PAPER • OPEN ACCESS

Discrete-phase-randomized coherent state source and its application in quantum key distribution

To cite this article: Zhu Cao *et al* 2015 *New J. Phys.* **17** 053014

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
4 December 2014

REVISED
11 April 2015

ACCEPTED FOR PUBLICATION
13 April 2015

PUBLISHED
13 May 2015

PAPER

Discrete-phase-randomized coherent state source and its application in quantum key distribution

Zhu Cao[1], **Zhen Zhang**[1], **Hoi-Kwong Lo**[2] **and Xiongfeng Ma**[1]

[1] Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, People's Republic of China

[2] Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada

E-mail: xma@tsinghua.edu.cn

Keywords: quantum key distribution, coherent state, discrete phase randomization, decoy state

Abstract

Coherent state photon sources are widely used in quantum information processing. In many applications, such as quantum key distribution (QKD), a coherent state functions as a mixture of Fock states by assuming that its phase is continuously randomized. In practice, such a crucial assumption is often not satisfied, and therefore the security of existing QKD experiments is not guaranteed. To bridge this gap, we provide a rigorous security proof of QKD with discrete-phase-randomized coherent state sources. Our results show that the performance of the discrete-phase randomization case is close to its continuous counterpart with only a small number (say, 10) of discrete phases. Compared to the conventional continuous phase randomization case, where an infinite amount of random bits are required, our result shows that only a small amount (say, 4 bits) of randomness is needed.

1. Introduction

In many quantum optics applications, such as quantum key distribution (QKD) [1, 2], linear optics quantum computing [3], bit commitment [4], coin flipping [5], and blind quantum computing [6], a perfect single-photon source is assumed to be used, which is not feasible with current technology. Instead, a weak laser is widely used to replace the single-photon source in practice. A laser can be well described by a coherent state [7],

$$|\alpha\rangle = \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{1.1}$$

on which a phase modulation by $\theta \in [0, 2\pi)$ implements the operation $|\alpha\rangle$ to $|\alpha \mathrm{e}^{\mathrm{i}\theta}\rangle$. For a coherent state, there is a nonzero probability of getting components other than single-photons, such as vacuum states and multiphoton states. To model this imperfection, a photon number channel model is used [8], which assumes that the phase of the coherent state is randomized,

$$\frac{1}{2\pi} \int_0^{2\pi} |\alpha \mathrm{e}^{\mathrm{i}\theta}\rangle\langle \alpha \mathrm{e}^{\mathrm{i}\theta}| \, d\theta = \sum_{n=0}^{\infty} \mathrm{e}^{-|\alpha|^2} \frac{|\alpha|^2}{n!} |n\rangle\langle n|. \tag{1.2}$$

A physical interpretation behind equation (1.2) is that when the phase of a coherent state is randomized, it is equivalent to a mixed state of Fock states whose photon number follows a Poisson distribution with a mean of $|\alpha|^2$. In other words, the Fock states are totally decohered from each other with continuous phase randomization.

We remark that phase randomization as specified in equation (1.2) is a common assumption in the theoretical models of many quantum information processing protocols. In practice, as will be discussed later in this paper, the assumption of continuous phase randomization is often not satisfied in experiments. Therefore, the security of a protocol (e.g., the security of a generated key in QKD) is *not* guaranteed.

To illustrate the problem, for simplicity, let us consider the example of QKD. The first QKD protocol was published in 1984 by Bennett and Brassard (BB84) [1]. Lots of progress has been made since then, both theoretically and experimentally [9]. For the BB84 protocol, secure key bits can be transmitted only when single-photon states are used. From the study of photon-number-splitting attacks [10], one can see that multiphoton components are not secure for the BB84 protocol. The key idea in taking this imperfection into consideration is in performing privacy amplification on key bits from good (single-photon) states and bad (multiphoton) states separately [11]. Meanwhile, to accurately quantify the amounts of key bits from good and bad states, the decoy-state method has been proposed [8, 12, 13] and experimentally demonstrated [14–18].

For all the existing security analysis for coherent-state QKD protocols, including a recent QKD protocol [19], continuous phase randomization, equation (1.2), is assumed. It has been shown that when the phase is not randomized, the performance will be substantially reduced with a strict security proof [20]. In fact, there are experimental quantum hacking demonstrations showing that a QKD system may be attacked when the phase is not randomized [21, 22].

There are two means to randomize the phase in practice: passive and active. In a passive phase randomization process, the laser is turned on and off to generate pulses. One might be tempted to make a naive argument that by switching a laser on and off, the phase is fully randomized. Note that it is experimentally challenging to rigorously verify that a *continuous* phase is indeed *fully* random. Moreover, experiments in random-number generation have shown that there are indeed residue correlations between the phases of adjacent pulses [23], especially in the case of high-speed applications [24], which directly rejects the claim since fully randomized phases have no correlations. Thus we avoid this approach here.

In the active phase randomization process, a phase modulator is used to randomly modulate the phases. In this case, the modulator can only perform discrete phase randomization, unless it uses an infinite amount of random numbers. In a recent experiment [25] with coherent states, each global phase was chosen from one of the over 1000 possible values. First, such a large number of phases demands high precision control, which is a challenge for practical implementations. Second, even with 1000 phases, the phase is still discrete and the key rate may be deviated from the continuous-randomization case. So far, *no* rigorous bound on the key rate was derived in this experiment [25] or in any other QKD experimental papers. Since the work of Lo and Preskill was published [20], it has been a long-standing question to analyze the security of a practical QKD system with discrete-phase randomization and rectify the highly unsatisfactory situation that there is no proof of security in existing experiments.

In this work, we solve this long-standing open question by providing a rigorous security proof of QKD systems using discrete-phase-randomized coherent states. Here, we consider unconditional security, following the standard security proof [11]. That is to say, security against the most general type of attacks allowed by quantum mechanics on the quantum channel by an eavesdropper. We show that as the number of discrete phases increases, coherence between the Fock states in equation (1.1) decreases exponentially fast. As an application, we provide tight security bounds for both nondecoy- and decoy- state QKD protocols with discrete phase randomization. Our result applies to various encoding schemes of QKD, including time-bin, phase encoding, and polarization encoding.

In simulation, we compare the performance of our security bounds with the one provided by continuous phase randomization, which shows that our security bounds are tight when the number of phases goes to infinity. From a practical point of view, for a small number of phases (say, only $N = 10$ phases), with a typical set of experimental parameters, we observe that secret keys can be securely distributed over a fiber length of up to 138 km, close to 140 km in the continuous phase randomized case. Thus Alice needs less than 4 bits ($2^4 > 10$) of random numbers per pulse for phase randomization. In contrast, all previous security proofs essentially assume an infinite number of bits of random numbers per pulse. Therefore, we are making an improvement here. Moreover, our scheme is simple to implement. For instance, an implementation of active phase randomization with 1000 discrete phases has been reported in the literature [25]. Due to the massive reduction in the number of phases in our scheme (10 phases), one can expect a simpler implementation with a much higher repetition rate. In addition to QKD protocols, our analysis of discrete phase randomization is also readily applicable to linear optics quantum computation [3] and other quantum cryptographic primitives [5], because phase-randomized coherent sources also serve as major parts of those fields.

2. Results

The roadmap of this section is as follows. In section 2.1, we use the Schmidt decomposition to construct states that are close to Fock states from discrete-phase-randomized coherent states. In section 2.2, we present the phase encoding scheme when discrete-phase-randomized coherent states are used, and we investigate how close the approximated Fock states are. In section 2.3, we give a security proof and derive a key rate formula for a QKD

system with discrete-phase randomization. In section 2.4, we present the simulation results for two cases: with and without the decoy-state method.

2.1. Coherent state mixture

Here, we consider a coherent state source whose phase is randomly picked from N different values (i.e., each with probability $1/N$). For the sake of simplicity, we assume these N values are evenly distributed in $[0,\ 2\pi)$,

$$\left\{\theta_k = \frac{2\pi k}{N}\ |k = 0,\ 1,\ldots, N-1\right\}. \tag{2.1}$$

In the case of continuous phase randomization (when $N \to \infty$), equation (1.2) essentially shows that one can decompose the phase-randomized coherent mixed state into a statistical mixture of Fock states, $|n\rangle\langle n|$. In the application of QKD, as well as quantum computing [3], the single-photon state, $|1\rangle\langle 1|$, is the most important component.

