Practical Quantum Key Distribution with Non-Phase-Randomized Coherent States

Li Liu,[1,2,3] Yukun Wang,[3,*] Emilien Lavie,[3] Chao Wang,[3] Arno Ricou,[4] Fen Zhuo Guo,[1,2] and Charles Ci Wen Lim[3,4,†]

[1] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[4] *Centre for Quantum Technologies, National University of Singapore, Singapore*

(Received 6 May 2019; revised manuscript received 25 June 2019; published 22 August 2019)

Quantum key distribution (QKD) based on coherent states is well known for its implementation simplicity, but it suffers from loss-dependent attacks based on optimal unambiguous state discrimination. Crucially, previous research has suggested that coherent-state QKD is limited to short distances, typically below 100 km, assuming standard optical fiber loss and system parameters. In this work, we propose a six-coherent-state phase-encoding QKD protocol that is able to tolerate the total loss of up to 38 dB, assuming realistic system parameters, and up to 56 dB loss, assuming zero noise. The security of the protocol is calculated using a recently developed security proof technique based on semidefinite programming, which assumes only the inner-product information of the encoded coherent states, the expected statistics, and that the measurement is basis independent. Our results thus suggest that coherent-state QKD could be a promising candidate for high-speed provably secure QKD.

DOI: 10.1103/PhysRevApplied.12.024048

I. INTRODUCTION

Quantum key distribution (QKD) [1] is one of the most established quantum-information technologies to date. Its basic goal is to distribute secret keys between two remote users (called Alice and Bob) embedded in an untrusted network. Importantly, unlike conventional key distribution methods, QKD is provably secure and can be safely used with any cryptographic protocol that requires long-term security assurance. For an overview of QKD and its recent developments, we refer the interested reader to Refs. [2–4].

In prepare-and-measure QKD, there are generally two classes of coherent-state protocols, namely, those that are based on phase randomization and those that give the phase reference information to Eve (the adversary). In the former, one first uniformly randomizes the phase of the coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ to create a mixture of photon number states, i.e.,

$$\rho_\mu = \int_0^{2\pi} \frac{d\theta}{2\pi} |\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}| = e^{-\mu} \sum_{n\geq 0} \frac{\mu^n}{n!} |n\rangle\langle n|. \quad (1)$$

This mixture follows a Poisson distribution and emits a single-photon state with probability $\mu e^{-\mu}$ and multiphoton states with probability $1 - e^{-\mu}(1+\mu)$, where μ is the mean photon number of the signal. Then, by using a statistical technique called the decoy-state method to bound the fraction of detected single-photon states, one can get secret key rates that are comparable to those with a true single-photon source [5–7]. In the following, we refer to phase-randomized coherent-state QKD as decoy-state QKD since they often mean the same protocol in the literature.

In the case that the phase reference is given to Eve, she no longer sees a mixture of photon number states, but a coherent state $|\alpha_x\rangle$ that is randomly drawn from a set of possible preparations $\{|\alpha_x\rangle\}_x$, which is necessarily linearly independent. Crucially, based on this phase information, Eve can optimize her attack strategy to distinguish between different subsets of the preparation set [8–10]. In the worst-case scenario (given the channel loss is sufficiently high), she can determine the exact value of x by performing unambiguous state discrimination. For this reason, most existing security analyses of non-phase-randomized coherent-state QKD show that the tolerable channel loss is significantly below that of decoy-state QKD [11,12]. For example, assuming standard experimental settings, we find that the maximum distance (fiber length) of the

[*] elewayu@nus.edu.sg
[†] charles.lim@nus.edu.sg

phase-encoding coherent-state QKD protocol is generally shorter than 100 km, while decoy-state QKD can achieve up to about 250 km (see the simulation results below).

Yet, in practice, it may be more attractive to consider non-phase-randomized coherent-state QKD. The main reason is that the set of security assumptions for non-phase-randomized coherent-state QKD is typically less stringent than that of decoy-state QKD. To appreciate this point, we note that it is very important for decoy-state QKD systems to completely randomize the phase of their quantum signals. There could be serious security loopholes if this assumption is not met [9,10].

In more detail, to achieve a complete phase randomization of coherent states, one can either use gain-switching techniques [13,14] or active phase randomization using external modulators [15,16]. In the case of lasers using gain-switching techniques, each generated optical pulse carries a random and independent phase, which is derived from the intrinsic fluctuations due to the vacuum state. However, this is valid only if the laser diode is driven properly and the residual photons of each lasing event vanish before the next lasing [14]. Since the lasing interval should be longer than the effective photon lifetime of the laser diode to guarantee independent random phases, it may limit the maximum repetition rate of gain-switching-based QKD systems, especially when considering high-speed transmission. Moreover, it has also been shown that such a phase randomization method deteriorates if an external laser is injected into the cavity and contributes to field amplification, which may lead to potential side-channel attacks on practical systems [17].

