phase difference by detecting a photon. Whenever a photon is detected from the superposed ith and jth pulses, Bob announces $\{i, j\}$ and records the measured phase difference as his sifted key bit s_B. Alice records $s_A = s_i \oplus s_j$ as her sifted key bit. As shown in the Methods, if Bob receives the state $|\Psi_1\rangle$ intact, he learns s_A without errors.

We are now interested in how well Eve can guess the value of s_A. Figure 1a alone is not conclusive in this regard, because she has a control over the decision process of the indices $\{i, j\}$ through feeding a modified signal to Bob at step (II). To show that Eve's control is quite limited, consider another measurement procedure by Bob shown in Fig. 1b. In measurement M', Bob simply measures the location of the photon in the incoming L pulses to determine one of the indices, i. He also generates a random bit b. Subsequently, the RNG announces r, which determines the other index as $j = i + (-1)^b r (\mathrm{mod}\, L)$. As is proved in the Methods, this procedure is equivalent to M as far as the production of outcome $\{i, j\}$ is concerned. Hence, it suffices to show Eve's ignorance of s_A in Fig. 1b.

An intuitive reasoning for the ignorance is given as follows. Alice has emitted just one photon, so most of the L bits should be unknown to Eve when $L \gg 1$. In Fig. 1b, Eve's intervention affects only the decision of index i, and the other index j is chosen randomly from the rest of the $L-1$ bits through the random number r. We may thus expect that Eve has little information on s_j, and hence on $s_A = s_i \oplus s_j$.

What is remarkable here is that the above argument has no reference to how much Eve has disturbed the signal received by Bob. To make a rigorous security proof, we have only to show that Alice's sifted key bit s_A in Fig. 1b can be accumulated and converted to a secure final key, based on the fact that r is random and independent of i. There is no need to mention directly the state fed to Bob by Eve in the proof, and it is still valid for any attack strategy by Eve.

The difficulty in guessing the value of randomly chosen bit s_j appearing in Fig. 1b has been discussed in a slightly different context and called the information causality[16]. Our QKD scheme may be regarded as the combination of the information causality, which holds for classical and quantum signals alike, and the complementarity, which is unique to quantum mechanics. Bob's measurement in Fig. 1a reveals the phase difference, a wave-like property, while that in Fig. 1b identifies the location of the photon, a particle-like property. In quantum mechanics, such different measurements may result in incompatible consequences. In fact, Bob learns s_A in Fig. 1a, whereas in Fig. 1b the information causality forbids anyone from learning s_A, including Bob. The mere possibility of Bob's choosing the latter prevents Eve from learning s_A even if Bob has actually chosen the former.

It is also worth mentioning how our QKD protocol differs from the B92 protocol[3]. They are similar at many points. In both, Alice encodes the bit values on non-orthogonal states. Bob dictates which of the bits should be used. The dictation may be tampered with by Eve via modification of the signals, because it is based on the outcomes of Bob's measurement on them. It is, however, only our protocol that has a complementary scenario shown in Fig. 1b, which substantiates the existence of inherent randomness in Bob's dictation, beyond the reach of Eve's tampering.

The above basic idea can be implemented simply by a weak coherent laser pulse train as a light source and a variable-delay interferometer at the receiver (Fig. 2), which we name the round-robin differential phase-shift (RRDPS) QKD protocol. The setup is exactly the same as the differential phase-shift QKD protocol[7,17,18] except that the fixed delay line in the original is replaced by a variable delay line. For a security proof, we adopt a simple characterization of the source about the total photon number ν in the L-pulse train stated in the form of