In the case of a finite N, one can decompose the mixed state to a set of pure states in the hopes that one of them is close to a single-photon state. First, let us consider the case $N = 2$. We start with the initial state

$$|\Psi_2\rangle = |0\rangle_A|\sqrt{2}\,\alpha\rangle_B + |1\rangle_A|-\sqrt{2}\,\alpha\rangle_B, \tag{2.2}$$

where the phase of coherent state, $|\sqrt{2}\,\alpha\rangle_B$, is controlled by a quantum coin, A. The factor $\sqrt{2}$ is included in the state for system B to simplify later discussions. The normalization factor is ignored throughout the paper unless it matters. By performing a Schmidt decomposition

$$|\Psi_2\rangle = \left(|0\rangle_A + |1\rangle_A\right)|\lambda_0\rangle_B + \left(|0\rangle_A - |1\rangle_A\right)|\lambda_1\rangle_B, \tag{2.3}$$

where the two pure states are given by

$$\begin{aligned} |\lambda_0\rangle &= |\sqrt{2}\,\alpha\rangle + |-\sqrt{2}\,\alpha\rangle, \\ |\lambda_1\rangle &= |\sqrt{2}\,\alpha\rangle - |-\sqrt{2}\,\alpha\rangle. \end{aligned} \tag{2.4}$$

By substituting the definition of a coherent state, equation (1.1), it is not hard to see that $|\lambda_0\rangle$ ($|\lambda_1\rangle$) is a superposition of even (odd) photon number Fock states. By this decomposition, the Hilbert space is divided into the even and odd number Fock state spaces, $H_{\text{even}} \oplus H_{\text{odd}}$. Since $|\lambda_1\rangle$ only contains odd photon number Fock states, we expect that it is close to a single-photon state, which can be confirmed from the calculation of fidelity later.

In the case of general $N \geqslant 1$, the decomposition is similar but a bit more complex,

$$\begin{aligned} |\Psi_N\rangle &= \sum_{k=0}^{N-1} |k\rangle_A \left|\sqrt{2}\,\alpha e^{2k\pi i/N}\right\rangle_B \\ &= \sum_{j=0}^{N-1} |j\rangle_A \left|\lambda_j\right\rangle_B \end{aligned} \tag{2.5}$$

where $|j\rangle_A$ can be understood as a quantum coin with N random outputs, and the N pure states are given by

$$\left|\lambda_j\right\rangle = \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\sqrt{2}\,\alpha\right\rangle. \tag{2.6}$$

By substituting equation (1.1), we have the following observations for $|\lambda_j\rangle$. It is a superposition of Fock states whose photon numbers, modulo N, are the same j,

$$\left|\lambda_j\right\rangle = \sum_{l=0}^{\infty} \frac{\left(\sqrt{2}\,\alpha\right)^{lN+j}}{\sqrt{(lN+j)!}}\ |lN+j\rangle. \tag{2.7}$$

Then, it is not hard to see that $|\lambda_j\rangle$ becomes close to a Fock state when N is large, since $\sqrt{(lN+j)!}$ increases quickly. When $N \to \infty$, it becomes a Fock state, $|\lambda_j\rangle = |j\rangle$. Later in the simulation, one can see that when $N = 10$, the mixed coherent state becomes close to a Fock state mixture in terms of the performance of the QKD. Similar to the case of $N = 2$, the Hilbert space is divided into $H_{0 \bmod N} \oplus H_{1 \bmod N} \oplus \ldots \oplus H_{(N-1) \bmod N}$.

Next, we can figure out the probability if Alice performs a projection measurement on the photon state in the basis of $|\lambda_j\rangle$, which is simply the norm of equation (2.7),

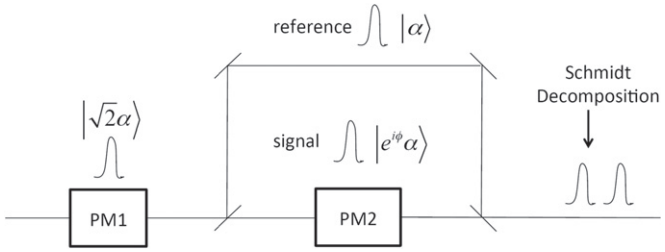

Figure 1. Schematic diagram for the phase-encoding QKD scheme with coherent states. The first phase modulator, *PM*1, is used for phase randomization according to equation (2.1), and the second one, *PM*2, is used for QKD encoding, $\phi \in \{0, \pi/2, \pi, 3\pi/2\}$.

$$P_j = \frac{\langle \lambda_j | \lambda_j \rangle}{\sum_{j=0}^{N-1} \langle \lambda_j | \lambda_j \rangle} = \sum_{l=0}^{\infty} \frac{\mu^{lN+j} e^{-\mu}}{(lN+j)!}, \tag{2.8}$$

where $\mu = 2\,|\alpha|^2$. When $N \to \infty$, it becomes a photon number channel and follows a Poisson distribution, $\mu^j e^{-\mu}/j!$.

2.2. Coherent state scheme

A typical scheme using a coherent state source (e.g., a phase-encoding QKD scheme), is shown in figure 1, which is essentially an interferometer. In the state-preparation stage, Alice prepares a weak coherent state $|\sqrt{2}\,\alpha\rangle$, whose phase is modulated randomly by the first phase modulator, *PM*1. The state is separated into two pulses, $|\alpha\rangle_r$ and $|\alpha\rangle_s$, by a beam splitter. Then Alice encodes the bit and basis information (say, according to the BB84 protocol) in the relative phase via the second phase modulator, *PM*2.

Here, for simplicity, we consider the case that the reference pulse has the same intensity as the signal. Our results can be extended to the strong reference case [26, 27] and the asymmetric case [28], as well as to other encoding schemes such as polarization encoding and time-bin encoding [29].

In the scheme with discrete *N*-phase randomization, the photon source is decomposed into states $|\lambda_j\rangle$, as shown in equation (2.6). After going through the phase encoding scheme as shown in figure 1, the four BB84 states encoded in $|\lambda_j\rangle$ can be written as

$$\begin{aligned}
|0_x^L\rangle &= \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|e^{2k\pi i/N}\alpha\right\rangle \\
|1_x^L\rangle &= \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|-e^{2k\pi i/N}\alpha\right\rangle \\
\left|0_y^L\right\rangle &= \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|ie^{2k\pi i/N}\alpha\right\rangle \\
\left|1_y^L\right\rangle &= \sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|-ie^{2k\pi i/N}\alpha\right\rangle,
\end{aligned} \tag{2.9}$$

where we omit the subscript *j* on the left side, but it should be understood that the four states do depend on *j*.

The key point to guarantee the security of the BB84 protocol is that Eve cannot distinguish the state in two conjugate bases, *X* and *Y*. The two density matrices in the two bases can be written as

$$\begin{aligned}
\rho_x &= |0_x^L\rangle\langle 0_x^L| + |1_x^L\rangle\langle 1_x^L| \\
\rho_y &= \left|0_y^L\right\rangle\left\langle 0_y^L\right| + \left|1_y^L\right\rangle\left\langle 1_y^L\right|.
\end{aligned} \tag{2.10}$$

Note that each logical state should be regarded as a pure normalized state. In the ideal case, where a basis-independent source, such as a single-photon source, is used, the density matrices in the two bases should be the same,

$$\rho_x = \rho_y. \tag{2.11}$$

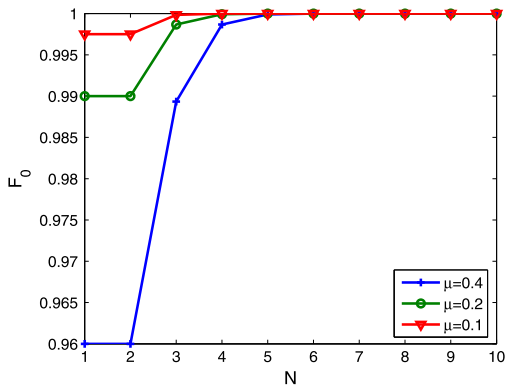

Figure 2. Plots of fidelity for different values of mean photon number μ. The fidelity here refers to F_0, which is always smaller than F_1 by the numerical evaluation.