As for active phase randomization with phase modulators, the idea is to simulate complete phase randomization using discrete random phase modulation. However, while one expects this method to be a good approximation of the ideal requirement (if the number of discrete phases is large enough), there is still a gap between the theory and practice of decoy-state QKD. Recently, it has been pointed out that the requirement of ideal phase randomization can be replaced by discrete phase randomization with some small penalty on the secret key rate [18]. This work represents an important step toward making decoy-state QKD more practical, but it introduces additional complexity [14,19] into the setup, which may be tricky (or even less desirable) when considering finite-key security analysis.

In this work, we propose a six-coherent-state protocol and show that it offers significant advantages in both secret key rate and transmission distance over existing coherent-state QKD protocols [12,20]. In order to achieve good secret key rates using non-phase-randomized coherent states, it is important to have a tight estimation of Eve's information about the secret key. While in principle one could obtain a tight estimation of Eve's information by considering all the possible eavesdropping strategies, it is computationally intractable to fully characterize them, especially if the underlying Hilbert space dimension is unknown. To resolve this technical difficulty, here we employ the numerical tool introduced in Ref. [20] to bound Eve's information, which roughly speaking, converts the characterization problem of Eve's strategies into a tractable hierarchy of semidefinite programs (SDP). It has been shown in Ref. [20] that the SDP method provides a tighter bound on Eve's information as compared to existing methods that use the so-called quantum coin method [12]. Additionally, the SDP method has semi-device-independent feature [21–26], namely, the detailed characterization of Bob's measurements is no longer necessary, but different from previous SDI, which is based on dimension or energy assumption, the analysis here is made based on the known inner product information of the coherent states. As such, the security certified by this method is robust against a large class of quantum device flaws and imperfections.

The organization of the paper is as follows. In Sec. II, for pedagogical reasons, we first review a standard coherent-state QKD protocol that encodes the secret key into the relative phase of the coherent states. In Sec. III, we first introduce a six-coherent-state protocol that allows the test coherent states to use different mean photon number from that of the key states. Then, we use the method introduced in Ref. [20] to derive the secret key rate of the protocol and simulate its expected performance using standard experimental parameters. Finally, we conclude our findings in Sec. IV.

II. PHASE-ENCODING BB84 COHERENT-STATE QKD

In this section, we first review a popular coherent-state QKD protocol, which is inspired by the celebrated Bennett and Brassard 1984 (BB84) QKD [1]. Here, the protocol encodes the secret bit into the relative phase of two coherent states, where the first coherent state is the signal state (the modulated signal) and the second coherent state is the reference state (fixed and whose phase reference is given to Eve). More specifically, Alice sends one of four states randomly:

$$\begin{aligned}
|\tilde{0}_{\text{key}}\rangle &= |\alpha\rangle_R \otimes |\alpha\rangle_S,\\
|\tilde{1}_{\text{key}}\rangle &= |\alpha\rangle_R \otimes |-\alpha\rangle_S,\\
|\tilde{0}_{\text{test}}\rangle &= |\alpha\rangle_R \otimes |i\alpha\rangle_S,\\
|\tilde{1}_{\text{test}}\rangle &= |\alpha\rangle_R \otimes |-i\alpha\rangle_S,
\end{aligned} \tag{2}$$

where the phase of α is relative to a fixed classical phase reference frame that Eve can access. Here, the subscripts S and R denote the signal state and reference state, respectively. Then, Bob measures the signal he receives in either the key basis or test basis. When Bob measures the signal in the key basis, he combines the two modes in an interferometer and directs modes $a_{0,\text{key}}$, $a_{1,\text{key}}$ to two different threshold photon detectors, where

$$a_{0,\text{key}} = (a_R + a_S)/\sqrt{2},$$
$$a_{1,\text{key}} = (a_R - a_S)/\sqrt{2}. \tag{3}$$

In an ideal case, if Alice sends $|\tilde{0}_{\text{key}}\rangle$ to Bob and he measures in the key basis, detector D_0 (model $a_{0,\text{key}}$) clicks (with some probability depending on the channel loss) and detector D_1 (model $a_{1,\text{key}}$) does not click. Likewise, if Alice sends $|\tilde{1}_{\text{key}}\rangle$, then detector D_0 does not click and detector D_1 clicks with some probability. Hence, Bob can determine the bit value that Alice encodes in the key basis. When Bob measures in the test basis, he directs modes $a_{0,\text{test}}$, $a_{1,\text{test}}$ to the detectors, where

$$a_{0,\text{test}} = (a_R + ia_S)/\sqrt{2},$$
$$a_{1,\text{test}} = (a_R - ia_S)/\sqrt{2}. \tag{4}$$

Similarly, Bob can determine the bit value that Alice encodes in the test basis. Then, Alice and Bob retain only the successful events in which they choose the same basis through public communication. After performing the error correction step and privacy amplification step, Alice and Bob obtain the final secure key.