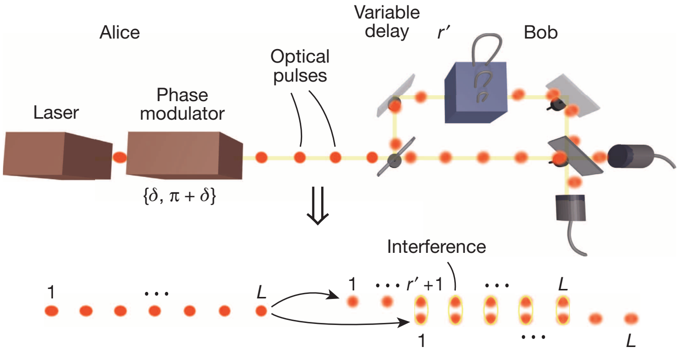

Figure 2 | Practical implementation of the proposed QKD scheme. Alice's laser emits a train of L pulses with interval T. She applies phase shift $\{0, \pi\}$ on each pulse according to a random bit sequence $s_1 \ldots s_L$. Bob splits the received train into two beams and superposes them after a random delay $r'T$ ($r' \in \{1, \ldots, L-1\}$). Detection of a photon determines Bob's sifted key bit s_B, and he announces the indices $\{i, j\}$ of the corresponding pair of pulses. Alice adopts $s_A = s_i \oplus s_j$ as her sifted key bit. The key rate is improved by applying random phase δ on each train (see the Methods).

$$\Pr(\nu > \nu_{\mathrm{th}}) \le e_{\mathrm{src}} \qquad (3)$$

with an integer $\nu_{\mathrm{th}} < \frac{L-1}{2}$ and a constant e_{src}. Let Q be the empirical rate of detection $Q := N/N_{\mathrm{em}}$ when a sifted key of length N is generated through N_{em} rounds of transmitting L-pulse trains. Then we can derive an asymptotic formula for the net production length of the secure key (see the Methods)

$$G = N\left[1 - h(e_{\mathrm{bit}}) - \frac{e_{\mathrm{src}}}{Q} - \left(1 - \frac{e_{\mathrm{src}}}{Q}\right) h\left(\frac{\nu_{\mathrm{th}}}{L-1}\right)\right] \qquad (4)$$

For clarity, let us consider the case where a nonclassical light source with $e_{\mathrm{src}} = 0$ is used instead of the laser, for which

$$G = N\left[1 - h(e_{\mathrm{bit}}) - h\left(\frac{\nu_{\mathrm{th}}}{L-1}\right)\right] \qquad (5)$$

The case with $\nu_{\mathrm{th}} = 1$ corresponds to the state $|\Psi_1\rangle$ used in the explanation of the basic idea. In equation (5), the third term $H_{\mathrm{PA}} = h(\nu_{\mathrm{th}}/(L-1))$ is a constant, which is in stark contrast with the conventional QKD protocols for which H_{PA} depends on the disturbance. The constant value of H_{PA} leads to two advantages of the new QKD protocol: (1) It has high tolerance of bit errors. For example, for $L = 128$ and $\nu_{\mathrm{th}} = 1$, G is positive up to $e_{\mathrm{bit}} = 0.35$. There is no fundamental limit on the error threshold smaller than 50%. (2) The secrecy of the final key is established after shortening the key length via privacy amplification by a fixed and predetermined fraction H_{PA}. There is no need to sacrifice a randomly chosen subset of signals to estimate an appropriate value of H_{PA}, which affects the rate of finite-sized key generation[9,10,19–21].

For the use of weak coherent pulses (WCPs) from a conventional laser, we show examples of asymptotic key rates per pulse, $G/(LN_{\mathrm{em}})$, as a function of channel transmission η in Fig. 3. For ground-based transmission, an optical fibre of 50 km decreases η by a factor of 10, whereas $\eta = 10^{-4}$ to 10^{-5} is expected for satellite-based transmission[22–24]. Figure 3 also shows rates of the BB84 protocol for comparison. When WCPs with the second-order correlation $g^{(2)}(0) = 1$ or a realistic single-photon source[25–27] with $g^{(2)}(0) = 0.01$ are used for BB84, the multi-photon emission from the source is exploited by Eve via photon-number splitting attacks[28,29], resulting in a poor key-rate scaling of $O(\eta^2)$. The present scheme with WCPs has a better scaling, close to $O(\eta)$, and surpasses the WCP-based or the single-photon-based BB84 protocol for small η.

