npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Quantum key distribution with setting-choice-independently correlated light sources

Akihiro Mizutani[1,2], Go Kato[3,4], Koji Azuma[5,4], Marcos Curty[6], Rikizo Ikuta[1], Takashi Yamamoto[1], Nobuyuki Imoto[1], Hoi-Kwong Lo[7] and Kiyoshi Tamaki[5,8]

Despite the enormous theoretical and experimental progress made so far in quantum key distribution (QKD), the security of most existing practical QKD systems is not rigorously established yet. A critical obstacle is that almost all existing security proofs make ideal assumptions on the QKD devices. Problematically, such assumptions are hard to satisfy in the experiments, and therefore it is not obvious how to apply such security proofs to practical QKD systems. Fortunately, any imperfections and security-loopholes in the measurement devices can be perfectly closed by measurement-device-independent QKD (MDI-QKD), and thus we only need to consider how to secure the source devices. Among imperfections in the source devices, correlations between the sending pulses and modulation fluctuations are one of the principal problems, which unfortunately most of the existing security proofs do not consider. In this paper, we take into account these imperfections and enhance the implementation security of QKD. Specifically, we consider a setting-choice-independent correlation (SCIC) framework in which the sending pulses can present arbitrary correlations but they are independent of the previous setting choices such as the bit, the basis and the intensity settings. Within the framework of SCIC, we consider the dominant fluctuations of the sending states, such as the relative phases and the intensities, and provide a self-contained information-theoretic security proof for the loss-tolerant QKD protocol in the finite-key regime. We demonstrate the feasibility of secure quantum communication, and thus our work constitutes a crucial step towards guaranteeing the security of practical QKD systems.

npj Quantum Information (2019)5:8 ; https://doi.org/10.1038/s41534-018-0122-y

INTRODUCTION

Quantum key distribution (QKD)[1] is one of the most promising applications of quantum information processing, and it is now on the verge of global commercialisation. Nonetheless, there are still several theoretical and experimental challenges[2] that need to be addressed before its wide-scale deployment. One such challenge is the lack of practical security proofs that bridge the gap between theory and practice. In the security proof of QKD, one typically assumes some mathematical models for Alice and Bob's devices. However, if these models do not faithfully capture the physical properties of the actual QKD devices, the security of the systems is no longer guaranteed. In fact, such discrepancies between device models assumed in security proofs and the properties of actual devices could be exploited by Eve to attack both the source[3,4] and the detection apparatuses in refs [5–12]. It is therefore indispensable for realising secure QKD to develop security proof techniques that can be applied to actual devices.

One possible approach to close this gap is to use device-independent QKD.[13–16] Its main drawback is, however, that it delivers a quite low secret key rate with current technology, and it still requires some device characterisations. Note that device-independent QKD is known to be vulnerable to memory attacks.[17] See also ref. [18] for experimentally feasible countermeasures against this type of attacks. An alternative solution is to use measurement-device-independent (MDI) QKD,[19] which guarantees the security of QKD without making any assumption on the measurement device. That is, MDI-QKD completely closes the security loophole in the detection unit. This technique still requires, however, that certain assumptions on the source device are satisfied.

Unfortunately, the status of the security proofs with practical light sources is not fully satisfactory since most of the existing security proofs do not consider any imperfections (other than multiple photon emission) of the source devices. For instance, finite-key security analyses with a single-photon source[20–22] and those with a coherent light source[23–25] consider an unrealistic scenario in which there are no noises or imperfections in the QKD devices. As a result, the states of emitted pulses are identical and independent and the optical modulations are perfect, i.e., the phase modulation values are $\{0, \pi/2, \pi, 3\pi/2\}$ and the intensity of a pulse is modulated exactly as prescribed by the protocol. A few finite-key security analyses[26,27] consider the imperfections, where in ref. [27] nearest neighbour intensity correlations are accommodated, and in ref. [26] imperfect IID (independent and identically distributed) phase modulation errors are accommodated.

[1]Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan; [2]Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa 247-8501, Japan; [3]NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan; [4]NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan; [5]NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan; [6]EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain; [7]Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada and [8]Graduate School of Science and Engineering for Research, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan
Correspondence: Akihiro Mizutani (Mizutani.Akihiro@dy.MitsubishiElectric.co.jp)

Received: 30 April 2018 Accepted: 15 December 2018
Published online: 23 January 2019

Published in partnership with The University of New South Wales

npj nature partner journals

Among the imperfections in the source, one of the crucial problems is the presence of correlations among the sending pulses. We categorise these correlations into two types: the first type is setting-choice-independent correlation (SCIC) where the correlation is independent of Alice's choices of settings such as the bit, the basis, and the intensity settings, and the second type is setting-choice-dependent correlation (SCDC) where the correlation is dependent on Alice's setting choices. For instance, the former case (SCIC) may arise when the temperature in the laser drifts slowly over time due to thermal effects, where such drift could depend on how long we have operated a device and the ambient temperature of the room. Another example may be found in modulation devices which are operated by power supply fluctuating in time. On the other hand, the latter case (SCDC) occurs when the i^{th} sending state could depend on the previous setting choices that Alice has made up to the $(i-1)^{\text{th}}$ pulse. That is to say, secret information encoded in the previous quantum signals sent by Alice could be leaked to subsequent quantum signals sent by Alice. In other words, subsequent signals could act as side channels for previous signals. Recently, the SCDC between intensities of different pulses has been observed experimentally.[27] Also, the authors of ref. [27] conducted a security analysis which is valid for the restricted scenario where only the nearest neighbour intensity correlation is considered. More in general, however, the i^{th} state could be dependent on all the previous setting choices that Alice has made. This general correlation seems to be very hard to deal with theoretically, and even if we would have a theoretical countermeasure against it, the characterisation of the device might be highly non-trivial. Fortunately, it would be reasonable to assume that the SCDC could be eliminated if the modulation devices are initialised each time after Alice emits a pulse. For instance, before Alice sends the $(i+1)^{\text{th}}$ pulse, she applies a random voltage to the modulation devices several times until the setting-choice information up to the i^{th} pulse which is stored in the device is deleted. This potential solution may decrease the repetition rate of the source, but this could be overcome by multiplexing several sources, for instance by employing integrated silicon photonics.[28–30] With this reasonable solution, we are left with rigorously dealing with SCIC.

In this paper, we consider the dominant fluctuations of the sending state, such as the relative phase[26,31–33] and the intensity[26,27,34,35] within the framework of SCIC, and we provide an information-theoretic security proof in the finite-key regime. In particular, we consider the loss-tolerant QKD protocol[36] that is a BB84 type protocol which, unlike the standard BB84 protocol,[37] has the advantage of being robust against phase modulation errors. The loss-tolerant protocol is highly practical and has been experimentally demonstrated in both prepare & measure QKD[32,38,39] and MDI-QKD in ref. [33]. Our main contribution is to explicitly write down all the assumptions that we impose on QKD systems, and by using only these assumptions we give a self-contained security proof, which enhances implementation security of QKD. Our numerical simulations of the key generation rate show that provably secure keys can be distributed over long distances within a reasonable number of pulses sent, e.g. 10^{12} pulses.

The paper is organised as follows. In the Results section, we introduce the assumptions on the devices and the protocol considered. Also, we present a formula for the key generation length of the protocol. This formula depends on the parameters that need to be estimated; the estimation results for these parameters are shown in this section. In the final part of the Results section, we present our numerical simulation results for the key generation rate. Here, we assume realistic intervals for the actual phases and intensities under the framework of SCIC, and we show that secure communication is possible within a reasonable time frame of signal transmission, say 10^{12} signals.

RESULTS

Here, we introduce the assumptions on Alice and Bob's devices and the protocol we consider throughout this paper. To describe the assumptions, we use a shorthand notation $\boldsymbol{X}^i := X^i, X^{i-1}, \ldots, X^1$ for a sequence of random variables $\{X^j\}_{j=1}^{i}$ and $X^0 := 0$. In what follows, we first summarise the assumptions we make on the sending devices as well as those on the measurement devices, and then we move on to the description of the protocol.

Assumptions on Alice's transmitter

(A-1) Assumption on the sending state $\hat{\rho}^i(\theta^i,\mu^i)_{B^i}$

(A-1-i) Coherent-state assumption: Alice employs a coherent light source with a Poissonian photon number distribution in any basis, bit and intensity setting. Here we denote by $c^i \in \mathcal{C} := \{0_Z, 1_Z, 0_X\}$ Alice's bit and basis choice for the i^{th} pulse, and by $k^i \in \mathcal{K} := \{k_1, k_2, k_3\}$ Alice's intensity setting choice for the i^{th} pulse. The method introduced in this paper is general and can be applied to many different protocols. To simplify the discussion, however, we consider the loss-tolerant three-state protocol[36] with two decoy states.