To prove the security of the protocol, one can either use the quantum coin method [12] or the SDP method proposed in Ref. [20]. It has been demonstrated in the latter that the SDP method provides a tighter security analysis. Interestingly, the authors of Ref. [20] also suggested that it may be useful to vary the test coherent states. In particular, the authors demonstrated that, in the case of coherent-one-way QKD, it is possible to significantly extend the key distribution distance by varying the intensity of the test coherent state in the protocol. In light of this observation, we propose the following phase-encoding QKD protocol.

III. SIX-COHERENT-STATE QKD

Here, we detail our proposed six-coherent-state protocol and illustrate one of its possible implementation schemes in Fig. 1.

Preparation.—Alice randomly prepares one of those six quantum code states $\{|\psi_z\rangle\}_{z=1}^{6}$: $|\psi_1\rangle = |\sqrt{\mu_1}\rangle_R|\sqrt{\mu_1}\rangle_S$, $|\psi_2\rangle = |\sqrt{\mu_1}\rangle_R|{-\sqrt{\mu_1}}\rangle_S$, $|\psi_3\rangle = |\sqrt{\mu_2}\rangle_R|i\sqrt{\mu_2}\rangle_S$, $|\psi_4\rangle = |\sqrt{\mu_2}\rangle_R|{-i\sqrt{\mu_2}}\rangle_S$, $|\psi_5\rangle = |\sqrt{\mu_3}\rangle_R|e^{i\theta_1}\sqrt{\mu_4}\rangle_S$, or $|\psi_6\rangle = |\sqrt{\mu_3}\rangle_R|e^{-i\theta_2}\sqrt{\mu_4}\rangle_S$, shown in Fig. 2. Then, she sends it to Bob via the quantum channel. The states $|\psi_1\rangle$ and $|\psi_2\rangle$ are used to extract keys, while the rest are used to estimate Eve's information about the secret key. In this case, the key bit is encoded in the relative phase of the signal state and reference state. Here, the intensities and phases are free parameters, which are used to optimize the secret key rate.

Measurement.—Upon receiving the state, Bob directs it to the interferometer to recover the bit information. We use positive-operator valued measures (POVMs) to describe Bob's interference operations: Bob randomly performs one of two possible POVMs denoted by $\{B_y^b\}$, where $y \in \{0, 1\}$ represents the basis choice. Taking signal loss and detection inefficiency into account, each measurement has three possible outcomes $b \in \{0, 1, \emptyset\}$, where $\emptyset$ represents the empty detection event. In the event that

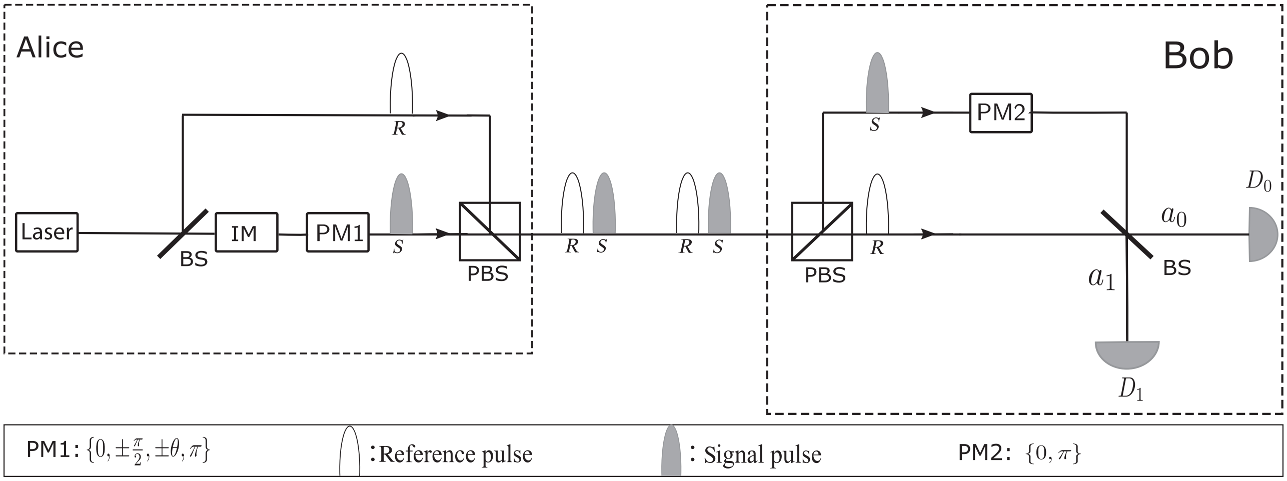


FIG. 1. Schematic of the six-coherent-state QKD protocol. The intensity modulator (IM) and phase modulator 1 (PM1) are positioned at Alice's site to prepare the intended coherent states, $|\psi_z\rangle$. As shown in the latter, the optimization suggests that all the reference pulses are the same; thus, IM and PM1 are only added in the "S" path to modulate the intensities of signal pulses. Phase modulator 2 (PM2) at Bob's site is used to randomly rotate the phase of the signal signal by 0 or π. To avoid reducing the intensities of the coherent states, we can either use the polarization multiplexing method, as shown in the figure, or deploy active optical switches.