In the security analysis, one of the key parameters is the basis dependence of the source, which is the fidelity between the two states in the X and Y bases,

$$F_j\left(\rho_x, \rho_y\right) = \mathrm{tr}\sqrt{\sqrt{\rho_y}\rho_x\sqrt{\rho_y}} \geqslant \left|\frac{\sum_{l=0}^{\infty}\frac{\mu^{lN+j}}{(lN+j)!}2^{-\frac{lN+j}{2}}\left(\cos\frac{lN+j}{4}\pi+\sin\frac{lN+j}{4}\pi\right)}{\sum_{l=0}^{\infty}\frac{\mu^{lN+j}}{(lN+j)!}}\right| \tag{2.12}$$

where $\mu = 2\,|\alpha|^2$ and the detailed fidelity evaluation is shown in the appendices.

Denote $F_j^{(t)}$ as the t-th order approximation of the fidelity, by taking $l = 0, \ldots, t$ in the summation. The zeroth order is

$$F_j^{(0)} \geqslant \left|2^{-j/2}\left(\cos\frac{j}{4}\pi+\sin\frac{j}{4}\pi\right)\right| + O\left(\frac{\mu^N j!}{(N+j)!}\right). \tag{2.13}$$

One can see that $F_0^{(0)} = F_1^{(0)} = 1$ and $F_2^{(0)} = 1/2$, $F_3^{(0)} = 0$, $F_4^{(0)} = 1/4, \ldots$. Since when $F < 1/\sqrt{2}$ would not render any positive key rate [20], it is confirmed that multiphoton states are not secure for QKD due to their large basis dependence in the BB84 protocol.

Take the first-order for $|\lambda_0\rangle$ and $|\lambda_1\rangle$,

$$\begin{aligned} F_0^{(1)} &\geqslant 1 - \left(1 - 2^{-\frac{N-1}{2}}\cos\frac{N-1}{4}\pi\right)\frac{\mu^N}{N!} + O\left(\frac{\mu^{2N}}{(N!)^2}\right) \\ F_1^{(1)} &\geqslant 1 - \left(1 - 2^{-\frac{N}{2}}\cos\frac{N}{4}\pi\right)\frac{\mu^N}{(N+1)!} + O\left(\frac{\mu^{2N}}{[(N+1)!]^2}\right). \end{aligned} \tag{2.14}$$

The fidelity approaches 1 rapidly as N becomes large, especially when μ is small, as shown in figure 2. This shows that with enough discrete phases, one can approximate the vacuum state and the single-photon state infinitely well, which is useful in applications such as QKD.

2.3. Key rate

In the perfect phase-randomized case, the key rate formula is given by the standard Gottesman–Lo–Lütkenhaus–Preskill (GLLP) security analysis for QKD with practical devices [8, 11],

$$\begin{aligned} R &\geqslant -I_{ec} + Q_1\left[1 - H\left(e_1^p\right)\right], \\ I_{ec} &= fQ_\mu H\left(E_\mu\right), \\ Q_1 &= Y_1\mu e^{-\mu}. \end{aligned} \tag{2.15}$$

Here, I_{ec} is the cost of error correction; Q_μ and E_μ are the overall gain and quantum bit error rate (QBER), respectively, which can be directly measured in QKD experiments; Q_1, Y_1, and e_1^p are the gain, yield, and phase error rate of the single-photon component, respectively; $\mu e^{-\mu}$ is the (Poisson) probability that Alice sends single-photon states; μ denotes the expected photon number of the signal state; f denotes the error correction

efficiency; and $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary Shannon entropy function, where p is a binary probability. We assume that Alice and Bob run the efficient BB84 [30] and take the basis shift factor to be 1.

The QKD key rate formula, equation (2.15), is derived using ideas of entanglement distillation [31] and complementarity [32]. It satisfies the composable security definition [33, 34]. In QKD protocols, Alice and Bob need to perform error correction to eliminate the errors and share an identical key. In this error-correction procedure, a fraction of I_{ec} is sacrificed from the raw key. Then, they need to eliminate the eavesdropper's information on the error-corrected key via privacy amplification. The perfect phase randomization allows us to consider the signal as a mixture of Fock states and estimate the contributions of the components of different photon numbers separately [8]. Since multiphoton components are not secure in the BB84 protocol [10], only the single-photon component Q_1 will appear in the key formula [11]. The amount of the eavesdropper's information in the single-photon component is related to the phase error rate, e_1^p.

The core of a practical security analysis is to figure out the privacy amplification term, $Q_1[1 - H(e_1^p)]$, in equation (2.15). For a single-photon state, it is a basis-independent source; thus its phase error rate is equal to its bit error rate [35]. Now, the key point of the analysis is to estimate the yield and bit error rate of the single-photon component, Y_1 and e_1^b. This estimation can be done with different means, such as the decoy-state method [8, 12, 13].

In the case of discrete phase randomization, the photon source is not decomposed into Fock states. Instead, we decompose the channel into $|\lambda_j\rangle$, according to equation (2.5). The single-photon state will be replaced by $|\lambda_1\rangle$ and the Poisson distribution will be replaced by equation (2.8). Then, the approximated single-photon state, $|\lambda_1\rangle$, is no longer a basis-independent source. The basis dependence of the source is evaluated in section 2.2, which causes deviation between the bit and phase error rates.

Now we can slightly modify equation (2.15) to fit our case

$$R \geqslant -I_{ec} + \sum_j P_j Y_j \left[1 - H\left(e_j^p\right)\right], \tag{2.16}$$

where P_j is given in equation (2.8). The yield, Y_j, and bit error rate e_j^b of $|\lambda_j\rangle$, can be estimated by the decoy-state method. Here, without any confusion, we use the same notation as the Fock-state case for simplicity. Given the basis dependence, Δ_j, one can bound the phase error rate e_j^p from e_j^b similar to the work of Lo and Preskill [20],

$$e_j^p \leqslant e_j^b + 4\Delta_j\left(1-\Delta_j\right)\left(1-2e_j^b\right) + 4\left(1-2\Delta_j\right)\sqrt{\Delta_j\left(1-\Delta_j\right)e_j^b\left(1-e_j^b\right)}. \tag{2.17}$$

The basis dependence is defined as

$$\Delta_j = \frac{1-F_j}{2Y_j}. \tag{2.18}$$

where the fidelities, F_j, are given in equation (2.12). The key difference between our result and the original GLLP analysis is that the bit and phase error rates are not the same in the 'single'-photon component.

From the evaluation of the basis dependence, it is not hard to show that only $j = 0$ and $j = 1$ would contribute positively to the final key rate. Thus, the key rate evaluation becomes the following minimization problem.

$$\min_{0\leqslant Y_j, e_j^b \leqslant 1} \left\{P_0 Y_0\left[1 - H\left(e_0^p\right)\right] + P_1 Y_1\left[1 - H\left(e_1^p\right)\right]\right\}. \tag{2.19}$$

There are other constraints based on the gain and QBER obtained from the experiments. Note that with other security proof techniques, the key rate given in equation (2.16) can be improved. For example, the vacuum component, Q_0, is shown [36] to have no phase errors when the photon number channel model is applied.

2.4. Parameter estimation

Now, we need to estimate the key parameters, Y_j and e_j^b. First, let us consider the no-decoy-state case, where we assume all the losses and errors come from $|\lambda_0\rangle$ and $|\lambda_1\rangle$; in the worst case scenario,

$$\begin{aligned} P_0 Y_0 + P_1 Y_1 &\geqslant Q_\mu - \sum_{j=2}^{N-1} P_j, \\ e_0 P_0 Y_0 + e_1 P_1 Y_1 &\leqslant E_\mu Q_\mu. \end{aligned} \tag{2.20}$$

Since the right side of equation (2.20) can be obtained from the experiment directly, one can easily solve the minimization problem presented in equation (2.19) to get the key rate.