(A-1-ii) Single-mode assumption: The i^{th} signals are in a single-mode. The single-mode condition means that each i^{th} emitted signal can be mathematically characterised by a single creation operator. This creation operator can, however, be different for different pulses.

(A-1-iii) Phase-encoding assumption: Alice uses phase encoding, i.e., she encodes the i^{th} bit and basis information into the relative phase θ^i between two pulses, a signal and a reference pulse. This assumption is for ease of discussion, and our proof can be applied to other encodings, such as a polarisation encoding.

(A-1-iv) Perfect phase randomisation assumption: A common phase $\delta \in [0, 2\pi)$ of signal and reference pulses is perfectly randomised.

(A-1-v) Same intensity assumption on signal and reference pulses: The intensities of the signal and the reference pulses are equal to $\mu^i/2$ where μ^i denotes the i^{th} actual value of the intensity generated by Alice's source. Note that this assumption is not mandatory. Even if the intensities of the i^{th} signal and reference pulses differ, the security proof can be established by introducing an additional filter operation in the security proof as explained in ref. [36].

(A-1-vi) No side-channel assumption: There are no side-channels in Alice's source and Eve can only manipulate Bob's system B with her arbitrary prepared ancilla.

With above six assumptions (A-1-i)-(A-1-vi), given the phase and the intensity, the i^{th} sending state $\hat{\rho}^i(\theta^i,\mu^i)_{B^i}$ to Bob in system B^i can be described as

$$\hat{\rho}^i(\theta^i,\mu^i)_{B^i} = \frac{1}{2\pi}\int_0^{2\pi} \hat{P}\left[\left|e^{\mathrm{i}(\delta+\theta^i)}\sqrt{\mu^i/2}\right\rangle_{S^i}\left|e^{\mathrm{i}\delta}\sqrt{\mu^i/2}\right\rangle_{R^i}\right] d\delta. \tag{1}$$

Here, we define $\hat{P}[|\cdot\rangle] := |\cdot\rangle\langle\cdot|$, the subscripts S^i and R^i respectively represent the optical modes of the i^{th} signal and reference pulse, and $\left|e^{i\theta}\sqrt{\mu}\right\rangle_{S^i(R^i)}$ denotes a coherent state in mode $S^i(R^i)$, i.e., $\left|e^{i\theta}\sqrt{\mu}\right\rangle_{S^i(R^i)} = e^{-\mu/2}\sum_{n=0}^{\infty}(e^{i\theta}\sqrt{\mu})^n|n\rangle_{S^i(R^i)}/\sqrt{n!}$ with $|n\rangle_{S^i(R^i)}$ being a Fock state with n photons in mode $S^i(R^i)$. Eq. (1) can be rewritten as

$$\hat{\rho}^i(\theta^i,\mu^i)_{B^i} = \sum_{n^i=0}^{\infty} p(n^i|\mu^i)\hat{P}\left[\left|\hat{\Upsilon}^i(\theta^i,n^i)\right\rangle_{B^i}\right], \tag{2}$$

where $p(n^i|\mu^i) := e^{-\mu^i}(\mu^i)^{n^i}/n^i!$ and the n-photon state

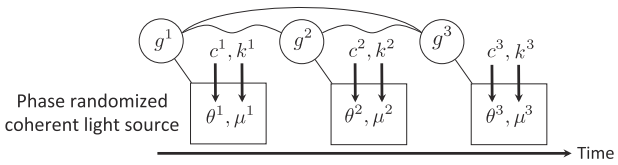

Fig. 1 A phase randomised coherent light source with SCIC (with $N_{\text{sent}} = 3$). The internal states of the source device $\{g^i\}_{i=1}^{N_{\text{sent}}}$ that determine $\{\theta^i\}_{i=1}^{N_{\text{sent}}}$ and $\{\mu^i\}_{i=1}^{N_{\text{sent}}}$ are setting-choice-independently correlated [see assumption (A-2)]. In each trial, Alice inputs c^i and k^i to the source device, and depending on these choices and g^i, the phase θ^i and the intensity μ^i are determined. Importantly, the internal states of the source device $\{g^i\}_{i=1}^{N_{\text{sent}}}$ can be arbitrary correlated with each other. Note that the secret information contained in previous signals (namely, $\boldsymbol{c}^{i-1}$ and $\boldsymbol{k}^{i-1}$) is not leaked to subsequent signals. This avoids the side channel problem

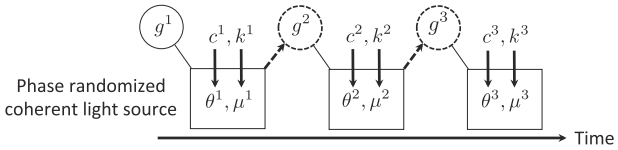

Fig. 2 This figure exemplifies SCDC that is forbidden in our security assumptions (with $N_{\text{sent}} = 3$). It shows that the i^{th} internal state of the source device g^i depends on the previous outcomes $\boldsymbol{\theta}^{i-1}$ and $\boldsymbol{\mu}^{i-1}$. In this case, the secret information contained in the previous quantum signals (namely, $\boldsymbol{c}^{i-1}$ and $\boldsymbol{k}^{i-1}$) could be leaked to the i^{th} quantum signal sent by Alice. In other words, the i^{th} sending signal could act as a side channel for the previous $(i-1)^{\text{th}}$ signals

$\hat{P}[|\hat{\Upsilon}^{n^i}(\theta^i, n^i)\rangle_{B^i}]$ of the i^{th} signal is defined as

$$\hat{P}[|\hat{\Upsilon}^{n^i}(\theta^i, n^i)\rangle_{B^i}] := \frac{\hat{N}_{B^i}^{n^i}\hat{\rho}^i(\theta^i, \mu^i)_{B^i}\hat{N}_{B^i}^{n^i}}{\mathrm{tr}\left[\hat{N}_{B^i}^{n^i}\hat{\rho}^i(\theta^i, \mu^i)_{B^i}\right]}, \tag{3}$$

where $\hat{N}_{B^i}^{n^i} := \sum_{k=0}^{n^i} \hat{P}\left[|n^i - k\rangle_{S^i}|k\rangle_{R^i}\right]$.

In the following, we first explain our correlation model for the source device, and we make assumptions on how the phases $\{\theta^i\}_{i=1}^{N_{\text{sent}}}$ and the intensities $\{\mu^i\}_{i=1}^{N_{\text{sent}}}$ are determined in the source device, where N_{sent} denotes the number of pulse pairs (signal and reference pulses) sent by Alice. See Fig. 1 for a schematic explanation of our correlation model of the source device. For illustration purposes, we exemplify in Fig. 2 setting-choice-dependent correlation (SCDC) that is not taken into account in our security analysis.

(A-2) Assumption on the correlation: setting-choice-independent correlation (SCIC). The correlation model we consider is setting-choice-independent correlation (SCIC), which means that the internal state of the source device which determines the i^{th} sending state is arbitrarily correlated with the previous internal states of the source device but it does not depend on the previous setting choices made by Alice. We denote by g^i the classical random variable representing the i^{th} internal state of the source device; it determines the correspondence between the setting choices (c^i and k^i) and the output parameters from the source device (θ^i and μ^i). We suppose that g^i depends on the past internal state of the source device $\boldsymbol{g}^{i-1}$ and is independent of the past setting choices and output parameters. Note that since the output parameters (θ^i and μ^i) have the information of the setting choices (c^i and k^i), we also need to impose the independence of g^i from $\boldsymbol{\theta}^{i-1}$ and $\boldsymbol{\mu}^{i-1}$. Hence, if we denote the i^{th} setting choices and output parameters by

$$P^i := (\theta^i, \mu^i, c^i, k^i), \tag{4}$$

the SCIC model can be mathematically expressed in terms of a probability distribution satisfying for any $\boldsymbol{P}^{i-1}$ and $\boldsymbol{g}^{i-1}$ the following

$$p(g^i|\boldsymbol{g}^{i-1}, \boldsymbol{P}^{i-1}) = p(g^i|\boldsymbol{g}^{i-1}). \tag{5}$$

For example, suppose that g^i is a temperature T^i of the source device of the i^{th} pulse emission, and $\hat{\rho}(\theta^i, \mu^i)$ is determined once T^i, c^i and k^i are fixed. Now, imagine a situation where θ^i and μ^i tend to deviate from ideal values when T^i gets higher. Then, if a temperature T^i is correlated with previous temperatures $\boldsymbol{T}^{i-1}$, sets of sending states $\{\hat{\rho}^i(\theta^i, \mu^i)\}_{c^i,k^i}$ for different i are also correlated. But, Eq. (5) excludes a situation where T^i depends on $\boldsymbol{P}^{i-1}$. This excludes, for instance, that if the previous setting choice is $c^{i-1} = 0_Z$, T^i gets increased, but otherwise does not. With the constraint in Eq. (5), the sets of sending states $\{\hat{\rho}^i(\theta^i, \mu^i)\}_{c^i,k^i}$ for different i are correlated, but each i^{th} setting choice information is only encoded to the i^{th} sending pulse.