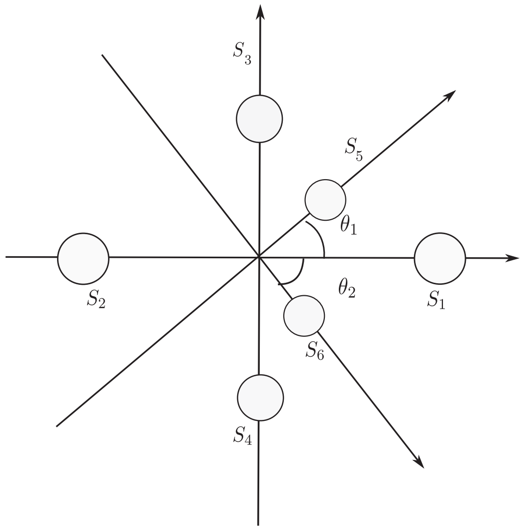


FIG. 2. Distribution of coherent states in phase space. The key basis represents the real part of the space. Here, the intensities and phases $\{\theta_1, \theta_2\}$ are given by the optimization: in fact, the optimization suggests that the optimal encoding scheme is given by $\mu_1 = \mu_2 = \mu_3$ and $\theta_1 = \theta_2 = \pi/2$.

both detectors click, Bob assigns a random bit to it. Additionally, we require that Bob's measurements satisfy the basis-independent assumption: measurement operators corresponding to detection loss are the same for both measurement settings, i.e., $B_0^{\emptyset} = B_1^{\emptyset}$. This is to ensure that the probability of detecting a signal is independent of Bob's measurement choice, which is necessary to rule out detection side-channel attacks exploiting the channel loss [27]. Thus Bob's three-outcome POVM is equivalent to a two-outcome POVM that determines the key bit, preceded by a basis-independent "filter."

Parameter estimation and key distillation.—Alice and Bob announce their basis choices through the public channel and decide if the error rates fulfill certain thresholds. If the test is successful, then Alice and Bob proceed with error correction and privacy amplification to extract a secret key.

To compute the security of the protocol, we can use a certain entropic uncertainty relation for quantum memories [28] and Fano's inequality [29]. Using these, it has been shown in Appendix C of Ref. [20] that the asymptotic secret key rate of QKD against collective attacks is

$$R_{\text{key}}^{\infty} \geq \max\{0, p_{\text{det}}[1 - h_2(e_{\text{bit}}) - h_2(e_{\text{ph}})]\}, \tag{5}$$

where e_{bit} and e_{ph} are the bit error rate and phase error rate of the key basis, p_{det} is the probability of detection in the key basis, and $h_2(\cdot)$ is the binary entropy function. The extension to general attacks is then achieved by using proof techniques like the postselection technique [30] or entropy accumulation theorem [31]. These results imply that it is sufficient to consider security against collective attacks.

A. SDP optimization problem for bounding Eve's information

From Eq. (5), we see that the secret key rate is obtained once we know the detection probability, bit error rate, and the phase error rate. To obtain these values, we first consider that Alice, Bob, and Eve share a purified tripartite state $|\Phi\rangle$ after the transmission,

$$|\Phi\rangle = \frac{|+\rangle_A|\phi_1\rangle_{BE} + |-\rangle_A|\phi_2\rangle_{BE}}{\sqrt{2}}, \tag{6}$$

where Eve's set of possible operations is considered in $|\phi_1\rangle_{BE}$ and $|\phi_2\rangle_{BE}$. Conditioned on Bob observing a successful detection, the bit error rate of the key basis is then given by

$$\begin{aligned} e_{\text{bit}} &= \frac{\langle\Phi|(|+\rangle\langle+| \otimes B_0^1 + |-\rangle\langle-| \otimes B_0^0)|\Phi\rangle}{p_{\text{det}}} \\ &= \frac{\langle\phi_1|B_0^1|\phi_1\rangle + \langle\phi_2|B_0^0|\phi_2\rangle}{2p_{\text{det}}}. \end{aligned} \tag{7}$$

The phase error rate in this case is the bit error rate that Alice and Bob observe if $|\Phi\rangle$ is measured in the $\{|+i\rangle\langle+i|, |-i\rangle\langle-i|\}$ basis by Alice and the B_1 basis by Bob. Mathematically, this is given by

$$\begin{aligned} e_{\text{ph}} &= \frac{\langle\Phi|(|+i\rangle\langle+i| \otimes B_1^0 + |-i\rangle\langle-i| \otimes B_1^1)|\Phi\rangle}{2p_{\text{det}}} \\ &= \frac{1}{2} - \text{Im}\left\{\frac{\langle\phi_1|B_1^0|\phi_2\rangle - \langle\phi_1|B_1^1|\phi_2\rangle}{2p_{\text{det}}}\right\}. \end{aligned} \tag{8}$$

One can see that p_{det} and e_{bit} are experimentally accessible, while the phase error rate e_{ph}, which is related to Eve's information about the secret bit, is not. To get a tight estimation of e_{ph}, in principle one should optimize over Eve's set of possible operations, namely, captured in the transformed states $|\phi_1\rangle_{BE}$ and $|\phi_2\rangle_{BE}$ under the constraints imposed by the expected statistics. However, as we mentioned earlier, this type of characterization problem is often intractable or impossible to solve directly.