There is a popular technique called decoy-state QKD[12–14], in which pulses with different amplitudes are randomly mixed in the signal to monitor the photon-number-splitting attacks. It stands in sharp contrast to our protocol. Figure 3 also shows the asymptotic key rate for the ideal decoy-state BB84 protocol[13], in which the statistics of single-photon

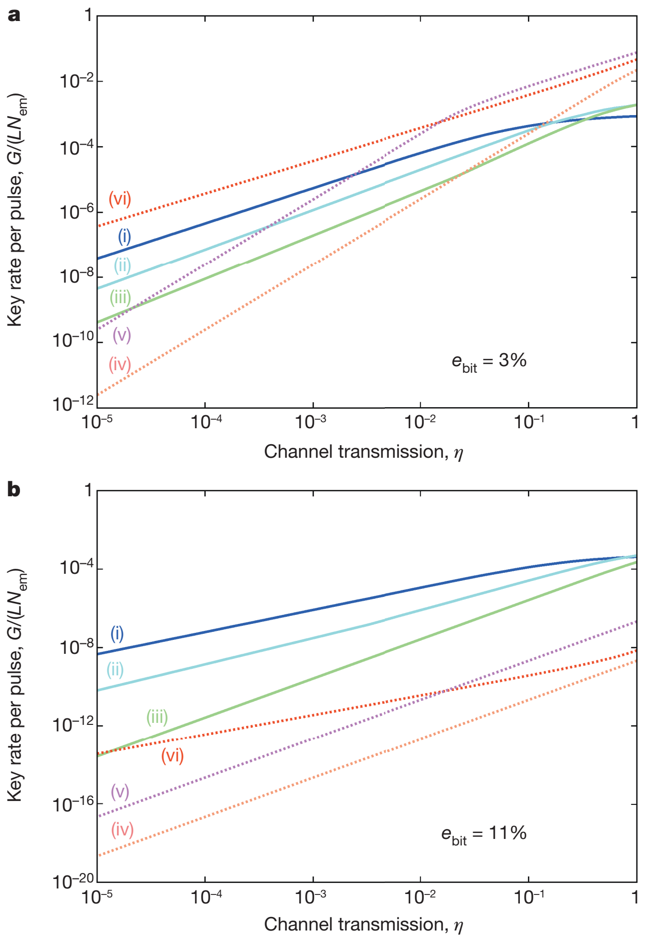

Figure 3 | Key rates versus channel transmission. **a**, The rates for $e_{\mathrm{bit}} = 0.03$. **b**, The rates for $e_{\mathrm{bit}} = 0.11$. Lines labelled (i)–(iii) represent the proposed protocol with $L = 128$, 32 and 16. The rates are optimized over the choice of ν_{th} and the mean photon number μ of a WCP through the relation $Q = L\eta\mu e^{-L\eta\mu}/2$ and $e_{\mathrm{src}} = 1 - \sum_{\nu=0}^{\nu_{\mathrm{th}}} \mu^{-\nu}/\nu!$. The optimized value of μ is around 0.05 for line (i) when $\eta < 0.01$. Lines labelled (iv)–(vi) represent BB84 protocols with double-pulse phase coding, using WCPs (iv), realistic single-photon source with the second-order correlation $g^{(2)}(0) = 0.01$ (v), and WCPs with infinite decoy states (vi).

emission events are precisely characterized via decoy signals. Although the asymptotic rate is better than our protocol by one order of magnitude, for a finite-sized key the decoy-state BB84 protocol suffers from a trade-off between the overhead of processing a large-sized key and the inefficiency of inserting many decoy signals to reach a required accuracy in the estimation of parameters[9,10]. Our protocol is much simpler in this regard, requiring no sampling for determining H_{PA}. As a result, a positive key rate is achieved even with N being as small as 10^3 (see Methods). For a higher bit-error rate, our protocol becomes better than the decoy-state BB84 even in the asymptotic limit, owing to its high tolerance on the errors. If we consider the use of modern digital coherent communication systems with 40 Gbits s^{-1} differential phase-shift signals and assume the receiver's overall detection efficiency to be 10%, we can generate a secure key at a rate of 200 bits s^{-1} for a channel length of 200 km and an error rate of 11%.

The variable delay used in our scheme will be implemented as a series of switchable optical delay lines of $T, 2T, 4T, 8T, \ldots$, where T is the time interval between the neighbouring pulses. Because the delay is fixed for each train of L pulses, the switching speed can be much slower than T, and it affects only the duty ratio.

The proposed QKD protocol demonstrates that spreading quantum information coherently over hundreds of quantum systems such as optical pulses provides a novel way of utilizing it for secure communication. The fact that the quantum effect survives under large noise suggests that similar encoding techniques may be useful for other applications of quantum information working in the presence of noise.