(A-3) Assumption on the random choice of c^i and k^i. We assume that conditioned on the past realisation $\boldsymbol{P}^{i-1}$ and $\boldsymbol{g}^i$, then c^i and k^i are independent of each other and also independent of $\boldsymbol{P}^{i-1}$ and of $\boldsymbol{g}^i$, which is expressed by the following condition

$$p(c^i, k^i|\boldsymbol{g}^i, \boldsymbol{P}^{i-1}) = p(c^i)p(k^i). \tag{6}$$

(A-4) Assumption on the independence of θ^i and μ^i. We suppose that the phase θ^i (intensity μ^i) only depends on the setting choice c^i (k^i) and on g^i. Mathematically, this means that the probability distributions satisfy

$$p(\theta^i, \mu^i|c^i, k^i, \boldsymbol{g}^i, \boldsymbol{P}^{i-1}) = p(\theta^i|c^i, g^i)p(\mu^i|k^i, g^i). \tag{7}$$

(A-5) Assumption on unique determination of θ^i and μ^i. The phase θ^i (intensity μ^i) is uniquely determined given g^i and the setting choice c^i (k^i) as $\theta^i_{c^i,g^i}$ ($\mu^i_{k^i,g^i}$), that is, θ^i (μ^i) is a function of c^i (k^i) and g^i. This is expressed as

$$p(\theta^i|c^i, g^i) = \delta(\theta^i, \theta^i_{c^i,g^i}),\ p(\mu^i|k^i, g^i) = \delta\left(\mu^i, \mu^i_{k^i,g^i}\right), \tag{8}$$

where $\delta(x, y)$ denotes the Kronecker delta. Note that Eq. (8) does not impose any restriction on $\{g^i\}_{i=1}^{N_{\text{sent}}}$ since there exists the information of θ^i and μ^i somewhere in the source device, and we can take the parameters $\{g^i\}_{i=1}^{N_{\text{sent}}}$ such that $\{g^i\}_{i=1}^{N_{\text{sent}}}$ uniquely determine the correspondence between $\{c^i\}_{c^i\in\mathcal{C}}$ and $\{\theta^i_{c^i,g^i}\}_{c^i\in\mathcal{C}}$, and $\{k^i\}_{k^i\in\mathcal{C}}$ and $\{\mu^i_{k^i,g^i}\}_{k^i\in\mathcal{C}}$.

For our security analysis, we define the random variable associated to tagged events as follows.

(D-1) Definition of a tagged random variable. For the internal state of the source device g^i, we define the *untagged* set $\mathcal{G}^i_{\text{unt}}$ as

$$\mathcal{G}^i_{\text{unt}} = \{g^i|\forall c^i \in \mathcal{C},\ \forall k^i \in \mathcal{K},\ \theta^i_{c^i,g^i} \in R^{c^i}_{\text{ph}},\ \mu^i_{k^i,g^i} \in R^{k^i}_{\text{int}}\}, \tag{9}$$

and if $g^i \in (\notin)\mathcal{G}^i_{\text{unt}}$, we call the i^{th} pulse the untagged (tagged) signal, which we denote by $t^i = u$ (t). In the above definition of the untagged set, $R^{c^i}_{\text{ph}}$ and $R^{k^i}_{\text{int}}$ respectively denote a possible interval of the phase for c^i and a possible interval of the intensity for k^i.

(A-6) Assumption on the intervals for the phase and intensity. The i^{th} interval of the phase $R^{c^i}_{\text{ph}}$ is assumed to be given by

$$R^{0_Z}_{\text{ph}} = \left[\theta^{\text{L}}_{0_Z}, \theta^{\text{U}}_{0_Z}\right],\ R^{1_Z}_{\text{ph}} = \left[\theta^{\text{L}}_{1_Z}, \theta^{\text{U}}_{1_Z}\right],\ R^{0_X}_{\text{ph}} = \left[\theta^{\text{L}}_{0_X}, \theta^{\text{U}}_{0_X}\right] \tag{10}$$

for all instances i, where $R^{0_Z}_{\text{ph}}$, $R^{1_Z}_{\text{ph}}$ and $R^{0_X}_{\text{ph}}$ do not overlap each other and the parameters $\{\theta^{\text{L}}_c\}_{c\in\mathcal{C}}$ and $\{\theta^{\text{U}}_c\}_{c\in\mathcal{C}}$ must satisfy $-\frac{\pi}{6} < \theta^{\text{L}}_{0_Z} \le 0$, $0 \le \theta^{\text{U}}_{0_Z} < \frac{\pi}{6}$, $\frac{5\pi}{6} < \theta^{\text{L}}_{1_Z} \le \pi$, $\pi \le \theta^{\text{U}}_{1_Z} < \frac{7\pi}{6}$, $\frac{\pi}{3} < \theta^{\text{L}}_{0_X} \le \frac{\pi}{2}$, and

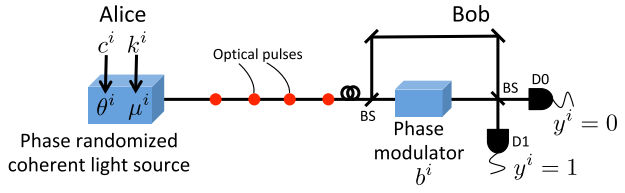

Fig. 3 Description of the actual protocol with a typical measurement setup. In the i^{th} trial (with $1 \le i \le N_{\text{sent}}$), Alice's source device emits two consecutive coherent pulses: a signal and a reference pulse. Alice first inputs the basis and bit information $c^i \in \mathcal{C}$ and the intensity setting $k^i \in \mathcal{K}$ that she selects probabilistically. Let θ^i and μ^i denote the relative phase between the signal and the reference pulses and the total actual intensity of both pulses, respectively. On the receiving side, Bob uses a 50:50 beamsplitter (BS) to split the received pulses into two beams. Afterward, he applies a phase shift 0 or $\pi/2$ to one of them according to his basis choice $b^i = Z$ or $b^i = X$, respectively. The pulses are then recombined at a 50:50 BS. A click in the detector D0 (D1) provides Bob the bit $y^i = 0$ ($y^i = 1$)

$\frac{\pi}{2} \le \theta^{\mathsf{U}}_{0_X} < \frac{2\pi}{3}$. Also, the i^{th} interval of the intensity $R^{k^i}_{\text{int}}$ has the form

$$R^{k}_{\text{int}} = [\mu^{-}_{k}, \mu^{+}_{k}], \tag{11}$$

for all instances i, and we suppose that the following three conditions are satisfied: $\mu^{+}_{k_3} < \mu^{-}_{k_2}$, $\mu^{+}_{k_2} + \mu^{+}_{k_3} < \mu^{-}_{k_1}$ and $\mu^{+}_{k_1} \le 1$. Note that these conditions are needed in the decoy-state method that is used for the parameter estimation (see Sec. IV in the Supplemental material for details).

(A-7) Assumption on the number of tagged signals. We define the *good* set $\mathcal{G}^{N_{\text{sent}}}_{\text{good}}$ of $\boldsymbol{g}^{N_{\text{sent}}}$ as that whose number of tagged events $n_{\text{tag}} := |\{i | g^i \notin \mathcal{G}^i_{\text{unt}}\}|$ is upper bounded by a constant number N_{tag} as

$$\mathcal{G}^{N_{\text{sent}}}_{\text{good}} := \left\{ \boldsymbol{g}^{N_{\text{sent}}} \middle| n_{\text{tag}} \le N_{\text{tag}} \right\}. \tag{12}$$

We suppose that the probability of $\boldsymbol{g}^{N_{\text{sent}}}$ not being an element of $\mathcal{G}^{N_{\text{sent}}}_{\text{good}}$ is upper bounded by p_{fail}, which is expressed as

$$\sum_{\boldsymbol{g}^{N_{\text{sent}}} \notin \mathcal{G}^{N_{\text{sent}}}_{\text{good}}} p(\boldsymbol{g}^{N_{\text{sent}}}) \le p_{\text{fail}}. \tag{13}$$

Assumptions on Bob's measurement unit

(B-1) Assumption on basis-independent detection efficiency. We denote by $\left\{\hat{M}_{y^i,b^i}\right\}_{y^i \in \{0,1,\emptyset\}}$ the i^{th} POVM (positive operator-valued measure) for Bob's measurement in the basis $b^i \in \mathcal{B} := \{Z, X\}$, where $\hat{M}_{0,b^i}$ $\left(\hat{M}_{1,b^i}\right)$ represents the POVM element associated to the detection of the bit value $y^i = 0$ (1) in the basis b^i, and the element $\hat{M}_{\emptyset,b^i}$ represents the failure of outputting a bit value. We suppose that whether a detection occurs or not for each pulse pair does not depend on the chosen measurement basis b^i; this condition is represented as

$$\hat{M}_{\emptyset} := \hat{M}_{\emptyset,Z} = \hat{M}_{\emptyset,X}. \tag{14}$$

(B-2) Assumption on the random choice of the measurement basis. We assume that Bob measures each incoming signal in a basis $b^i \in \mathcal{B}$ chosen independently of the previous basis choices and measurement outcomes. This condition is expressed in terms of the probability distribution as

$$p(b^i | \boldsymbol{b}^{i-1}, \boldsymbol{y}^{i-1}) = p(b^i). \tag{15}$$

(B-3) Assumption on no side-channels. We suppose that there are no side-channels in Bob's measurement device.