Here, we employ the numerical tool introduced in Ref. [20] to estimate the phase error rate, which converts the initial characterization problem into a hierarchy of semidefinite programs. More specifically, each hierarchy forms a convex set that is approximated to the quantum set from outside. Importantly, by going to higher hierarchies, the approximation becomes tighter. The quantum set here means the set of measurement statistics compatible with the set of prepared quantum signals and Bob's measurements. Thus, in using this method, we can optimize over the various convex sets to bound Eve's information, which, in turn, provides a lower bound on the secret key rate of the protocol.

With this SDP method, the detailed characterization of the quantum signals and measurements, including their dimension, is no longer required in the analysis. Therefore, the transmission channel can be seen as an isometric evolution in higher dimension that takes the initial quantum signal state to some pure output signal state , which is shared between the receivers Bob and the network environment (possibly Eve). The inner product of the output states is preserved after the transmission, i.e., $\langle\phi_z|\phi'_z\rangle = \langle\psi_z|\psi'_z\rangle = \lambda_{zz'}$. In the same way, the POVMs $\{B_y^b\}$ can be assumed as projective measurements in higher dimension. Then, we say that the probabilities of observing outcomes b given setting y and z admits a quantum system, if there exist a quantum state $|\phi_z\rangle$ and operators B_y^b such that

$$p(b|y,z) = \langle\phi_z|B_y^b|\phi_z\rangle, \tag{9}$$

where the operators $\{B_y^b\}$ follow the properties:

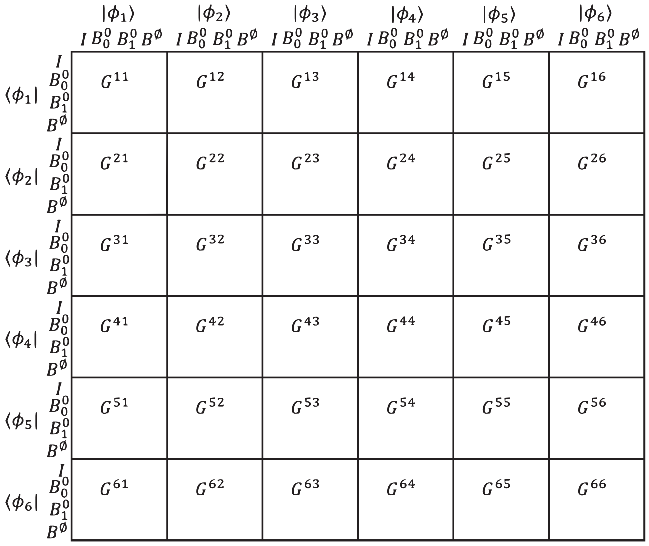
(i) for any $y, B_y^b B_y^{b'} = 0,\ \forall\, b \neq b'$,
(ii) $\Sigma_b B_y^b = \mathbb{I}$,
(iii) $(B_y^b)^2 = B_y^b = (B_y^b)^\dagger$.

A family of necessary conditions satisfied by the quantum observed probabilities thus can be introduced. Denote $\mathcal{S} = \{S_1, \ldots, S_m\}$ as a finite set of m operators, where each element is a linear combination of products of $\{B_y^b\}$. We define the $nm \times nm$ block Gram matrix G:

$$G = \Sigma_{z,z'=1}^n G^{zz'} \otimes |e_z\rangle\langle e_{z'}|,$$
$$\text{with } G_{(i,j)}^{zz'} = \langle\phi_z|S_i^\dagger \cdot S_j|\phi_{z'}\rangle, \tag{10}$$

in which $G_{(i,j)}^{zz'}$ is defined as the inner product of the vectors $\langle\phi_z|S_i^\dagger$ and $S_j|\phi_{z'}\rangle$, for all $z, z' \in [n]$, $i,j \in [m]$. $G_{(i,j)}^{zz'}$ is the ij entry of the matrix $G^{zz'}$ and $\{|e_z\rangle\}_{z=1}^n$ represents the standard orthonormal basis of $\mathbb{R}^n$. Evidently, the matrix G is Hermitian and positive semidefinite (PSD) [32] by definition.