METHODS SUMMARY

Bob's alternative choices of measurements. Let $+_L$ denote summation modulo L. When a single-photon input state $\hat{\rho}$ is fed to measurement M, Bob announces $\{k, k+_L r\}$ and obtains $s_{\mathrm{B}} = s$ at probability $\langle k,s|\hat{\rho}|k,s\rangle/2$ with $|k,s\rangle := (|k\rangle + (-1)^s |k+_L r\rangle)/\sqrt{2}$. Given that $\langle k, s|\Psi_1\rangle = 0$ when $s \neq s_k \oplus s_{k+_L r}$, Bob's guess s_{B} is always equal to s_{A} if he has received state $|\Psi_1\rangle$. The probability of announcing $\{i, j\}$ (note that $\{j, i\}$ is regarded as the same value) is calculated to be $P(\{i,j\}) = [P(i) + P(j)] \left[\delta_{i+_L r,j} + \delta_{j+_L r,i}\right]/2$, where $P(k) = \langle k|\hat{\rho}|k\rangle$ is the probability of finding a photon in the kth pulse.

The calculation of $P(\{i, j\})$ for the case of Fig. 1b also leads to the same expression. This shows that the relation between the quantum signal received from Eve and the announced value $\{i, j\}$ is identical for Fig. 1a and Fig. 1b.

Derivation of secure key rates. The random phase shift δ enables Alice to tag each of the rounds with $\nu > \nu_{\mathrm{th}}$ in principle[30]. We assume that this tagged portion, at most Ne_{src}/Q bits, is fully leaked to Eve, leading to the $-e_{\mathrm{src}}/Q$ term in equation (4).

For the untagged portion, it can be shown that the sequence $s_1 s_2 \cdots s_L$ is equivalent to the outcome of $\{|0\rangle, |1\rangle\}$-basis measurement on L qubits prepared in a state fulfilling the promise that, if they are measured in a conjugate $\{|+\rangle, |-\rangle\}$-basis, no more than ν_{th} qubits are found to be in the $|-\rangle$ state. The key bit $s_{\mathrm{A}} = s_i \oplus s_j$ is then given by $\{|0\rangle, |1\rangle\}$-basis measurement on qubit j after a controlled-NOT operation on qubits i and j. It can be shown that the probability of finding qubit j in the state $|-\rangle$ is at most $\nu_{\mathrm{th}}/(L - 1)$, leading[11] to the remaining term in equation (4).

Online Content Any additional Methods, Extended Data display items and Source Data are available in the online version of the paper; references unique to these sections appear only in the online paper.

Received 29 November 2013; accepted 27 March 2014.

1. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* 175–179 (IEEE Press, 1984).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
3. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68,** 3121–3124 (1992).
4. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81,** 3018–3021 (1998).
5. 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).
6. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
7. Inoue, K., Waks, E. & Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **68,** 022317 (2003).
8. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88,** 057902 (2002).
9. Cai, R. Y. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11,** 045024 (2009).
10. Hayashi, M. & Nakayama, R. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths. Preprint at http://arxiv.org/abs/1302.4139 (2013).
11. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **11,** 045018 (2009).
12. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
13. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
14. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
15. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
16. Pawlowski, M. *et al.* Information causality as a physical principle. *Nature* **461,** 1101–1104 (2009).
17. Takesue, H. *et al.* Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature Photon.* **1,** 343–348 (2007).
18. 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).
19. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48,** 351–406 (2001).
20. Hayashi, M. & Tsurumaru, T. Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *New J. Phys.* **14,** 093014 (2012).
21. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nature Commun.* **3,** 634 (2012).

22. Bourgoin, J. *et al.* A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New J. Phys.* **15,** 023006 (2013).
23. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nature Photon.* **7,** 382–386 (2013).
24. Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photon.* **7,** 387–393 (2013).
25. He, Y.-M. *et al.* On-demand semiconductor single-photon source with near-unity indistinguishability. *Nature Nanotechnol.* **8,** 213–217 (2013).
26. Yuan, Z. *et al.* Electrically driven single-photon source. *Science* **295,** 102–105 (2002).
27. Claudon, J. *et al.* A highly efficient single-photon source based on a quantum dot in a photonic nanowire. *Nature Photon.* **4,** 174–177 (2010).
28. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51,** 1863–1869 (1995).
29. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
30. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect device. *Quant. Inf. Comput.* **4,** 325 (2004).