Let us remark that our security model allows the use of threshold detectors; this simply implies that Bob's Z and X basis measurements are not necessarily measurements on a qubit space. Note also that any error in the detection apparatus (say, for example, modulation errors) can be accommodated in our security proof as long as the assumptions stated in (B-1)-(B-3) are satisfied.

Protocol description

We describe the protocol of which we prove the security. See Fig. 3 for a typical setup of the actual protocol. In particular, we consider the loss-tolerant protocol in ref. [36]. Also, we suppose that Alice uses the decoy-state method[40–42] with one signal and two decoys, and we consider asymmetric coding, i.e., the Z and X bases are chosen with probabilities $p^A_Z := \sum_{c^i = 0_Z, 1_Z} p(c^i)$ and $p^A_X := p(c^i = 0_X)$, respectively. In addition, we assume that the secret key is generated from those events where both Alice and Bob select the Z basis regardless of their intensity settings.

Next, we show in detail how the protocol runs. In its description, $|A|$ represents the cardinality of a set or length of a bit string depending on whether A is a set or a bit string, respectively. The protocol is composed of the following steps:

(Step 0) Device characterisation and protocol parameter choice. First, Alice characterises her source to determine the value of the parameters R^{c}_{ph}, R^{k}_{int} for all $c \in \mathcal{C}$ and $k \in \mathcal{K}$, N_{tag} and p_{fail}. Also, Alice and Bob decide the secrecy parameter ε_s given by Eq. (19), the correctness parameter ε_c, the upper bound on N_{sent} which we shall denote by N, and the quantity N_{det} that is associated to the termination condition.

After this characterisation step, Alice (Bob) repeats the following step 1 (step 2) and both Alice and Bob repeat step 3 for $i = 1,\ldots,$ N_{sent} until the condition in the sifting step is met. Note that we adopt the iterative sifting procedure with a basis independent termination condition, which has been recently analysed in ref. [43]. In this procedure, after each quantum transmission round, Bob announces whether or not the received signal produced a detection click in his measurement apparatus. And, in the case of a detection click, both Alice and Bob announce their basis choices, and Bob also declares his measurement outcome except for the event where both of them selected the Z basis. Then, the quantum communication part of the protocol terminates when the basis independent termination condition is satisfied.

(Step 1) Preparation. For each i, Alice randomly selects the intensity setting $k^i \in \mathcal{K}$ with probabilities $p_{k_1} := p(k^i = k_1)$, $p_{k_2} := p(k^i = k_2)$ and $p_{k_3} := p(k^i = k_3)$, and the basis $a^i \in \mathcal{B}$ with probabilities p^A_Z and $p^A_X = 1 - p^A_Z$. Afterward, if $a^i = Z$ she chooses the bit information with probability 1/2; otherwise, she chooses $c^i = 0_X$. Finally, she generates the signal and reference pulses according to her choice of k^i and c^i, and sends them to Bob via a quantum channel.

(Step 2) Measurement. Bob measures the incoming signal and reference pulses using the measurement basis $b^i \in \mathcal{B}$, which he selects with probabilities $p^B_Z := p(b^i = Z)$ and $p^B_X := p(b^i = X)$. The outcome is recorded as $\{0, 1, \perp, \emptyset\}$, where $\perp$ and $\emptyset$ represent, respectively, a double click event, i.e., the two detectors click, and a no click event. If the outcome is $\perp$, Bob assigns a random bit to the event. Note that this random assignment is not mandatory. Indeed, Bob can always choose a particular bit value, say 0, for the double click events. This deterministic procedure also preserves the basis-independence detection efficiency condition described in Eq. (14). As a result, Bob obtains $y^i \in \{0, 1, \emptyset\}$. The outcomes 0 and 1 will be called a detection event.

(Step 3) Sifting. Bob declares over an authenticated public channel whether or not he obtained a detection event. If yes, Alice and Bob announce their basis choices, and Alice identifies if

the event can be assigned to the following sets for all $k \in \mathcal{K}$: $\mathcal{S}_{Z,Z,k,\mathrm{det}} := \{i|a^i = b^i = Z,\ k^i = k,\ y^i \neq \emptyset\}$. Moreover, if $a^i \neq Z$ or $b^i \neq Z$, Alice asks Bob to also announce his measurement outcome, and Alice identifies if the event can be assigned to the following sets for all $c \in \mathcal{C}$, $k \in \mathcal{K}$, $b \in \mathcal{B}$ and $y \in \{0, 1\}$: $\mathcal{S}_{c,k,\mathrm{det},y,b} := \{i|c^i = c, k^i = k, b^i = b, y^i = y\}$. Then, Alice checks if the following termination condition is satisfied for a prefixed N_{det}: $S_{\mathrm{det}} := |\mathcal{S}_{\mathrm{det}}| \geq N_{\mathrm{det}}$ for the set $\mathcal{S}_{\mathrm{det}} = \{i|y^i \neq \emptyset\}$. Once this termination condition is met after sending N_{sent} pulses, the results associated to the set $\mathcal{S}_{Z,Z,\mathrm{det}} := \cup_{k\in\mathcal{K}}\mathcal{S}_{Z,Z,k,\mathrm{det}}$ form Alice and Bob's sifted keys $\boldsymbol{\kappa}_A^{\mathrm{sift}}$ and $\boldsymbol{\kappa}_B^{\mathrm{sift}}$. That is, the length of these sifted keys is $|\boldsymbol{\kappa}_A^{\mathrm{sift}}| = |\boldsymbol{\kappa}_B^{\mathrm{sift}}| = |\mathcal{S}_{Z,Z,\mathrm{det}}|$. If the termination condition is not met after sending N pulses, then Alice and Bob abort the protocol.

(Step 4) Parameter estimation. Alice calculates a lower bound for the parameter $S_{Z,Z,n=1,u,\mathrm{det}} := |\mathcal{S}_{Z,Z,n=1,u,\mathrm{det}}|$, where $\mathcal{S}_{Z,Z,n,u,\mathrm{det}} := \{i|a^i = b^i = Z, n^i = n, t^i = u, y^i \neq \emptyset\}$ is a subset of $\mathcal{S}_{Z,Z,\mathrm{det}}$ composed of those elements where Alice emitted an untagged n-photon state. We call a lower bound on $S_{Z,Z,1,u,\mathrm{det}}$ as $S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$, which is given by Eq. (21). Also, she calculates an upper-bound $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ on the number of phase errors $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ for the set $\mathcal{S}_{Z,Z,1,u,\mathrm{det}}$, whose quantity is given by Eq. (24). If the upper bound $e^{\mathrm{U}}_{\mathrm{ph}|Z,Z,1,u,\mathrm{det}} := N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}/S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$ on the phase error rate $e_{\mathrm{ph}|Z,Z,1,u,\mathrm{det}} := N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}/S_{Z,Z,1,u,\mathrm{det}}$ satisfies $e^{\mathrm{U}}_{\mathrm{ph}|Z,Z,1,u,\mathrm{det}} \geq \overline{e^{\mathrm{U}}_{\mathrm{ph}|Z,Z,1,u,\mathrm{det}}}$, where $\overline{e^{\mathrm{U}}_{\mathrm{ph}|Z,Z,1,u,\mathrm{det}}}$ corresponds to the phase error rate associated with a zero secret key rate [see Eq. (20)], Alice and Bob abort the protocol. Otherwise, they proceed to step 5.

(Step 5) Bit error correction. Through public discussions, Bob corrects his sifted key $\boldsymbol{\kappa}_B^{\mathrm{sift}}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_A^{\mathrm{sift}}$ and obtains $\boldsymbol{\kappa}_B^{\mathrm{cor}}$ $\left(|\boldsymbol{\kappa}_B^{\mathrm{cor}}| = |\mathcal{S}_{Z,Z,\mathrm{det}}|\right)$.

(Step 6) Privacy amplification. Alice and Bob conduct privacy amplification by shortening $\boldsymbol{\kappa}_A^{\mathrm{sift}}$ and $\boldsymbol{\kappa}_B^{\mathrm{cor}}$ to obtain the final keys $\boldsymbol{\kappa}_A^{\mathrm{fin}}$ and $\boldsymbol{\kappa}_B^{\mathrm{fin}}$ of size $|\boldsymbol{\kappa}_A^{\mathrm{fin}}| = |\boldsymbol{\kappa}_B^{\mathrm{fin}}| = \ell$ with ℓ given by Eq. (20).