We simulate a typical QKD system [37] and compare various cases of N. The result is shown in figure 3, from which we can see that with only four random phases, the performance of discrete phase randomization is close to the performance of continuous phase randomization. We can also observe that the key rate of one phase and two

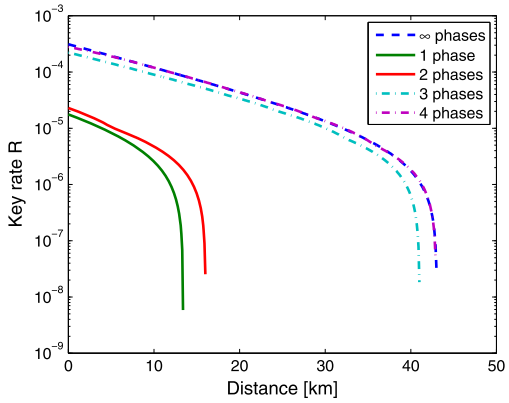

Figure 3. Plots of key rates of the no-decoy-state scheme for different numbers of random phases, N. When $N = 1$, it refers to the no phase randomization case. When $N \to \infty$, it approaches the continuous phase randomization case.

phases are similar, but there is a gap when the phase number becomes three. This can be explained as follows. We note that $F_0^{(2)}$ of $N = 1$ coincides with equation (22) in the work of Lo and Preskill [20]; thus our fidelity formula also extends to the $N = 1$ case. Also, we notice that the first-order term of $N = 1$ vanishes, making the key rate performance of $N = 1$ and $N = 2$ similar—both are of order $1 - O(\mu^2)$. For $N \geqslant 3$, the performance is improved to $1 - O(\mu^N)$. The details of this simulation and all following simulations are shown in the Appendices.

For the case of the decoy-state method, the analysis is trickier. In the perfect phase randomized case, the decoy-state method immensely improves the key rate by offering accurate parameter estimation for equation (2.19). In the security proof of the decoy-state method, the photon number channel model guarantees the following equalities,

$$\begin{aligned} Y_n(\text{signal}) &= Y_n(\text{decoy}), \\ e_n(\text{signal}) &= e_n(\text{decoy}) \end{aligned} \tag{2.21}$$

since all the Fock states, $|n\rangle\langle n|$, are the same in the signal and decoy-states. Thus, adding decoy-states imposes more equations constraints on the parameters,

$$\begin{aligned} Q_\mu &= \sum_{j=0}^{+\infty} \frac{\mu^j e^{-\mu}}{j!} Y_j, \\ E_\mu Q_\mu &= \sum_{j=0}^{+\infty} \frac{\mu^j e^{-\mu}}{j!} e_j Y_j, \\ Q_\nu &= \sum_{j=0}^{+\infty} \frac{\nu^j e^{-\nu}}{j!} Y_j, \\ E_\nu Q_\nu &= \sum_{j=0}^{+\infty} \frac{\nu^j e^{-\nu}}{j!} e_j Y_j, \end{aligned} \tag{2.22}$$

without inducing more variables other than the original unknown variables. Here, $\mu^j e^{-\mu}/j!$ is the (Poisson) probability that Alice sends j photon states. This consequently gives tighter bounds on Y_j and e_j.

This is not so straightforward in the case of N discrete phase randomization, because

$$\left|\lambda_j^{\mu}\right\rangle \neq \left|\lambda_j^{\nu}\right\rangle \tag{2.23}$$

as defined in equation (2.7), where μ and ν are the intensities of signal and decoy-states. Thus, we do not have the simple relations as the continuous phase randomization case, equation (2.21). Fortunately, we have shown that $|\lambda_j\rangle$ is close to the Fock state, $|j\rangle$. We expect the inequality shown in equation (2.23) to be an approximate equality.

Following the quantum coin argument used in the GLLP security analysis [11], the yield and error rate difference between the signal and decoy-states are given by

$$\begin{aligned} \left|Y_j^{\mu} - Y_j^{\nu}\right| &\leqslant \sqrt{1 - F_{\mu\nu}^2}, \\ \left|e_j^{\mu} Y_j^{\mu} - e_j^{\nu} Y_j^{\nu}\right| &\leqslant \sqrt{1 - F_{\mu\nu}^2}, \end{aligned} \tag{2.24}$$

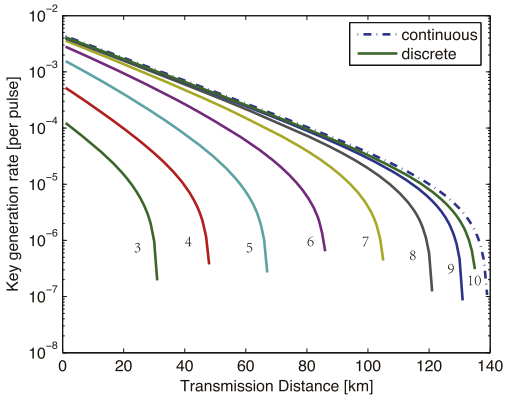

Figure 4. Plots of key rates of the decoy-state scheme for different numbers of random phases, N. Dashed line refers to the continuous phase randomization case. Solid lines from left to right refer to increasing N from 3 to 10.

where

$$F_{\mu\nu} = 1 - O\left(\frac{\mu^N}{N!}\right). \tag{2.25}$$

Now the extra constraints added to the minimization problem of equation (2.19) for the decoy-state method are, along with equation (2.24),

$$\begin{aligned} Q_\mu &= \sum_{j=0}^{N-1} P_j^\mu Y_j^\mu, \\ E_\mu Q_\mu &= \sum_{j=0}^{N-1} e_j^\mu P_j^\mu Y_j^\mu, \\ Q_\nu &= \sum_{j=0}^{N-1} P_j^\nu Y_j^\nu, \\ E_\nu Q_\nu &= \sum_{j=0}^{N-1} e_j^\nu P_j^\nu Y_j^\nu, \end{aligned} \tag{2.26}$$

where P_j^μ are given in equation (2.8). If more decoy-states are used, more linear equations will be added to equation (2.26).

We simulate a QKD system [37] with vacuum+weak decoy-state [38] and compare various cases of phase number N. The decoy and signal intensities are numerically optimized to maximize the key rate. The result is shown in figure 4, from which we can see that with only 10 random phases, the performance of discrete phase randomization is close to the performance of continuous phase randomization.

Note that the QBER with discrete phases highly depends on the experimental parameters. According to our simulation model, each QBER in figures 3 and 4 is a function of the signal intensity, μ, which is numerically optimized to maximize the key rate. This may not lead to the highest tolerable QBER for a given transmission distance. The reason is that by tuning the signal intensity, μ, smaller, one can increase the tolerable QBER at the expense of lowering the key rate. Eventually, the hard bound on the allowable QBER is 11%, just like the single-photon BB84 protocol, despite the number of discrete phases used, as we are following the Shor-Preskill security proof [35] and an infinitely small μ effectively turns a coherent state source into a single-photon source.

3. Discussion

In summary, we just need 10 random phases for the discrete phase randomization, the fidelity of which is close to the continuous case. We demonstrate the effect of discrete phase randomization by taking the QKD protocol as an example, and we show that it gives a big improvement to the performance. Without phase randomization, the key rate decays rapidly as a function of the transmittance of the channel, and drops to zero after less than 15 km of optical fibers, as shown in figure 3. In contrast, with discrete phase randomization, the key rate scales linearly as a function of the transmittance, and the QKD remains feasible over 138 km of fibers, as shown in figure 4. Since only four bits of random numbers per pulse—which already give $2^4 = 16 > 10$ possible phases—are

required for phase randomization, our scheme is highly practical. Note that a much harder discrete phase randomization experiment with 1000 phases [25] has already been demonstrated. Moreover, our method may not only apply to the same signal and reference pulse amplitudes case, but also to the asymmetric amplitude case and the strong reference pulse case. We remark that our discrete phase randomization idea applies to other quantum information processing protocols, including blind quantum computing and quantum coin tossing.