Acknowledgements We thank H. Takesue and K. Tamaki for helpful discussions. This work was supported by the Funding Program for World-Leading Innovative R & D on Science and Technology (FIRST), Grant-in-Aid for Scientific Research on Innovative Areas number 21102008 (MEXT), and Photon Frontier Network Program (MEXT).

Author Contributions All authors contributed to the initial conception of the ideas, to the working out of details, and to the writing and editing of the manuscript.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Correspondence and requests for materials should be addressed to M.K. (koashi@qi.t.u-tokyo.ac.jp).

METHODS

Bob's alternative choices of measurements. Let $+_L$ denote summation modulo L, and $\hat{P}(|\phi\rangle) : = |\phi\rangle\langle\phi|$. Bob's measurement M is fully characterized by a set of operators

$$\hat{E}^{(r)}_{k,s} \ : = \frac{1}{2}\hat{P}\left(\frac{|k\rangle + (-1)^s|k +_L r\rangle}{\sqrt{2}}\right) \qquad (6)$$

where the probability of outcome (k, s) ($k \in \{1,\ldots,L\}, s \in \{0,1\}$) is given by $\mathrm{Tr}\left(\hat{\rho}\hat{E}^{(r)}_{k,s}\right)$ for single-photon input state $\hat{\rho}$. From this outcome, he announces $\{k, k+_L r\}$ (the order being irrelevant) and adopts $s_\mathrm{B} = s$. Given that $\langle \Psi_1|\hat{E}^{(r)}_{k,s}|\Psi_1\rangle = 0$ when $s \neq s_k \oplus s_{k+_L r}$, Bob's guess s_B is always equal to s_A if he has received state $|\Psi_1\rangle$.

In measurement M, the probability $P(\{i,j\})$ of announcing $\{i,j\}$ (where $i \neq j$) is given by $\sum_s \mathrm{Tr}\left(\hat{\rho}\hat{E}^{(r)}_{i,s}\right)\delta_{i+_L r,j} + \sum_s \mathrm{Tr}\left(\hat{\rho}\hat{E}^{(r)}_{j,s}\right)\delta_{j+_L r,i}$, where $\delta_{x,y}$ is 1 for $x = y$ and 0 for $x \neq y$. This is calculated to be

$$P(\{i,j\}) = [P(i) + P(j)]\left[\delta_{i+_L r,j} + \delta_{j+_L r,i}\right]/2 \qquad (7)$$

where $P(k) = \langle k|\hat{\rho}|k\rangle$ is the probability of finding a photon in the kth pulse.

In Fig. 1b, Bob announces $\{k, k+_L(-1)^b r\}$ ($k = 1, \ldots, L$; $b = 0, 1$) at probability $P(k)/2$. Noticing that $P(\{i, j\})$ is contributed from the cases $k = i$ and $k = j$, we see that it is also given by equation (7). This shows that the relation between the quantum signal received from Eve and the announced value $\{i, j\}$ is identical for Fig. 1a and Fig. 1b. Therefore, if a statement regarding Eve's knowledge about Alice's sifted key is proved for Fig. 1b, it should also be true for Fig. 1a.

Derivation of secure key rates. Here we give a security proof and derive the final key rate for the proposed QKD protocol shown in Fig. 2. We first show that Alice's random bit sequence $s_1 \ldots s_L$ can be regarded as an outcome of Z-basis measurement on L qubits. Let $|\Psi\rangle$ be the state of an L-pulse train emitted from the laser source. In the actual setup, Alice chooses $s_1 \ldots s_L$ randomly and applies phase shifts accordingly, resulting in the emitted state $\otimes_k(-1)^{s_k\hat{n}_k}|\Psi\rangle$, where $\hat{n}_k \ : = \hat{a}^\dagger_k\hat{a}_k$ is the photon-number operator for the kth pulse. Instead[18], she could prepare L qubits and the L pulses in an entangled state

$$2^{-L/2}\bigotimes_{k=1}^{L}\sum_{s_k=0,1}|s_k\rangle_k(-1)^{s_k\hat{n}_k}|\Psi\rangle \qquad (8)$$

where $\{|0\rangle_k, |1\rangle_k\}$ is the Z-basis states of the kth qubit. The states of the L pulses are identical to those in the actual setup, and if Alice needs bit value s_k, she may simply measure the kth qubit on the Z basis.