Taking $\mathcal{S} = \{\mathbb{I}, B_0^0, B_1^0, B^\emptyset\}$, for example, the matrix G is depicted in Fig. 3. The whole matrix G is partitioned into 6×6 sub-blocks $\{G^{zz'}\}_{zz'}$ by the classifier z, where each sub-block has size 4×4 and is illustrated in Fig. 4. The entries of every sub-block $G^{zz'}$ partly reflect the properties of (i)–(iii) satisfied by the operators and the overlaps of the signal states. For instance, property (ii) implies that we can introduce the identity operator $\mathbb{I}$ and remove one of the operators. Property (i) implies $G_{2,2}^{zz'} = \langle\phi_z|B_0^0 B_0^0|\phi_{z'}\rangle = \langle\phi_z|B_0^0|\phi_{z'}\rangle$ and $G_{2,4}^{zz'} = \langle\phi_z|B_0^0 B^\emptyset|\phi_{z'}\rangle = 0$. Meanwhile, property (iii) implies $\langle\phi_z|B_y^b B_y^{b'}|\phi_z\rangle = (\langle\phi_z|B_y^{b'} B_y^b|\phi_z\rangle)^\dagger$.



	$\vert\phi_1\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$	$\vert\phi_2\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$	$\vert\phi_3\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$	$\vert\phi_4\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$	$\vert\phi_5\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$	$\vert\phi_6\rangle$ $I\ B_0^0\ B_1^0\ B^\emptyset$
$\langle\phi_1\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{11}	G^{12}	G^{13}	G^{14}	G^{15}	G^{16}
$\langle\phi_2\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{21}	G^{22}	G^{23}	G^{24}	G^{25}	G^{26}
$\langle\phi_3\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{31}	G^{32}	G^{33}	G^{34}	G^{35}	G^{36}
$\langle\phi_4\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{41}	G^{42}	G^{43}	G^{44}	G^{45}	G^{46}
$\langle\phi_5\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{51}	G^{52}	G^{53}	G^{54}	G^{55}	G^{56}
$\langle\phi_6\vert$ I B_0^0 B_1^0 $B^\emptyset$	G^{61}	G^{62}	G^{63}	G^{64}	G^{65}	G^{66}

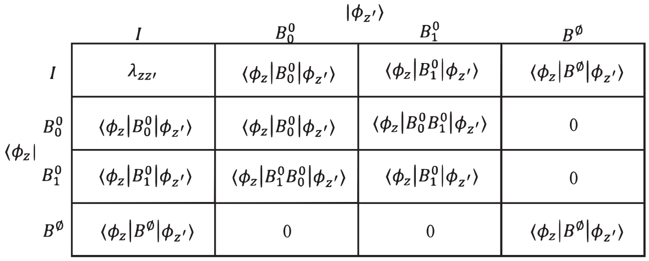
FIG. 3. The Gram matrix under six quantum states and the operator set of $\mathcal{S} = \{\mathbb{I}, B_0^0, B_1^0, B^\emptyset\}$. We assume that $B_0^\emptyset = B_1^\emptyset = B^\emptyset$. Actually, this matrix is equivalent to the Gram matrix formed by the set $\{B_0^0, B_0^1, B_1^0, B_1^1, B^\emptyset\}$, since the correlations related to B_y^1 can be represented by $\mathbb{I} - B_y^0 - B^\emptyset$. The reason we consider $\mathcal{S}$ is that it can reduce the matrix dimension.

In addition, since the overlaps of the code states are known, we have $\langle\phi_z|\mathbb{I}|\phi_{z'}\rangle = \lambda_{zz'}$.

From the definition, each set $\mathcal{S}$ of operators yields a different Gram matrix G and different linear constraints. The choice of a particular $\mathcal{S}$ may seem arbitrary, but not all operators in $\mathcal{S}$ are independent. Moreover, they can be organized in a hierarchical structure, such that $\mathcal{S}$ can be defined inductively:

$$\mathcal{S}_1 = \{\mathbb{I}, B_y^b\},$$
$$\mathcal{S}_2 = \mathcal{S}_1 \bigcup \{B_y^b B_{y'}^{b'}\},$$
$$\mathcal{S}_3 = \mathcal{S}_2 \bigcup \{B_y^b B_{y'}^{b'} B_y^b\},$$
$$\mathcal{S}_4 = \ldots \tag{11}$$

Thus, with each increase of the hierarchy, not only the dimension of the Gram matrix becomes larger, but also



		$\vert\phi_{z'}\rangle$		
	I	B_0^0	B_1^0	$B^\emptyset$
I	$\lambda_{zz'}$	$\langle\phi_z\vert B_0^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B_1^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B^\emptyset\vert\phi_{z'}\rangle$
$\langle\phi_z\vert$ B_0^0	$\langle\phi_z\vert B_0^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B_0^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B_0^0 B_1^0\vert\phi_{z'}\rangle$	0
B_1^0	$\langle\phi_z\vert B_1^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B_1^0 B_0^0\vert\phi_{z'}\rangle$	$\langle\phi_z\vert B_1^0\vert\phi_{z'}\rangle$	0
$B^\emptyset$	$\langle\phi_z\vert B^\emptyset\vert\phi_{z'}\rangle$	0	0	$\langle\phi_z\vert B^\emptyset\vert\phi_{z'}\rangle$

FIG. 4. The sub-block of the Gram matrix.