There are a few interesting prospective projects. First, due to the finite length of the key, statistical fluctuation needs to be taken into consideration, which can be dealt with by finite key analysis, as in a recent work [39]. Second, the N-discrete-phase-randomization process might not be perfect in an actual system (i.e., there can be a small fluctuation in the phase modulation such that the actual phase applied will be $\{\delta_k + \frac{2\pi k}{N}\}_{k=0,1,\ldots,n-1}$, where δ_k is a small fluctuating value that can be positive or negative). The imperfect phase modulation can be dealt with by modifying our fidelity calculations. More precisely, one can replace the coherent state $|e^{2k\pi i/N}\alpha\rangle$ by $|e^{2k\pi i/N+\delta_k}\alpha\rangle$ in equation (2.9) and calculate the fidelity in equation (2.12). We expect that the result will be robust against small δ_k. Besides the usual BB84 QKD protocols, our idea can also be extended to measurement-device-independent QKD [40] by treating both sources as being discrete phase randomized.

Acknowledgments

The authors acknowledge insightful discussions with C-H F Fung and X Yuan. This work was supported by the National Basic Research Program of China, Grants No. 2011CBA00300 and No. 2011CBA00301, the 1000 Youth Fellowship program in China, and NSERC.

Appendix A. Basis dependence

This appendix and the following appendices function as follows. In appendix A, the basis dependence between the X and Y (the fidelity of two density matrices) for $|\lambda_j\rangle$ is calculated when N discrete randomized phases are used. In appendix B, we present the parameter estimation of the decoy-state method. In appendix C, the pseudo codes for both nondecoy and decoy simulations are given.

To make the derivation easier to understand, we use index n to represent the photon number, index k to represent the discrete phase, and index j to represent the decomposed Fock-state approximations.

We restate the four BB84 states, phase encoded in the decomposed state $|\lambda_j\rangle$, as presented in the main text,

$$
\begin{aligned}
|0_x^L\rangle &= \frac{\sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|e^{2k\pi i/N}\alpha\right\rangle}{\sqrt{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}} \\
|1_x^L\rangle &= \frac{\sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|-e^{2k\pi i/N}\alpha\right\rangle}{\sqrt{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}} \\
\left|0_y^L\right\rangle &= \frac{\sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|ie^{2k\pi i/N}\alpha\right\rangle}{\sqrt{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}} \\
\left|1_y^L\right\rangle &= \frac{\sum_{k=0}^{N-1} e^{-2kj\pi i/N} \left|e^{2k\pi i/N}\alpha\right\rangle \left|-ie^{2k\pi i/N}\alpha\right\rangle}{\sqrt{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}},
\end{aligned}
\tag{A.1}
$$

where the denominators are the normalization factors.

To evaluate the fidelity between the two states in the two bases, we calculate the related inner products of these four states,

$$
\begin{aligned}
\left\langle 0_x^L \middle| 0_y^L \right\rangle = \left\langle 1_x^L \middle| 1_y^L \right\rangle &= \frac{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{|\alpha|^2(1+i)} e^{-2k\pi i/N}}{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}, \\
\left\langle 0_x^L \middle| 1_y^L \right\rangle = \left\langle 1_x^L \middle| 0_y^L \right\rangle &= \frac{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{|\alpha|^2(1-i)} e^{-2k\pi i/N}}{Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N} e^{2|\alpha|^2 e^{-2k\pi i/N}}}.
\end{aligned}
\tag{A.2}
$$

The detailed calculations of inner products and norms are shown in appendix A.2. Now we substitute these values to evaluate fidelity,

$$\begin{aligned} F\left(\rho_x, \rho_y\right) &= F\left(|0_x^L\rangle\langle 0_x^L| + |1_x^L\rangle\langle 1_x^L|, \left|0_y^L\right\rangle\left\langle 0_y^L\right| + \left|1_y^L\right\rangle\left\langle 1_y^L\right|\right) \\ &\geqslant F\left(|-\rangle|0_x^L\rangle + |+\rangle|1_x^L\rangle, |+i\rangle\left|0_y^L\right\rangle + |-i\rangle\left|1_y^L\right\rangle\right) \\ &= \frac{1}{2}\left|\left(\langle -|\langle 0_x^L| + \langle +|\langle 1_x^L|\right)\left(|+i\rangle\left|0_y^L\right\rangle + |-i\rangle\left|1_y^L\right\rangle\right)\right| \\ &= \frac{\sqrt{2}}{4}\left|\left\langle 0_x^L\middle|0_y^L\right\rangle + i\left\langle 0_x^L\middle|1_y^L\right\rangle + i\left\langle 1_x^L\middle|0_y^L\right\rangle + \left\langle 1_x^L\middle|1_y^L\right\rangle\right| \\ &= \frac{\sqrt{2}}{2}\left|\frac{\sum_{k=0}^{N-1} \mathrm{e}^{2kj\pi \mathrm{i}/N}\left[\mathrm{e}^{|\alpha|^2(1+i)\mathrm{e}^{-2k\pi \mathrm{i}/N}} + i\mathrm{e}^{|\alpha|^2(1-i)\mathrm{e}^{-2k\pi \mathrm{i}/N}}\right]}{\sum_{k=0}^{N-1} \mathrm{e}^{2kj\pi \mathrm{i}/N}\mathrm{e}^{2|\alpha|^2\mathrm{e}^{-2k\pi \mathrm{i}/N}}}\right| \end{aligned} \tag{A.3}$$

where $|\pm\rangle$ and $|\pm i\rangle$ are the normalized eigenstates of the X and Y bases. The inequality comes from the fact that the fidelity of two mixed states is the maximal of the fidelity of all the purifications. Here, we use the intuition that two Bell states are the same,

$$|+\rangle|-\rangle + |-\rangle|+\rangle = |+i\rangle|+i\rangle + |-i\rangle|-i\rangle. \tag{A.4}$$

Now, let us simplify equation (A.3); we expect it to be close to 1 when N is large.

$$F\left(\rho_x, \rho_y\right) \geqslant \frac{\sqrt{2}}{2}\left|\frac{\sum x^{-j}\left[\mathrm{e}^{|\alpha|^2(1+i)x} + i\mathrm{e}^{|\alpha|^2(1-i)x}\right]}{\sum x^{-j}\mathrm{e}^{2|\alpha|^2 x}}\right| \tag{A.5}$$

where the summation is taken over $x = 1, \mathrm{e}^{2\pi \mathrm{i}/N}, \ldots, \mathrm{e}^{2\pi \mathrm{i}(N-1)/N}$, N dots evenly distributed on the unit circle of the complex plane. Take the Taylor expansion of $\mu = 2|\alpha|^2 \geqslant 0$ around 0,

$$\begin{aligned} F\left(\rho_x, \rho_y\right) &\geqslant \left|\frac{\sum x^{-j}\sum_{n=0}^{\infty}\frac{\left(\mu x/\sqrt{2}\right)^n}{n!}\left(\cos\frac{n\pi}{4} + \sin\frac{n\pi}{4}\right)}{\sum x^{-j}\sum_{n=0}^{\infty}\frac{(\mu x)^n}{n!}}\right| \\ &= \left|\frac{\sum_{n=0}^{\infty}\frac{\left(\mu/\sqrt{2}\right)^n}{n!}\left(\cos\frac{n\pi}{4} + \sin\frac{n\pi}{4}\right)\sum x^{n-j}}{\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\sum x^{n-j}}\right| \\ &= \left|\frac{\sum_{l=0}^{\infty}\frac{\mu^{lN+j}}{(lN+j)!}2^{-\frac{lN+j}{2}}\left(\cos\frac{lN+j}{4}\pi + \sin\frac{lN+j}{4}\pi\right)}{\sum_{l=0}^{\infty}\frac{\mu^{lN+j}}{(lN+j)!}}\right|. \end{aligned} \tag{A.6}$$

The details of the Taylor expansion and the calculation of $\sum x^{n-j}$ are shown in appendix A.3.