It is useful for later discussion to ask what happens if Alice measures the L qubits in the X basis $\{|+\rangle, |-\rangle\}$ with $|\pm\rangle := 2^{-1/2}(|0\rangle \pm |1\rangle)$. Let n_- be the number of qubits found in state $|-\rangle$. The statistics of n_- is related to the photon number distribution in $|\Psi\rangle$. In fact, it is seen from equation (8) that if the kth pulse contains an even number of photons, the state of the kth qubit is $|+\rangle_k$, and if the number is odd, the state is $|-\rangle_k$. Hence n_- is no larger than the total photon number. The argument so far holds for any pure state $|\Psi\rangle$, so it is also true when the source emits a mixed state. We thus conclude that, if the source fulfils equation (3)

$$\Pr(n_- > \nu_\mathrm{th}) \leq e_\mathrm{src} \qquad (9)$$

Next, we relate Bob's apparatus in Fig. 2 to measurement M. We assume that the detectors can discriminate between a single photon from two or more photons, and that dark countings and inefficiency can be equivalently ascribed to a property of the transmission channel. Bob declares successful detection when a photon is detected from a superposed pulse and no other detection occurs in the whole pulse train. This ensures that the detected signal comes from a single-photon state. When the delay is $r'T$, the measurement is characterized similarly to equation (6) by operators

$$\hat{F}^{(r')}_{k',s} \ : = \frac{1}{2}\hat{P}\left(\frac{|k'\rangle + (-1)^s|k' + r'\rangle}{\sqrt{2}}\right) \qquad (10)$$

except that it is defined only if $1 \leq k' \leq L - r'$. To see that this is equivalent to measurement M except at an efficiency of 1/2, introduce an auxiliary random bit c to define $r = r'$ and $k = k'$ if $c = 0$, while $r = L - r'$ and $k = k' + r'$ if $c = 1$. Then r is uniformly random. Given r, the probability of outcome (k, s) for input state $\hat{\rho}$ is written as

$$\Pr(k,s) = \frac{1}{2}\mathrm{Tr}\left(\hat{\rho}\hat{F}^{(r)}_{k,s}\right) + \frac{1}{2}\mathrm{Tr}\left(\hat{\rho}\hat{F}^{(L-r)}_{k+r-L,s}\right) \qquad (11)$$

where it is understood that $\hat{F}^{(r')}_{k',s} = 0$ for $k' \geq L - r' + 1$ or $k' \leq 0$. It turns out that one of the terms always vanishes and $\Pr(k,s) = \mathrm{Tr}\left(\hat{\rho}\hat{E}^{(r)}_{k,s}\right)/2$. We thus conclude that Bob's apparatus is equivalent to measurement M preceded by a filter that allows only single-photon states to pass through with efficiency 1/2.

To assess how much Eve knows about Alice's key bit s_A, we may assume that Bob carries out measurement M'. Learning i, b and r, Alice applies a controlled-NOT operation to the qubit i as control and qubit $j = i + (-1)^b r (\mathrm{mod}\, L)$ as target. The key bit $s_\mathrm{A} = s_i \oplus s_j$ in the original protocol is now equivalent to the outcome of Z-basis measurement on qubit j. If one measures this qubit in X basis instead, the probability of a 'phase error', namely, of finding it in the $|-\rangle$ state, is no more than e_ph, defined by

$$e_\mathrm{ph} = \frac{e_\mathrm{src}}{Q} + \left(1 - \frac{e_\mathrm{src}}{Q}\right)\frac{\nu_\mathrm{th}}{L-1} \qquad (12)$$

This is because the controlled-NOT operation does not affect the X eigenstates of the target, the index j is chosen uniformly from all qubits except the ith via random number r, and finally equation (9) ensures that among the N rounds contributing the sifted key, at least $N - N_\mathrm{em}e_\mathrm{src}$ rounds satisfy $n_- \leq \nu_\mathrm{th}$ in the limit of large N. Then, if $e_\mathrm{ph} < 1/2$, she can extract a secure final key of length $N[1 - h(e_\mathrm{ph})]$ by privacy amplification[11]. Bob composes his sifted key from bit s_B in each round. The error reconciliation will be achieved by letting Alice send $Nh(e_\mathrm{bit})$ bits of encrypted information to Bob such that he can reconcile his sifted key to Alice's. The net production length is then given by

$$G = N\left[1 - h(e_\mathrm{bit}) - h\left(e_\mathrm{ph}\right)\right] \qquad (13)$$