Secret key generation length

We present a formula to compute the secret key generation length ℓ that guarantees that the protocol introduced above is $\varepsilon_{\mathrm{sec}}$-secure. According to the universal composable security framework,[44,45] we say that a protocol is $\varepsilon_{\mathrm{sec}}$-secure if it is both ε_{c}-correct and ε_{s}-secret where $\varepsilon_{\mathrm{sec}} = \varepsilon_{\mathrm{c}} + \varepsilon_{\mathrm{s}}$.[46] We say that the protocol is ε_{c}-correct if $p(\boldsymbol{\kappa}_A^{\mathrm{fin}} \neq \boldsymbol{\kappa}_B^{\mathrm{fin}}) \leq \varepsilon_{\mathrm{c}}$ holds. Also, we say that the protocol is ε_{s}-secret if

$$\frac{1}{2}||\hat{\rho}^{\mathrm{fin}}_{AE} - \hat{\rho}^{\mathrm{ideal}}_{AE}|| \leq \varepsilon_{\mathrm{s}} \tag{16}$$

holds in terms of the trace norm, where $\hat{\rho}^{\mathrm{fin}}_{AE} = \sum_{\boldsymbol{\kappa}_A^{\mathrm{fin}}} p(\boldsymbol{\kappa}_A^{\mathrm{fin}})|\boldsymbol{\kappa}_A^{\mathrm{fin}}\rangle\langle\boldsymbol{\kappa}_A^{\mathrm{fin}}| \otimes \hat{\rho}_E(\boldsymbol{\kappa}_A^{\mathrm{fin}})$ is a classical-quantum state between Alice's final key and Eve's system after finishing the protocol and $\hat{\rho}^{\mathrm{ideal}}_{AE}$ is an ideal state in which Alice's key is uniformly distributed over $2^{|\boldsymbol{\kappa}_A^{\mathrm{fin}}|}$ values and decoupled from Eve's system. We suppose that the following two conditions for the random variables $S_{Z,Z,1,u,\mathrm{det}}$ and $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ are satisfied

$$p(S_{Z,Z,1,u,\mathrm{det}} < S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}|S_{\mathrm{det}} = N_{\mathrm{det}}) \leq \varepsilon_Z, \tag{17}$$

$$p(N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}} > N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}|n_{\mathrm{tag}} \leq N_{\mathrm{tag}}, S_{\mathrm{det}} = N_{\mathrm{det}}) \leq \varepsilon_{\mathrm{PH}} \tag{18}$$

regardless of Eve's attack. In this case, for any $\varepsilon_{\mathrm{PA}} > 0$, by setting[24,47]

$$\varepsilon_{\mathrm{s}} = \sqrt{2}\sqrt{\varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{PH}}} + \varepsilon_Z, \tag{19}$$

it can be shown that the protocol is ε_{c}-correct and ε_{s}-secret if the final key length ℓ satisfies

$$\ell \leq \ell_{\mathrm{SCIC}} := S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}\left[1 - h\left(\frac{N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}}{S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}}\right)\right] - \log_2\frac{2}{\varepsilon_{\mathrm{PA}}} - \lambda_{\mathrm{EC}}(\varepsilon_{\mathrm{c}}), \tag{20}$$

where $h(x)$ is the binary entropy function, and $\lambda_{\mathrm{EC}}(\varepsilon_{\mathrm{c}})$ is the cost of error correction to achieve ε_{c}-correctness. Note that the expressions of $S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$ and $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ are given in Eqs. (21) and (24), respectively.

Results of parameter estimation

Here, we summarise the estimation results of $S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$ and $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$. All the detailed derivations of these quantities can be found in Secs. IV and V in the Supplemental material, respectively.

First, regarding the estimation of $S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$, we employ the decoy-state method and we obtain the lower bound on $S_{Z,Z,1,u,\mathrm{det}}$ as

$$\begin{aligned} S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}} = {} & \frac{\mu_{k_1}^- \sum_{k\in\mathcal{K}} p_k \mu_k^- e^{-\mu_k^-}}{\left(\mu_{k_2}^+ - \mu_{k_3}^-\right)\left(\mu_{k_1}^- - \mu_{k_2}^+ - \mu_{k_3}^-\right)} \\ & \left\{ \frac{e^{\mu_{k_2}^-}\left[S^-_{Z,Z,k_2,u,\mathrm{det}} - g_{\mathrm{MA}}(\varepsilon_{\mathrm{MA}}^{Z,k_2,u}, p_Z^B, N_{\mathrm{det}})\right]}{p_{k_2}} \right. \\ & - \frac{e^{\mu_{k_3}^+}\left[S_{Z,Z,k_3,\mathrm{det}} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{Z,k_3,u}, p_Z^B, N_{\mathrm{det}}\right)\right]}{p_{k_3}} - \frac{\left(\mu_{k_2}^+\right)^2 - \left(\mu_{k_3}^-\right)^2}{\left(\mu_{k_1}^-\right)^2} \\ & \left. \left(\frac{e^{\mu_{k_1}^+}\left[S_{Z,Z,k_1,\mathrm{det}} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{Z,k_1,u}, p_Z^B, N_{\mathrm{det}}\right)\right]}{p_{k_1}}\right) \right\} + g_{\mathrm{MA}}(\varepsilon_{\mathrm{MA}}^{Z,1,u}, p_Z^B, N_{\mathrm{det}}) \end{aligned} \tag{21}$$

except for error probability

$$\varepsilon_Z := \sum_{k\in\mathcal{K}} \varepsilon_{\mathrm{MA}}^{Z,k,u} + \varepsilon_{\mathrm{MA}}^{Z,1,u} + p_{\mathrm{fail}} \tag{22}$$

for any $\varepsilon_{\mathrm{MA}}^{Z,k,u} > 0$ and $\varepsilon_{\mathrm{MA}}^{Z,1,u} > 0$. Here, we define $S^-_{Z,Z,k_2,u,\mathrm{det}} := S_{Z,Z,k_2,\mathrm{det}} - N_{\mathrm{tag}}$ and the statistical fluctuation term in the Modified Azuma's inequality (see Sec. III in the Supplemental material) is given by $g_{\mathrm{MA}}(\varepsilon, q, n) = \frac{\sqrt{\ln\varepsilon(\ln\varepsilon - 18nq)} - \ln\varepsilon}{3}$.

Second, we present the estimation result of the number of phase errors $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ for the untagged single-photon emission events in $\boldsymbol{\kappa}_A^{\mathrm{sift}}$. Before describing its expression, we first review briefly the main idea for deriving the number of phase errors. Our analysis is based on the security proofs[26,31,36] of the loss-tolerant protocol. These methods[26,31,36] require to estimate the number of single-photon detection events that Bob would have obtained if he had measured some virtual states in a basis (the X basis) complementary to the key generation basis (namely, the Z basis). Importantly, it turns out that the number of single-photon detection events can be written as a linear combination of those $\{S_{c,n=1,u,\mathrm{det},y,X}\}_{c\in\mathcal{C},y\in\{0,1\}}$, which will be defined soon, of the actual states sent by Alice. To obtain the numbers of these detection events, we use the detection events $\{\mathcal{S}_{c,k,\mathrm{det},y,b=X}\}_{c\in\mathcal{C},k\in\mathcal{K},y\in\{0,1\}}$ including basis mismatched events (i.e., the detection events where Alice and Bob's basis choices are different). By employing these observed number of detection events, we can estimate the number of single-photon detection events of the virtual states (and therefore the number of phase errors).