A.1. Approximations: large N or small μ

Here, we want to check the fidelity given in equation (A.6) when N is large or μ is small. The zeroth order, by taking $l = 0$ in the summation,

$$\begin{aligned} F_j^{(0)} &= \left|\frac{\frac{\mu^j}{j!}2^{-\frac{j}{2}}\left(\cos\frac{j}{4}\pi + \sin\frac{j}{4}\pi\right)}{\frac{\mu^j}{j!}}\right| + O\left(\frac{\mu^N j!}{(N+j)!}\right) \\ &\approx \left|2^{-j/2}\left(\cos\frac{j}{4}\pi + \sin\frac{j}{4}\pi\right)\right| \end{aligned} \tag{A.7}$$

One can see that $F_0^{(0)} = F_1^{(0)} = 1$ and $F_2^{(0)} = 1/2$, $F_3^{(0)} = 0$, $F_4^{(0)} = 1/4, \ldots$. It is confirmed that multiphoton states are not secure for the BB84 QKD protocol.

The first-order approximation, by taking $l=0$ and $l=1$ in the summation,

$$\begin{aligned}
F_j^{(1)} &= \left| \frac{\frac{\mu^j}{j!}2^{-\frac{j}{2}}\left(\cos\frac{j}{4}\pi+\sin\frac{j}{4}\pi\right)+\frac{\mu^{N+j}}{(N+j)!}2^{-\frac{N+j}{2}}\left(\cos\frac{N+j}{4}\pi+\sin\frac{N+j}{4}\pi\right)}{\frac{\mu^j}{j!}+\frac{\mu^{N+j}}{(N+j)!}} \right| \\
&\quad + O\left(\frac{\mu^{2N}j!}{(2N+j)!}\right) \\
&= \left| \frac{2^{-\frac{j}{2}}\left(\cos\frac{j}{4}\pi+\sin\frac{j}{4}\pi\right)+\frac{\mu^{N}j!}{(N+j)!}2^{-\frac{N+j}{2}}\left(\cos\frac{N+j}{4}\pi+\sin\frac{N+j}{4}\pi\right)}{1+\frac{\mu^{N}j!}{(N+j)!}} \right| \\
&\quad + O\left(\frac{\mu^{2N}j!}{(2N+j)!}\right) \\
&= \left| 2^{-\frac{j}{2}}\left(\cos\frac{j}{4}\pi+\sin\frac{j}{4}\pi\right)-\left[1-2^{-\frac{N+j}{2}}\left(\cos\frac{N+j}{4}\pi+\sin\frac{N+j}{4}\pi\right)\right] \right. \\
&\quad \left. \times\frac{\mu^N j!}{(N+j)!} \right| \\
&\quad + O\left(\left[\frac{\mu^N j!}{(N+j)!}\right]^2\right)+O\left(\frac{\mu^{2N}j!}{(2N+j)!}\right)
\end{aligned} \tag{A.8}$$

Since $N \geqslant j$, the second $O(\cdot)$ in the last equality can be neglected. The first-order approximation will approach the zeroth order exponentially fast, $O(\mu^N/N!)$. We are interested in the first two cases, $j=0$ and $j=1$,

$$\begin{aligned}
F_0^{(1)} &= 1-\left[1-2^{-\frac{N}{2}}\left(\cos\frac{N}{4}\pi+\sin\frac{N}{4}\pi\right)\right]\frac{\mu^N}{N!}+O\left(\frac{\mu^{2N}}{(N!)^2}\right) \\
&= 1-\left(1-2^{-\frac{N-1}{2}}\cos\frac{N-1}{4}\pi\right)\frac{\mu^N}{N!}+O\left(\frac{\mu^{2N}}{(N!)^2}\right) \\
F_1^{(1)} &= 1-\left[1-2^{-\frac{N+1}{2}}\left(\cos\frac{N+1}{4}\pi+\sin\frac{N+1}{4}\pi\right)\right]\frac{\mu^N}{(N+1)!} \\
&\quad + O\left(\left[\frac{\mu^N}{(N+1)!}\right]^2\right) \\
&= 1-\left(1-2^{-\frac{N}{2}}\cos\frac{N}{4}\pi\right)\frac{\mu^N}{(N+1)!}+O\left(\frac{\mu^{2N}}{[(N+1)!]^2}\right)
\end{aligned} \tag{A.9}$$

We note that the second-order approximation of F_0 when $N=1$ coincides with equation (22) in [20]; thus our fidelity formula also extends to the $N=1$ case. Also, we notice the first-order term when $N=1$ vanishes, making the key rate performance of $N=1$ and $N=2$ similar—both are of order $1-O(\mu^2)$. For $N \geqslant 3$, the performance is improved to $1-O(\mu^N)$.

A.2. Inner products and norms

Inner products,

$$\begin{aligned}
\left\langle 0_x^L \middle| 0_y^L \right\rangle &= \left(\sum_{l=0}^{N-1} \mathrm{e}^{2lj\pi \mathrm{i}/N} \left\langle \mathrm{e}^{2l\pi \mathrm{i}/N}\alpha \right| \left\langle \mathrm{e}^{2l\pi \mathrm{i}/N}\alpha \right| \right) \\
&\quad \times \left(\sum_{k=0}^{N-1} \mathrm{e}^{-2kj\pi \mathrm{i}/N} \left| \mathrm{e}^{2k\pi \mathrm{i}/N}\alpha \right\rangle \middle| i\mathrm{e}^{2k\pi \mathrm{i}/N}\alpha \right\rangle \right)
\end{aligned}$$

$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)j\pi i/N}\left\langle e^{2l\pi i/N}\alpha\middle|e^{2k\pi i/N}\alpha\right\rangle\left\langle e^{2l\pi i/N}\alpha\middle|ie^{2k\pi i/N}\alpha\right\rangle$$
$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)j\pi i/N}e^{-|\alpha|^2\left[2-(1+i)e^{2(k-l)\pi i/N}\right]}$$
$$= Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N}e^{|\alpha|^2(1+i)e^{-2k\pi i/N}} \tag{A.10}$$

where we use the fact that $e^{2kj\pi i/N}$ and $e^{-2k\pi i/N}$ each form a ring in the complex plane, and

$$\left\langle 0_x^L\middle|1_y^L\right\rangle = \left(\sum_{l=0}^{N-1} e^{2lj\pi i/N}\left\langle e^{2l\pi i/N}\alpha\middle|\left\langle e^{2l\pi i/N}\alpha\right|\right)\times\left(\sum_{k=0}^{N-1} e^{-2kj\pi i/N}\left|e^{2k\pi i/N}\alpha\right\rangle\middle|-ie^{2k\pi i/N}\alpha\right\rangle\right)$$
$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)j\pi i/N}\left\langle e^{2l\pi i/N}\alpha\middle|e^{2k\pi i/N}\alpha\right\rangle\left\langle e^{2l\pi i/N}\alpha\middle|-ie^{2k\pi i/N}\alpha\right\rangle$$
$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)j\pi i/N}e^{-|\alpha|^2\left[2-(1-i)e^{2(k-l)\pi i/N}\right]}$$
$$= Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2kj\pi i/N}e^{|\alpha|^2(1-i)e^{-2k\pi i/N}} \tag{A.11}$$

Norms,

$$\langle 0_x^L|0_x^L\rangle = \left(\sum_{l=0}^{N-1} e^{2l\pi i/N}\left\langle e^{2l\pi i/N}\alpha\middle|\left\langle e^{2l\pi i/N}\alpha\right|\right)\times\left(\sum_{k=0}^{N-1} e^{-2k\pi i/N}\left|e^{2k\pi i/N}\alpha\right\rangle\middle|e^{2k\pi i/N}\alpha\right\rangle\right)$$
$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)\pi i/N}\left\langle e^{2l\pi i/N}\alpha\middle|e^{2k\pi i/N}\alpha\right\rangle^2$$
$$= \sum_{l=0}^{N-1}\sum_{k=0}^{N-1} e^{2(l-k)\pi i/N}e^{-2|\alpha|^2\left[1-e^{2(k-l)\pi i/N}\right]}$$
$$= Ne^{-2|\alpha|^2}\sum_{k=0}^{N-1} e^{2k\pi i/N}e^{2|\alpha|^2e^{-2k\pi i/N}} \tag{A.12}$$

Here, we use the inner products between two coherent states,

$$\langle\alpha|\beta\rangle = \exp\left(-\frac{1}{2}|\alpha|^2 + \alpha^*\beta - \frac{1}{2}|\beta|^2\right)$$
$$\langle\alpha e^{i\phi}|\alpha e^{i\theta}\rangle = e^{-|\alpha|^2(1-\exp[i(\theta-\phi)])}. \tag{A.13}$$

It is not hard to see that by adding a same phase to ϕ and θ, the result is the same.