This rate can be improved by applying a common random optical phase shift δ to all the L pulses in the actual protocol. This makes the emitted quantum state of the train into a classical mixture of states with fixed total photon numbers, enabling Alice to tag each of the rounds with $\nu > \nu_\mathrm{th}$ in principle though she need not do so in practice[30]. We may then assume that Eve completely knows the sifted key bits for the tagged portion (at most Ne_src/Q bits), while the rest is treated as if $e_\mathrm{src} = 0$. This leads to equation (4) in the main text and is used in Fig. 3.

If we omit the random optical phase shift δ, the rate for $L = 128$ and $e_\mathrm{bit} = 0.03$ decreases by about 10% from the rate shown in Fig. 3. On the other hand, if we are allowed to assume that the emitted photon number obeys a Poissonian distribution, the rate for $L = 128$ and $e_\mathrm{bit} = 0.03$ is larger than the one shown in Fig. 3 by about 30% even if we omit the random optical phase shift.

Finally, we briefly discuss an expected behaviour of our protocol for a finite-sized key. Let $\bar{f}(k; n,p) : = \sum_{j>k} p^j(1-p)^{n-j} n!/[j!(n-j)!]$ be the tail distribution for finding more than k successful events in a binomial distribution. Except for a probability $\epsilon_1 : = \bar{f}(Nr_1; N_\mathrm{em}, e_\mathrm{src})$, we may choose Nr_1 bits among the N sifted key bits to include all the tagged portion. We make no assumption about the phase errors for the chosen Nr_1 bits. If we count the number of phase errors for the remaining $N' := N(1 - r_1)$ bits, it should be no larger than $N'r_2$ except for a probability $\epsilon_2 : = \bar{f}(N'r_2; N', \nu_{th}/(L-1))$. The imperfection in the final key is characterized through the failure probability ϵ in identifying the phase error pattern when NH_PA bits of error syndrome are given[10,11,20]. Given $s > 0$, we choose r_1 and r_2 to satisfy $\epsilon_1 = \epsilon_2 = 2^{-s}$. Then, we have $\epsilon \leq 3 \times 2^{-s}$ for $H_\mathrm{PA} = r_1 + (1 - r_1)h(r_2) + s/N$. The commonly assumed quality of the key corresponds to about $s = 70$ to 160.

As an example, consider the case with $L = 128$, $\eta = 2 \times 10^{-3}$, and $e_\mathrm{bit} = 0.03$. The results below do not change significantly if η is chosen to be smaller, such as $\eta = 10^{-5}$. Asymptotically, the rate is optimized when $\mu = 0.0541$ with $\nu_\mathrm{th} = 17$, leading to $p_1 := e_\mathrm{src}N_\mathrm{em}/N = 0.047$, $p_2 := \nu_\mathrm{th}/(L - 1) = 0.134$, and $H_\mathrm{PA} = H^\mathrm{asy}_\mathrm{PA} \ : = p_1 + (1 - p_1)h(p_2) = 0.588$. For a finite length N, let us first use a crude Gaussian approximation of $\ln\left[\bar{f}(k; n,p)\right] \cong -(k - np)^2/[(2np(1-p)]$. This leads to $r_1 \cong p_1 + \sqrt{(2\ln 2)p_1(s/N)}$ and $r_2 \cong p_2 + \sqrt{(2\ln 2)p_2(1-p_2)\left(s/N'\right)}$. For $N \gg s$, substituting numerics gives $H_\mathrm{PA} \cong H^\mathrm{asy}_\mathrm{PA}\left(1 + 1.98\sqrt{s/N}\right)$. A better estimate is given by a rigorous bound $\log_2\bar{f}(k; n,p) \leq -nD(k/n||p)$ with $D(q||p) := q\log_2(q/p) + (1 - q)\log_2[(1 - q)/(1 - p)]$. We calculated the finite-size rate after optimizing over μ and ν_th for each N, and then derived its fraction R to the asymptotic optimal rate of 1.16×10^{-5}. For $s = 100$, we found $R = 3.3\%$ for $N = 10^3$, $R = 53\%$ for $N = 10^4$, $R = 84\%$ for $N = 10^5$, and $R = 95\%$ for $N = 10^6$.