In the main text, for simplicity of its expression, we only describe $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ with the following restricted phase intervals (with $0 \leq \theta < \pi/6$):

$$R^{0_Z}_{\mathrm{ph}} = [-\theta, \theta], R^{1_Z}_{\mathrm{ph}} = [\pi - \theta, \pi + \theta], R^{0_X}_{\mathrm{ph}} = \left[\frac{\pi}{2} - \theta, \frac{\pi}{2} + \theta\right]. \tag{23}$$

Note that the expression of $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ with the general phase intervals in Eq. (10) should be referred to Sec. V B in the Supplemental material. Under the assumption of Eq. (23), $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ can be written as a linear combination of the parameters $S'_{c,1,u,\mathrm{det},y,X}$, which are bounds on the cardinality of the sets $\mathcal{S}_{c,1,u,\mathrm{det},y,X} = \left\{i | c^i = c, n^i = 1, t^i = u, b^i = X, y^i = y\right\}$, as

$$N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}} = \frac{p_Z^A p_Z^B (1+\sin\theta)}{2} \sum_{y=0}^{1} \sum_{c\in\mathcal{C}} \Gamma^{\mathrm{U}}_{y,c} \frac{S'_{c,1,u,\mathrm{det},y\oplus 1,X} + \mathrm{sgn}(\Gamma^{\mathrm{U}}_{y,c}) g_{\mathrm{A}}(N_{\mathrm{det}}, \varepsilon_{\mathrm{A}}^{c,1,u,y,X})}{p(c) p_X^B} + g_{\mathrm{A}}\left(N_{\mathrm{det}}, \varepsilon_{\mathrm{A}}^{\mathrm{ph},Z,1,u}\right). \tag{24}$$

Here, we define the statistical fluctuation term of the Azuma's inequality[48] as $g_{\mathrm{A}}(x,y) := \sqrt{2x \ln 1/y}$ and the functions $\{\Gamma^{\mathrm{U}}_{y,c}\}_{y,c}$[31] as $\Gamma^{\mathrm{U}}_{0,0_Z} = \frac{\sin\theta}{\sin\theta + \cos^2\frac{\theta}{2}}$ $(0 \le \Gamma^{\mathrm{U}}_{0,0_Z} < \sqrt{2}-1)$, $\Gamma^{\mathrm{U}}_{0,1_Z} = \Gamma^{\mathrm{U}}_{0,0_Z}$, $\Gamma^{\mathrm{U}}_{0,0_X} = \frac{1-\sin\theta}{\cos 2\theta - \sin\theta}$ $\left(1 \le \Gamma^{\mathrm{U}}_{0,0_X} < \infty\right)$, $\Gamma^{\mathrm{U}}_{1,0_Z} = \frac{\cos\theta}{\cos\theta - \sin^2\frac{\theta}{2}}$ $\left(1 \le \Gamma^{\mathrm{U}}_{1,0_Z} < 3+\sqrt{6}\right)$, $\Gamma^{\mathrm{U}}_{1,1_Z} = \Gamma^{\mathrm{U}}_{1,0_Z}$ and $\Gamma^{\mathrm{U}}_{1,0_X} = -\frac{1-\sin\theta}{1+\sin\theta}$ $(-1 \le \Gamma^{\mathrm{U}}_{1,0_X} < -1/3)$. Regarding $S'_{c,1,u,\mathrm{det},y,X}$, we take the following upper or lower bounds on $S_{c,1,u,\mathrm{det},y,X} := |\mathcal{S}_{c,1,u,\mathrm{det},y,X}|$, depending on the sign of $\Gamma^{\mathrm{U}}_{y,c}$, such that $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ takes its upper bound:

$$S'_{c,1,u,\mathrm{det},y,X} = \begin{cases} S^{\mathrm{U}}_{c,1,u,\mathrm{det},y,X} & \text{if} \quad \Gamma^{\mathrm{U}}_{y,c} > 0, \\ S^{\mathrm{L}}_{c,1,u,\mathrm{det},y,X} & \text{if} \quad \Gamma^{\mathrm{U}}_{y,c} \le 0, \end{cases} \tag{25}$$

with

$$S^{\mathrm{U}}_{c,1,u,\mathrm{det},y,X} := \frac{\frac{\left[S_{c,k_2,\mathrm{det},y,X} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,k_2,u,y,X}, p_X^B, N_{\mathrm{det}}\right)\right] e^{-\mu_{k_3}^-}}{p_{k_2}} - \frac{\left[S^-_{c,k_3,u,\mathrm{det},y,X} - g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,k_3,u,y,X}, p_X^B, N_{\mathrm{det}}\right)\right] e^{-\mu_{k_2}^+}}{p_{k_3}}}{e^{-\mu_{k_2}^-} - \mu_{k_3}^- \mu_{k_2}^- - e^{-\mu_{k_2}^+} - \mu_{k_3}^+ \mu_{k_3}^+} \times \sum_{k\in\mathcal{K}} p_k \mu_k^+ e^{-\mu_k^+} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,1,u,y,X}, p_X^B, N_{\mathrm{det}}\right) \tag{26}$$

and

$$S^{\mathrm{L}}_{c,1,u,\mathrm{det},y,X} := \frac{\mu_{k_1}^- \sum_{k\in\mathcal{K}} p_k \mu_k^- e^{-\mu_k^-}}{\left(\mu_{k_2}^- - \mu_{k_3}^-\right)\left(\mu_{k_1}^- - \mu_{k_2}^+ - \mu_{k_3}^-\right)} \left\{ \frac{e^{\mu_{k_2}^-}\left[S^-_{c,k_2,u,\mathrm{det},y,X} - g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,k_2,u,y,X}, p_X^B, N_{\mathrm{det}}\right)\right]}{p_{k_2}} - \frac{e^{\mu_{k_3}^-}\left[S_{c,k_3,\mathrm{det},y,X} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,k_3,u,y,X}, p_X^B, N_{\mathrm{det}}\right)\right]}{p_{k_3}} - \frac{\left(\mu_{k_2}^+\right)^2 - \left(\mu_{k_3}^-\right)^2}{\left(\mu_{k_1}^-\right)^2} \left(\frac{e^{\mu_{k_1}^-}\left[S_{c,k_1,\mathrm{det},y,X} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,k_1,u,y,X}, p_X^B, N_{\mathrm{det}}\right)\right]}{p_{k_1}} \right) \right\} + g_{\mathrm{MA}}\left(\varepsilon_{\mathrm{MA}}^{c,1,u,y,X}, p_X^B, N_{\mathrm{det}}\right), \tag{27}$$

where $S^-_{c,k,u,\mathrm{det},y,X} := S_{c,k,\mathrm{det},y,X} - N_{\mathrm{tag}}$. Finally, we calculate the failure probability $\varepsilon_{\mathrm{PH}}$ associated to the estimation of $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ in Eq. (18), as $\varepsilon_{\mathrm{PH}} = \varepsilon^1_{\mathrm{PH}} + \varepsilon^2_{\mathrm{PH}}$, and we define $\varepsilon^1_{\mathrm{PH}} := \sum_{y=0}^{1} \sum_{c\in\mathcal{C}} \varepsilon_{\mathrm{A}}^{c,1,u,y,X} + \varepsilon_{\mathrm{A}}^{\mathrm{ph},Z,1,u}$ for any $\varepsilon_{\mathrm{A}}^{c,1,u,y,X} > 0$ and $\varepsilon_{\mathrm{A}}^{\mathrm{ph},Z,1,u} > 0$. $\varepsilon^2_{\mathrm{PH}}$, on the other hand, is composed of the failure probabilities associated to the estimation of $\{S_{c,1,u,\mathrm{det},y,X}\}_{y\in\{0,1\},c\in\mathcal{C}}$, and $\varepsilon^2_{\mathrm{PH}}$ has the form $\varepsilon^2_{\mathrm{PH}} = \sum_{y=0,1} \sum_{c\in\mathcal{C}} \varepsilon^{c,1,u,y,X}$ with $\varepsilon^{c,1,u,y,X} = \sum_{k=k_2,k_3} \varepsilon_{\mathrm{MA}}^{c,k,u,y,X} + \varepsilon_{\mathrm{MA}}^{c,1,u,y,X}$ or $\varepsilon^{c,1,u,y,X} = \sum_{k\in\mathcal{C}} \varepsilon_{\mathrm{MA}}^{c,k,u,y,X} + \varepsilon_{\mathrm{MA}}^{c,1,u,y,X}$ depending on whether we use the upper bound given by Eq. (26) or the lower bound given by Eq. (27).

Simulation of the key rate

We show the numerical simulation results of the key rate for a fibre-based QKD system. In the simulation, we assume that Bob uses a measurement setup with two single-photon detectors with detection efficiency $\eta_{\mathrm{det}} = 10\%$ and dark count probability per pulse $p_{\mathrm{dark}} = 10^{-5}$. These parameters are set to be the same as those in ref. [49]. The attenuation coefficient of the optical fibre is 0.2 dB/km and its transmittance is $\eta_{\mathrm{ch}} = 10^{-0.2l/10}$ with l denoting the fibre length. We denote the channel transmission rate including detection efficiency by $\eta := \eta_{\mathrm{ch}}\eta_{\mathrm{det}}$. The overall misalignment error of the measurement system is fixed to be $e_{\mathrm{mis}} = 1\%$. In addition, we assume an error correction cost equals to $\lambda_{\mathrm{EC}}(\varepsilon_{\mathrm{c}}) = 1.05 \times |\boldsymbol{\kappa}_A^{\mathrm{sift}}| h(e_{\mathrm{bit}}) + \log_2(1/\varepsilon_{\mathrm{c}})$, where e_{bit} is the bit error rate of the sifted key $(\boldsymbol{\kappa}_A^{\mathrm{sift}}, \boldsymbol{\kappa}_B^{\mathrm{sift}})$. Moreover, we suppose that the intervals of the intensity fluctuation in Eq. (11) are given by $R^k_{\mathrm{int}} = [\mu_k(1-r_k), \mu_k(1+r_k)]$ for $k \in \{k_1, k_2\}$ and $R^{k_3}_{\mathrm{int}} = [0, 10^{-3}]$ with μ_k denoting the expected intensity (we suppose that $\mu_{k_3} = 0$) and where r_k represents the deviation of the actual intensity from the expected value. For the intervals of the phase fluctuation R^i_{ph} in Eq. (23), we take the experimental value of phase modulation error from ref. [32] and we set $\theta = 0.03$ rad. Note that the phase fluctuation ±0.03 rad is the largest experimental value observed in ref. [32] in a protocol that uses the three states $\{0, \pi/2, 3\pi/2\}$ (see table III in ref. [32]). Note also that the authors of ref. [32] measured a different quantity from the one we need here. More precisely, ref. [32] assumes that each sending pulse is IID and measured the fixed deviation due to imperfect encoding. In contrast, we allow each pulse to be different (non-IID case) and we are interested in the deviation of each pulse from the mean. In our simulation, we simply assume that the result in ref. [32] gives us some reasonable estimation on the deviation θ. In Fig. 4, we consider the three cases: (I) $N_{\mathrm{tag}} = 0$ and $p_{\mathrm{fail}} = 0$, (II) $N_{\mathrm{tag}} = N_{\mathrm{sent}} \times 10^{-7}$ in the upper