A.3. Taylor expansion and summation

Taylor expansion:

$$e^{|\alpha|^2(1+i)x} + ie^{|\alpha|^2(1-i)x} = 1 + \frac{1+i}{2}\mu x + \frac{\left(\frac{1+i}{2}\mu x\right)^2}{2!} + \frac{\left(\frac{1+i}{2}\mu x\right)^3}{3!} + \ldots$$
$$+ i + i\frac{1-i}{2}\mu x + i\frac{\left(\frac{1-i}{2}\mu x\right)^2}{2!} + i\frac{\left(\frac{1-i}{2}\mu x\right)^3}{3!} + \ldots$$
$$= (1+i)\sum_{n=0}^{\infty}\left(\frac{\mu x}{\sqrt{2}}\right)^n\frac{1}{n!}\left(\cos\frac{n\pi}{4} + \sin\frac{n\pi}{4}\right) \tag{A.14}$$

Summation:

$$\sum_x x^{n-j} = \sum_{k=0}^{N-1} \mathrm{e}^{-2k(n-j)\pi \mathrm{i}/N}, \tag{A.15}$$

which equals N if $n-j \mod N = 0$ and equals 0 if $n-j \mod N \neq 0$. The summation is taken over $x = 1, \mathrm{e}^{2\pi \mathrm{i}/N}, \ldots, \mathrm{e}^{2\pi \mathrm{i}(N-1)/N}$, N dots evenly distributed on the unit circle of the complex plane.

Appendix B. Parameter deviation in the decoy-state method

Here we consider the parameter (Y_j and e_j) deviations between the signal states and the decoy-states in the case of N discrete phase randomization. Denote the intensity of the signal state to be μ and the decoy state to be ν, $\nu < \mu$. We want to figure out the relationships between Y_j^{μ}, e_j^{μ} and Y_j^{ν}, e_j^{ν}, respectively.

We follow the tagged idea for the phase error estimation [11]. First, we need to evaluate the fidelity between $|\lambda_j^{\mu}\rangle$ and $|\lambda_j^{\nu}\rangle$ as defined in the main text,

$$\begin{aligned} \left|\lambda_j^{\mu}\right\rangle &= \sum_{l=0}^{\infty} \frac{\alpha^{lN+j}}{\sqrt{(lN+j)!}} \left|lN+j\right\rangle \\ \left|\lambda_j^{\nu}\right\rangle &= \sum_{l=0}^{\infty} \frac{\beta^{lN+j}}{\sqrt{(lN+j)!}} \left|lN+j\right\rangle \end{aligned} \tag{B.1}$$

where $\mu = |\alpha|^2$ and $\nu = |\beta|^2$. We note that these are the states after phase randomization and before qubit encoding. Then the fidelity is given by

$$\begin{aligned} F\left(\left|\lambda_j^{\mu}\right\rangle, \left|\lambda_j^{\nu}\right\rangle\right) &= \frac{\left|\left\langle \lambda_j^{\mu} \middle| \lambda_j^{\nu} \right\rangle\right|}{\sqrt{\left\langle \lambda_j^{\mu} \middle| \lambda_j^{\mu} \right\rangle \left\langle \lambda_j^{\nu} \middle| \lambda_j^{\nu} \right\rangle}} \\ &= \frac{\left| \sum_{l=0}^{\infty} \frac{\left(\alpha^{*}\beta\right)^{lN+j}}{(lN+j)!} \right|}{\sqrt{\sum_{l=0}^{\infty} \frac{|\alpha|^{2\,lN+2j}}{(lN+j)!} \sum_{l=0}^{\infty} \frac{|\beta|^{2\,lN+2j}}{(lN+j)!}}} \\ &= \frac{\sum_{l=0}^{\infty} \frac{(\mu\nu)^{lN/2}}{(lN+j)!}}{\sqrt{\sum_{l=0}^{\infty} \frac{\mu^{lN}}{(lN+j)!} \sum_{l=0}^{\infty} \frac{\nu^{lN}}{(lN+j)!}}} \end{aligned} \tag{B.2}$$

In the last equality, we assume that $\alpha^{*}\beta$ is a real number, which can be set when their phases are the same. In the experiment, one can think of the scenario where the decoy-state intensity modulation is done after phase randomization. When $N \to \infty$, this fidelity will go to 1 as the photon number channel model. Take the first-order approximation when N is large or μ is small,

$$\begin{aligned} F\left(\left|\lambda_j^{\mu}\right\rangle, \left|\lambda_j^{\nu}\right\rangle\right) &= \frac{\left|1 + \frac{(\mu\nu)^{N/2} j!}{(N+j)!}\right|}{\left[\left(1 + \frac{\mu^N j!}{(N+j)!}\right)\left(1 + \frac{\nu^N j!}{(N+j)!}\right)\right]^{1/2}} \\ &\quad + O\left(\left[\frac{\mu^N j!}{(N+j)!}\right]^2\right) \\ &= 1 + \frac{(\mu\nu)^{N/2} j!}{(N+j)!} - \frac{1}{2}\frac{\mu^N j!}{(N+j)!} - \frac{1}{2}\frac{\nu^N j!}{(N+j)!} \end{aligned}$$

$$+ O\left(\left[\frac{\mu^N j!}{(N+j)!}\right]^2\right)$$
$$= 1 - \left[\frac{\mu^N + \nu^N}{2} - (\mu\nu)^{N/2}\right]\frac{j!}{(N+j)!}$$
$$+ O\left(\left[\frac{\mu^N j!}{(N+j)!}\right]^2\right) \tag{B.3}$$

One can show that equation (B.2) is a non-decreasing function with increasing j,

$$F\left(\left|\lambda_j^{\mu}\right\rangle, \left|\lambda_j^{\nu}\right\rangle\right) \geqslant F\left(|\lambda_0^{\mu}\rangle, |\lambda_0^{\nu}\rangle\right)$$
$$= \frac{\sum_{l=0}^{\infty}\frac{(\mu\nu)^{lN/2}}{(lN)!}}{\sqrt{\sum_{l=0}^{\infty}\frac{\mu^{lN}}{(lN)!}\sum_{l=0}^{\infty}\frac{\nu^{lN}}{(lN)!}}}$$
$$\equiv F_{\mu\nu} \tag{B.4}$$

Apply the quantum coin idea from GLLP [11],

$$\sqrt{Y_j^{\mu}Y_j^{\nu}} + \sqrt{\left(1 - Y_j^{\mu}\right)\left(1 - Y_j^{\nu}\right)} \geqslant F\left(\left|\lambda_j^{\mu}\right\rangle, \left|\lambda_j^{\nu}\right\rangle\right)$$
$$\sqrt{e_j^{\mu}Y_j^{\mu}e_j^{\nu}Y_j^{\nu}} + \sqrt{\left(1 - e_j^{\mu}Y_j^{\mu}\right)\left(1 - e_j^{\nu}Y_j^{\nu}\right)} \geqslant F\left(\left|\lambda_j^{\mu}\right\rangle, \left|\lambda_j^{\nu}\right\rangle\right) \tag{B.5}$$

Normally Y_j is in the order of channel transmittance, η. One can see that if $F(|\lambda_j^{\mu}\rangle, |\lambda_j^{\nu}\rangle) \leqslant \sqrt{1-\eta}$, the difference can be from $[0, 1]$, which would result in a zero key rate. On the other hand, if $F = 1$, we have $Y_j^{\mu} = Y_j^{\nu}$, which is reasonable since the yields of the same states should be the same.

With the calculations presented in appendix B.1, we can solve equation (B.6),

$$\left|Y_j^{\mu} - Y_j^{\nu}\right| \leqslant \sqrt{1 - F_{\mu\nu}^2}$$
$$\left|e_j^{\mu}Y_j^{\mu} - e_j^{\nu}Y_j^{\nu}\right| \leqslant \sqrt{1 - F_{\mu\nu}^2} \tag{B.6}$$

Note that once N, μ, and ν are given, $F_{\mu\nu}$ is given by equation (B.4), and hence the yield and error rate differences are fixed.