more new linear constraints are introduced. For example,

$$\begin{aligned}
\text{for } \mathcal{S}_2\text{: } &\langle\phi_z|B_0^0B_1^0|\phi_{z'}\rangle = \langle\phi_z|B_0^0\cdot B_0^0B_1^0|\phi_{z'}\rangle,\\
&\langle\phi_z|B_0^0B_1^0\cdot B_0^0|\phi_{z'}\rangle = \langle\phi_z|B_0^0\cdot B_1^0B_0^0|\phi_{z'}\rangle,\\
&\langle\phi_z|B_0^0B_1^0\cdot B_1^0B_0^0|\phi_{z'}\rangle = \langle\phi_z|B_0^0B_1^0B_0^0|\phi_{z'}\rangle,\ldots\\
\text{for } \mathcal{S}_3\text{: } &\langle\phi_z|B_0^0B_1^0\cdot B_0^0B_1^0|\phi_{z'}\rangle\\
&= \langle\phi_z|B_0^0\cdot B_1^0B_0^0B_1^0|\phi_{z'}\rangle\\
&= \langle\phi_z|B_0^0B_1^0B_0^0\cdot B_1^0|\phi_{z'}\rangle,\\
&\ \langle\phi_z|B_0^0B_1^0\cdot B_0^0B_1^0B_0^0|\phi_{z'}\rangle\\
&= \langle\phi_z|B_0^0B_1^0B_0^0\cdot B_1^0B_0^0|\phi_{z'}\rangle,\ldots
\end{aligned}$$

We denote the quantum set by $\mathsf{Q}(\lambda)$, which is formed by the probability distributions admitting a quantum system and the overlaps of the code states. Moreover, let the set of probability distributions defined by the hierarchy of step n be denoted as $\mathsf{Q}(\lambda)_n$. Then, we have that $\mathsf{Q}(\lambda) \subseteq \mathsf{Q}(\lambda)_n$. In fact, it has been demonstrated in Ref. [20] that, in the limit of n (i.e., $n \to \infty$), $\mathsf{Q}(\lambda)_n$ converges to $\mathsf{Q}(\lambda)$. Ultimately, this means that the secret key rate obtained by the SDP can only be tighter when considering higher hierarchies.

To compute Eq. (5), we thus only need to maximize e_{ph} using SDP under the condition that p_{det} and e_{bit} be fixed to some experimental model. In particular, the SDP problem for maximizing the phase error rate is

$$\begin{aligned}
\text{maximize: } & e_{\text{ph}}\\
\text{subject to: } & \langle\phi_z|\phi_{z'}\rangle = \lambda_{zz'}, \forall z, z'\\
& G \geq 0,\\
& \text{Tr}(F_k G) = p_k,\\
& \text{Tr}(R_k G) = g_k,\\
& e_{\text{bit}}, p_{\text{det}} \text{ fixed to the experimental model,}
\end{aligned} \quad (12)$$

where F_k's and R_k's are constant matrices. Note that F_k's are used to pick up the terms in G that are associated with the observed distributions $p(b|x,y)$; meanwhile, R_k's are used to pick up the terms in G, which are associated with the linear constraints induced by the quantum operators and states.

B. Numerical simulation

We simulate the secret key rate of the protocol using a realistic model, which includes total loss (including channel loss and detection efficiency), misalignment error of the optics, and the dark counts of single-photon detectors. As Bob uses two threshold detectors, there are four possible outcomes when he measures a signal. By mapping double clicks randomly into 0 or 1, Bob's measurement realizes a POVM with three outcomes: 0, 1 and inconclusive. Note that the double clicks are interpreted as key bits [12,33].

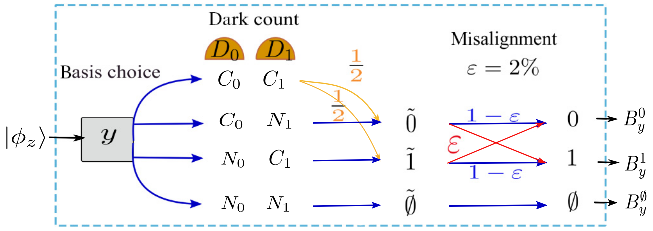


FIG. 5. Statistical model considering dark count and misalignment error, where $y \in \{0,1\}$ represents the basis choice; C_0 and C_1 (N_0 and N_1) denote the event that detection D_0 and D_1 click (do not click), respectively. The notation $\tilde{b} \in \{\tilde{0}, \tilde{1}, \tilde{\emptyset}\}$ represents the outcome without considering the misalignment error, while $b \in \{0, 1, \emptyset\}$ denotes the outcome considering the misalignment error.

In order to obtain a realistic detection model, we consider the error model illustrated in Fig. 5.

We assume that the detector dark count rate is $p_{\text{DC}} = 10^{-7}$ and misalignment error rate is $\varepsilon = 2\%$, which can be achieved with current technology [34–37].