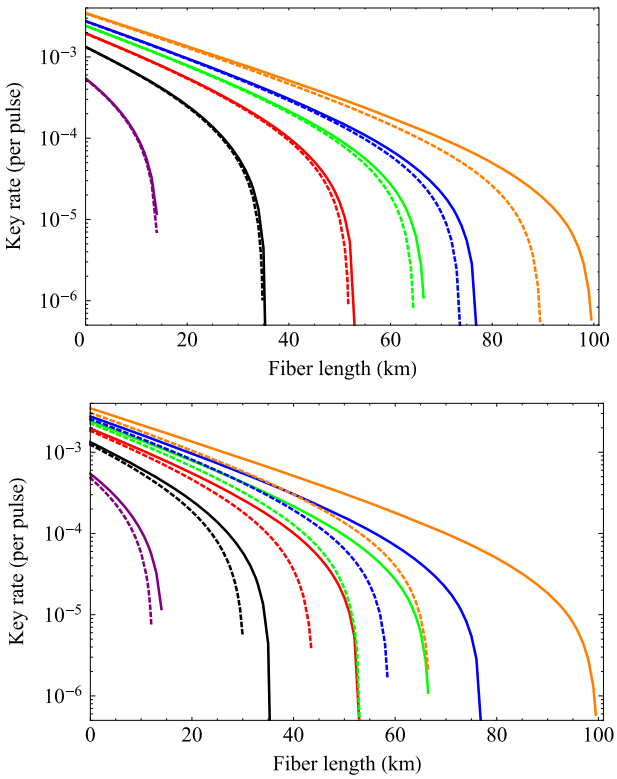

Fig. 4 The key rate (per pulse) in logarithmic scale versus fibre length for the case with the phase fluctuation of ±0.03 rad [namely, $\theta = 0.03$ in Eq. (23)] for any choice of $c^i \in \mathcal{C}$ and the intensity fluctuation of ±3% for the choice of $k^i \in \{k_1, k_2\}$ and $R^{k_3}_{\mathrm{int}} = [0, 10^{-3}]$ for the weakest decoy setting $k^i = k_3$. In solid lines, we assume (I) $N_{\mathrm{tag}} = 0$ and $p_{\mathrm{fail}} = 0$, and in the dashed lines, we assume (II) $N_{\mathrm{tag}} = N_{\mathrm{sent}} \times 10^{-7}$ in the upper figure and (III) $N_{\mathrm{tag}} = N_{\mathrm{sent}} \times 10^{-6}$ in the lower figure and $p_{\mathrm{fail}} = 0$. The secrecy and correctness parameters are $\varepsilon_{\mathrm{s}} = \varepsilon_{\mathrm{c}} = 10^{-10}$ and for each set of solid and dashed lines, the total number of signals sent by Alice is $N_{\mathrm{sent}} \in \{10^{10}, 10^{10.5}, 10^{11}, 10^{11.5}, 10^{12}\}$ from left to right. The rightmost solid and dashed lines respectively correspond to the asymptotic key rate of the cases (I)-(III) where no statistical flucuation terms in $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ and $S^{\mathrm{L}}_{Z,Z,1,u,\mathrm{det}}$ are taken into account. The experimental parameters are described in the main text

figure and (III) $N_{\rm tag} = N_{\rm sent} \times 10^{-6}$ in the lower figure and $p_{\rm fail} = 0$. The case (I) means that all the phases and the intensities lie in their intervals, and the case (II) [the case (III)] means that the number of tagged events is upper bounded by $N_{\rm sent} \times 10^{-7}$ in the upper figure [$N_{\rm tag} = N_{\rm sent} \times 10^{-6}$ in the lower figure].

Regarding the numbers of detection events $S_{Z,Z,k,\rm det}$ and $S_{c,k,\rm det,y,b}$, we generate these quantities by assuming the following specific setup. In particular, for the $i^{\rm th}$ trial, we consider that Alice sends Bob pairs of coherent states through the fibre of the form $\left|e^{{\rm i}(\delta+\theta_c)}\sqrt{\mu_k/2}\right\rangle_{S^i}\left|e^{{\rm i}\delta}\sqrt{\mu_k/2}\right\rangle_{R^i}$ with $\theta_{0_Z} = 0$, $\theta_{1_Z} = \pi$ and $\theta_{0_X} = \pi/2$ according to the choices of $k^i = k \in \mathcal{K}$ and $c^i = c \in \mathcal{C}$. Note that this assumption is used just to simulate the experimentally observed numbers (namely, $S_{Z,Z,k,\rm det}$ and $S_{c,k,\rm det,y,b}$), and we do not require this assumption in the actual experiments. Bob measures the incoming signals using a Mach-Zehnder interferometer with two 50:50 BSs and a phase modulator as shown in Fig. 3. More precisely, he uses the first 50:50 BS to split the received pulses into two beams, and after that he applies a phase shift 0 or $\pi/2$ to one of them according to his basis choice of $b^i = Z$ or $b^i = X$, respectively, and finally he lets the resulting pulses interfere with the second 50:50 BS. In this setup, we obtain the following probabilities:

$$p(y^i = y|c^i = y_Z, k^i = k, b^i = Z) = p(y^i = 0|c^i = 0_X, k^i = k, b^i = X)$$
$$= \left[1 - e^{-\frac{\eta\mu_k}{2}}(1 - p_d)\right]\left(1 - \tfrac{p_d}{2}\right), \quad p(y^i = y \oplus 1|c^i = y_Z, k^i = k, b^i = Z) = p(y^i = 1|c^i = 0_X, k^i = k, b^i = X) = \frac{p_d\left[1 + e^{-\frac{\eta\mu_k}{2}}(1-p_d)\right]}{2}$$

for $y \in \{0,1\}$, and $p(y^i = y|c^i = x_Z, k^i = k, b^i = X) = p(y^i = y|c^i = 0_X, k^i = k, b^i = Z) = \frac{1-(1-p_d)^2 e^{-\frac{\eta\mu_k}{2}}}{2}$ for $y, x \in \{0,1\}$. Moreover, we assume that the bit error rate $e_{\rm bit}$ is given by $e_{\rm bit} = \sum_{y=0,1} p(y^i = y \oplus 1|c^i = y_Z, k^i = k_1, b^i = Z) / \sum_{x,y=0,1} p(y^i = y|c^i = x_Z, k^i = k_1, b^i = Z) + e_{\rm mis}$. With these probabilities, we suppose that the experimentally observed numbers satisfy $S_{Z,Z,k,\rm det} = N_{\rm sent} \sum_{x,y=0,1} \frac{p_Z^A}{2} p_Z^B p_k \times p(y^i = y|c^i = x_Z, k^i = k, b^i = Z)$ and $S_{c,k,\rm det,y,b} = N_{\rm sent} p(c) p_b^B p_k \times p(y^i = y|c^i = c, k^i = k, b^i = b)$.