B.1. Bound the parameter difference between signal and decoy-state

To make it simpler, we rewrite equation (B.6) in the following form,

$$\sqrt{ab} + \sqrt{(1-a)(1-b)} \geqslant F \tag{B.7}$$

where $a, b \in [0, 1]$. Let $a = \sin^2 x$ and $b = \sin^2 y$, where $x, y \in [0, \pi/2]$. Then

$$F \leqslant \sin x \sin y + \cos x \cos y$$
$$= \cos(x - y). \tag{B.8}$$

Thus,

$$|x - y| \leqslant \arccos F. \tag{B.9}$$

Since F is close 1, $|x - y|$ is close to 0. That is, a and b are close to each other,

$$|a - b| = |\sin^2 x - \sin^2 y|$$
$$= |\sin(x + y)\sin(x - y)|$$
$$\leqslant \sin(\arccos F)$$
$$= \sqrt{1 - F^2} \tag{B.10}$$

Appendix C. Simulation

In this section, we calculate the key rates of both decoy and non-decoy methods derived in the main text. We use typical experimental parameters [37], which are $e_d = 0.033$, $\eta = 10^{-\alpha L/10}\eta_{Bob}$ where $\alpha = 0.2$ dB/km, $\eta_{Bob} = 0.045$, $Y_0 = 1.7 \times 10^{-6}$ and assumed an error-correction inefficiency, $f(e) = 1.16$. Here e_d is the

intrinsic error rate of Bob's detectors. For each value of the distance, the signal strength, μ, has been chosen to optimize the rate. In the simulation model, $Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta\mu}$.

C.1. Non-decoy

1. First we calculate $P_j = \sum_{l=0}^{\infty} \frac{\mu^{lN+j}\mathrm{e}^{-\mu}}{(lN+j)!}$.
2. Then we calculate $F_j(\rho_x, \rho_y) \geqslant \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!} 2^{-\frac{lN+j}{2}} \left(\cos\frac{lN+j}{4}\pi + \sin\frac{lN+j}{4}\pi \right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!}} \right|$.
3. For (e_0, e_1, Y_0, Y_1) in the domain defined by

$$P_0 Y_0 + P_1 Y_1 \geqslant Q_\mu - \sum_{j=2}^{N-1} P_j,$$
$$e_0 P_0 Y_0 + e_1 P_1 Y_1 \leqslant E_\mu Q_\mu$$

   according to the main text, where the notations are defined in the main text, we calculate Δ_j and e_j^p according to equations (2.17) and (2.18).
4. Substitute the above quantities into $\min_{0\leqslant Y_j, e_j^b \leqslant 1}\{P_0 Y_0[1 - H(e_0^p)] + P_1 Y_1[1 - H(e_1^p)]\}$ and numerically optimize (e_0, e_1, Y_0, Y_1) for the minimum.
5. Calculate the key rate, $R = \min_{0\leqslant Y_j, e_j^b \leqslant 1}\{P_0 Y_0[1 - H(e_0^p)] + P_1 Y_1[1 - H(e_1^p)]\} - I_{ec}$.

The signal intensity μ is numerically optimized to maximize the key rate. A typical value of μ ranges from 0.001 to 0.02. When the number of phases, N, is large, μ is approximately the decay rate, η.

C.2. Decoy

1. First we calculate $P_j = \sum_{l=0}^{\infty} \frac{\mu^{lN+j}\mathrm{e}^{-\mu}}{(lN+j)!}$.
2. Then we calculate $F_j(\rho_x, \rho_y) \geqslant \left| \frac{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!} 2^{-\frac{lN+j}{2}} \left(\cos\frac{lN+j}{4}\pi + \sin\frac{lN+j}{4}\pi \right)}{\sum_{l=0}^{\infty} \frac{\mu^{lN+j}}{(lN+j)!}} \right|$.
3. Next we calculate $F_{\mu\nu} = 1 - O\left(\frac{\mu^N}{N!}\right)$.
4. For (e_0, e_1, Y_0, Y_1) in the domain defined by

$$\left|Y_j^\mu - Y_j^\nu\right| \leqslant \sqrt{1 - F_{\mu\nu}^2}$$
$$\left|e_j^\mu Y_j^\mu - e_j^\nu Y_j^\nu\right| \leqslant \sqrt{1 - F_{\mu\nu}^2}$$
$$Q_\mu = \sum_{j=0}^{N-1} P_j^\mu Y_j^\mu$$
$$E_\mu Q_\mu = \sum_{j=0}^{N-1} e_j^\mu P_j^\mu Y_j^\mu,$$

   we calculate Δ_j and e_j^p according to equations (2.17) and (2.18).
5. Substitute the above quantities into $\min_{0\leqslant Y_j, e_j^b \leqslant 1}\{P_0 Y_0[1 - H(e_0^p)] + P_1 Y_1[1 - H(e_1^p)]\}$ and numerically optimize (e_0, e_1, Y_0, Y_1) for the minimum.
6. Calculate the key rate, $R = \min_{0\leqslant Y_j, e_j^b \leqslant 1}\{P_0 Y_0[1 - H(e_0^p)] + P_1 Y_1[1 - H(e_1^p)]\} - I_{ec}$.

The decoy and signal intensities, μ and ν, are numerically optimized to maximize the key rate. A typical value of μ is 0.5. One weak decoy-state with a typical mean photon number of $\nu = 0.001$ and one vacuum state are used.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE Press) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3
[3] Knill E, Laflamme R and Milburn G J 2001 *Nature* **409** 46
[4] Kent A 2012 *Phys. Rev. Lett.* **109** 130501
[5] Pappa A, Chailloux A, Diamanti E and Kerenidis I 2011 *Phys. Rev.* A **84** 052305
[6] Dunjko V, Kashefi E and Leverrier A 2012 *Phys. Rev. Lett.* **108** 200502
[7] Glauber R J 1963 *Phys. Rev.* **131** 2766–88
[8] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[9] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[10] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330–3
[11] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[12] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[13] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[14] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[15] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
[16] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
[17] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B and Pan J W 2007 *Phys. Rev. Lett.* **98** 010505
[18] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[19] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475–8
[20] Lo H K and Preskill J 2007 *Quantum Inf. Comput.* **7** 0431
[21] Sun S H, Gao M, Jiang M S, Li C Y and Liang L M 2012 *Phys. Rev.* A **85** 032304
[22] Tang Y L, Yin H L, Ma X, Fung C H F, Liu Y, Yong H L, Chen T Y, Peng C Z, Chen Z B and Pan J W 2013 *Phys. Rev.* A **88** 022308
[23] Xu F, Qi B, Ma X, Xu H, Zheng H and Lo H K 2012 *Opt. Express* **20** 12366–77
[24] Abellán C, Amaya W, Jofre M, Curty M, Acín A, Capmany J, Pruneri V and Mitchell M W 2014 *Opt. Express* **22** 1645–54
[25] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[26] Koashi M 2004 *Phys. Rev. Lett.* **93** 120501
[27] Tamaki K 2008 *Phys. Rev.* A **77** 032341
[28] Ferenczi A, Narasimhachar V and Lütkenhaus N 2012 *Phys. Rev.* A **86** 042327
[29] Marcikic I, de Riedmatten H, Tittel W, Scarani V, Zbinden H and Gisin N 2002 *Phys. Rev.* A **66** 062308
[30] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133–65
[31] Lo H K and Chau H F 1999 *Science* **283** 2050
[32] Koashi M 2006 *J. Phys. Conf. Ser.* **36** 98
[33] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 The universal composable security of quantum key distribution (*Second Theory of Cryptography Conf. TCC 2005, Lecture Notes in Computer Science* vol 3378) (Berlin: Springer) pp 386–406
[34] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries (*Second Theory of Cryptography Conference TCC 2005, Lecture Notes in Computer Science* vol 3378) (Berlin: Springer) pp 407–25
[35] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[36] Lo H K 2005 *Quantum Inf. Comput.* **5** 413–8
[37] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762–4
[38] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[39] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev.* A **89** 022307
[40] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503