With the above parameters, we simulate the key rate $\ell_{\rm SCIC}/N_{\rm sent}$ for a fixed value of the correctness and secrecy parameters $\varepsilon_{\rm c} = \varepsilon_{\rm s} = 10^{-10}$ and we set $\varepsilon_Z = 1/2 \times 10^{-10}$, $\varepsilon_{\rm PA} = \varepsilon_{\rm PH} = 1/16 \times 10^{-20}$, and $\varepsilon_{\rm MA}^{Z,k,u} = \varepsilon_{\rm MA}^{Z,1,u} = \varepsilon_Z/4 = 1/8 \times 10^{-10}$. We also assume that each failure probability which is contained in the expression of $\varepsilon_{\rm PH}^1$ and $\varepsilon_{\rm PH}^2$ takes the value $\varepsilon_{\rm A}^{c,1,u,y,X} = \varepsilon_{\rm A}^{{\rm ph},Z,1,u} = 1/26 \times \varepsilon_{\rm PH}$ and $\varepsilon_{\rm MA}^{c,k,u,y,X} = \varepsilon_{\rm MA}^{c,1,u,y,X} = 1/26 \times \varepsilon_{\rm PH}$, respectively, and we set $p_Z^A = p_Z^B = p_{k_1} = 0.8$ and $p_{k_2} = 0.1$. In the simulation, we perform a numerical optimisation of the key rate $\ell_{\rm SCIC}/N_{\rm sent}$ over the two free parameters μ_{k_1} and μ_{k_2}. In the solid and dashed lines in Fig. 4, we respectively plot the key rate of the cases (I), (II) and (III) for the finite-case when $N_{\rm sent} \in \{10^{10}, 10^{10.5}, 10^{11}, 10^{11.5}, 10^{12}\}$ (from left to right). For comparison, the rightmost solid and dashed lines respectively correspond to the asymptotic key rate of the cases (I), (II) and (III), where no statistical fluctuation terms in Eqs. (21) and (24) are taken into account. Our simulation results show the feasibility of secure key distribution within a reasonable time by employing practical devices that satisfy our device assumptions. For instance, if Alice uses a laser diode operating at 1 GHz repetition rate and she sends $N_{\rm sent} = 10^{12}$ signals, then we find that it is possible to distribute a 1-Mb secret key over a 75-km fibre link in <0.3 h. This scenario corresponds to the solid blue line (the fifth solid line from the left) shown in Fig. 4.

DISCUSSION

In summary, we have provided an information-theoretic security proof for the loss-tolerant QKD protocol which accommodates the setting-choice-independent correlation (SCIC) in the finite key regime. Within the framework of SCIC, the relative phases and intensities of the sending coherent states fluctuate over time. Once realistic intervals for these fluctuations (such as for instance ±0.03 rad and ±3%, respectively) are guaranteed, our numerical simulations have shown that secure quantum communication is feasible with a reasonable number of signal transmissions such as for example $N_{\rm sent} = 10^{12}$. Therefore, our results constitute a significant step towards realising secure quantum communication with practical source devices. On a more general outlook, we leave three open questions for the future works.

1. It is an important future work to devise a rigorous experimental method for characterising the source parameters described in Eqs. (10)–(13). Once such a method is established, characterisations could be conducted on-line or it would be repeated many times off-line in which we assume that the property of the source parameters is unchanged after the characterisation.
2. Another important future work is to prove the security of MDI-QKD based on our source model of the SCIC framework. The original proposal of the loss-tolerant protocol[36] can also be applied to MDI-QKD, and the analysis presented in this paper is an extension of the proof of ref. [36]. Therefore, it should be straightforward to apply our proof to MDI-QKD.
3. In our analysis, in order to take into account setting-choice-independent correlations, we use the Azuma's inequality. One possibility to improve the key rate would be to employ the improved decoy state analysis developed in ref. [50], which is known to result in a higher key rate than all the existing analyses for the decoy state. However, the analysis in ref. [50] assumes that there are no correlations among sending pulses, which is a striking difference from our source model, and it is not clear whether we can apply their analysis to our source.

DATA AVAILABILITY

No datasets were generated or analysed during the current study.

ACKNOWLEDGEMENTS

We thank Masato Koashi, Toshihiko Sasaki and Tatsuya Sumiya for crucial comments on the correlation model of the source devices, and Yuki Takeuchi for valuable discussions on the security analysis. A.M. acknowledges support from Grant-in-Aid for JSPS Fellows (KAKENHI Grant No. JP17J04177). G.K., K.A., and K.T. acknowledge support from ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan). K.T. acknowledges support from MEXT/JSPS KAKENHI Grant Number JP18H05237. M.C. acknowledges support from the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2014-54898-R, and the European Commission (project "QCALL"). N.I. acknowledges support from JST-CREST JPMJCR1671. H.K.L. acknowledges financial support from the Natural Sciences and Engineering Research Council of Canada (NSERC), the US Office of Naval Research (ONR), Canadian Foundation for Innovation (CFI), Ontario Research Fund (ORF) and Post-secondary Strategic Infrastructure Fund (SIF).

AUTHOR CONTRIBUTIONS

A.M., G.K., K.A., and K.T. constructed the framework of SCIC and performed the security analysis. Then, all the authors contributed to checking the validity of the framework and writing of the paper.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-018-0122-y).

Competing interests: The authors declare no competing interests.

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

REFERENCES

1. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595 (2014).
2. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 16025 (2016).
3. Sajeed, S. et al. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **91**, 032326 (2015).
4. Sun, S.-H. et al. Effect of source tampering in the security of quantum cryptography. *Phys. Rev. A* **92**, 022304 (2015).
5. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
6. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7**, 073 (2007).
7. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15**, 9388 (2007).
8. Makarov, V., Anisimov, A. & Skaar, J. Erratum: Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **78**, 019905 (2008).
9. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
10. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686 (2010).
11. Gerhardt, I. et al. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 349 (2011).
12. Weier, H. et al. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13**, 073024 (2011).
13. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proc. 39th Annual Symposium on Foundations of Computer Science*, 1998, 503–509 (IEEE, 1998).
14. Acín, A. et al. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
15. Vazirani, U. & Vidick, T. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **113**, 140501 (2014).
16. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **9**, 459 (2018).
17. Barrett, J., Colbeck, R. & Kent, A. Memory Attacks on Device-Independent Quantum Cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).
18. Curty, M. & Lo, H.-K. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *arXiv* **1711**, 08724 (2017).
19. Lo, H.-K., Curty, M. & Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
20. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
21. 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).
22. Tomamichel, M. & Leverrier, A. A largely self-contained and complete security proof for quantum key distribution. *Quantum* **1**, 14 (2017).
23. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
24. Hayashi, M. & Nakayama, R. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths. *New J. Phys.* **16**, 063009 (2014).
25. Curty, M., Xu, F., Cui, W., Lim, C. C. W., Tamaki, K. & Lo, H.-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).
26. Mizutani, A., Curty, M., Lim, C. C. W., Imoto, N. & Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **17**, 093011 (2015).
27. Yoshino, K. et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf.* **4**, 8 (2018).
28. Ding, Y. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **3**, 25 (2017).
29. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172 (2017).
30. Ma, C. et al. Integrated optics; Photonic integrated circuits; Quantum cryptography. *Optica* **3**, 1274 (2016).
31. Nagamatsu, Y. et al. Security of quantum key distribution with light sources that are not independently and identically distributed. *Phys. Rev. A* **93**, 042325 (2016).
32. Xu, F. et al. Experimental quantum key distribution with source flaws. *Phys. Rev. A* **92**, 032305 (2015).
33. Tang, Z., Wei, K., Bedroya, O., Qian, L. & Lo, H.-K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **93**, 042308 (2016).
34. Wang, X.-B., Peng, C.-Z., Zhang, J., Yang, L. & Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **77**, 042311 (2008).
35. Hayashi, M. Optimal decoy intensity for decoy quantum key distribution. *J. Phys. A Math. Theor.* **49**, 165301 (2016).
36. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90**, 052314 (2014).
37. Bennett, C. H. & Brassard, G. Quantum cryptography: public-key distribution and coin tossing. In *Proc. IEEE Int. Conference on Computers, Systems, and Signal Processing*, 175–179 (IEEE, NY, Bangalore, India, 1984).
38. Grünenfelder, F., Boaron, A., Rusca, D., Martin, A. & Zbinden, H. Simple and high-speed polarization-based QKD. *Appl. Phys. Lett.* **112**, 051108 (2018).
39. Boaron, A. et al. Simple 2.5 GHz time-bin quantum key distribution. *Appl. Phys. Lett.* **112**, 171108 (2018).
40. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
41. Lo, H.-K., Ma, X. & Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
42. Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
43. Tamaki, K. et al. Security of quantum key distribution with iterative sifting. *Quantum Sci. Technol.* **3**, 014002 (2017).
44. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. The universal composable security of quantum key distribution. *Theory of Cryptography* **3378**, 386–406 (2005).
45. Renner, R. & König, R. Universally composable privacy amplification against quantum adversaries, Springer. *Theory of Cryptography*. **3378**, 407–425 (2005).
46. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **11**, 045018 (2009).
47. Kawakami, S. Security of Quantum Key Distribution with Weak Coherent Pulses. *Ph.D. thesis, The University of Tokyo* (2017).
48. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J.* **19**, 357 (1967).
49. Kawakami, S., Sasaki, T. & Koashi, M. Finite-key analysis for quantum key distribution with weak coherent pulses based on Bernoulli sampling. *Phys. Rev. A* **96**, 012305 (2017).
50. Zhang, Z., Zhao, Q., Razavi, M. & Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **95**, 012333 (2017).