For a given total loss $1-\eta$, the probability of detectors clicking and not clicking without misalignment error are

$$\begin{aligned}
N_j(z,y) = (1-p_{\text{DC}})\Bigg[&\frac{\langle\sqrt{\eta}\phi_z|_R + (-1)^j e^{-iy(\pi/2)}\langle\sqrt{\eta}\phi_z|_S}{\sqrt{2}}|0\rangle\\
&\langle 0|\frac{|\sqrt{\eta}\phi_z\rangle_R + (-1)^j e^{iy(\pi/2)}|\sqrt{\eta}\phi_z\rangle_S}{\sqrt{2}}\Bigg],\\
C_j(z,y) = 1 - N_j(z,y),&
\end{aligned} \quad (13)$$

where $j \in \{0,1\}$ represents detector D_0 and D_1; $y \in \{0,1\}$ is Bob's basis choice; and $|\phi_z\rangle_S$ and $|\phi_z\rangle_R$ denote the signal and reference portion of the state $|\phi_z\rangle$, respectively.

Let $T(\tilde{b},z,y)$ denote the probability of getting the outcome $\tilde{b}$. We have that

$$\begin{aligned}
T(\tilde{0},z,y) &= C_0(z,y)N_1(z,y) + \frac{C_0(z,y)C_1(z,y)}{2},\\
T(\tilde{1},z,y) &= C_1(z,y)N_0(z,y) + \frac{C_0(z,y)C_1(z,y)}{2},\\
T(\tilde{\emptyset},z,y) &= N_0(z,y)N_1(z,y).
\end{aligned} \quad (14)$$

Considering the misalignment error ε, the probabilities of B_y^b are

$$\begin{aligned}
P(0,z,y) &= (1-\varepsilon)T(\tilde{0},z,y) + \varepsilon T(\tilde{1},z,y),\\
P(1,z,y) &= (1-\varepsilon)T(\tilde{1},z,y) + \varepsilon T(\tilde{0},z,y),\\
P(\emptyset,z,y) &= T(\tilde{\emptyset},z,y).
\end{aligned} \quad (15)$$

Thus, the statistics of each POVM measurement on each coming state can be evaluated, as shown in Table I. Accordingly, the probability of detecting a signal p_{det} for

TABLE I. The statistics of each POVM for each coming state.

	B_0^0	B_0^1	$B_y^{\emptyset}$	B_1^0	B_1^1
$\vert\phi_1\rangle$	$P(0,1,0)$	$P(1,1,0)$	$P(\emptyset,1,y)$	$P(0,1,1)$	$P(1,1,1)$
$\vert\phi_2\rangle$	$P(0,2,0)$	$P(1,2,0)$	$P(\emptyset,2,y)$	$P(0,2,1)$	$P(1,2,1)$
$\vert\phi_3\rangle$	$P(0,3,0)$	$P(1,3,0)$	$P(\emptyset,3,y)$	$P(0,3,1)$	$P(1,3,1)$
$\vert\phi_4\rangle$	$P(0,4,0)$	$P(1,4,0)$	$P(\emptyset,4,y)$	$P(0,4,1)$	$P(1,4,1)$
$\vert\phi_5\rangle$	$P(0,5,0)$	$P(1,5,0)$	$P(\emptyset,5,y)$	$P(0,5,1)$	$P(1,5,1)$
$\vert\phi_6\rangle$	$P(0,6,0)$	$P(1,6,0)$	$P(\emptyset,6,y)$	$P(0,6,1)$	$P(1,6,1)$

the key basis and the corresponding bit error rate e_{bit} is then given by

$$
\begin{aligned}
p_{\text{det}} &= T(\tilde{0},1,0) + T(\tilde{1},1,0) \\
&= 1-(1-p_{\text{DC}})^2 e^{-2\eta|\alpha|^2}, \\
e_{\text{bit}} &= \frac{\varepsilon T(\tilde{0},1,0)+(1-\varepsilon)T(\tilde{1},1,0)}{p_{\text{det}}} \\
&= \frac{\frac{p_{\text{DC}}}{2}+\varepsilon(1-p_{\text{DC}})+\left(\frac{p_{\text{DC}}}{2}-\varepsilon\right)(1-p_{\text{DC}})\,e^{-2\eta|\alpha|^2}}{p_{\text{det}}}.
\end{aligned} \tag{16}
$$

Subsequently, we maximize e_{ph} over the set of compatible probabilities using the first level of the hierarchy and the results of the numerical optimization with errors (blue curve) and without errors (rose curve) are shown in Fig. 6. Here, errors mean the dark count rate and misalignment error. In the absence of errors, namely, $p_{\text{DC}} = \varepsilon = 0$, the tolerable total loss is extended to more than 55 dB, which is extremely close to the collective beam-splitting attack bound (an upper bound on the secret key rate). This suggests that the six-coherent-state QKD protocol is pretty robust against the total loss in the absence of errors. Taking into account practical errors, the tolerable total loss reaches up to 38 dB, which is significantly higher than previous BB84 coherent-state protocol results [12,20] (around 23 and 25 dB, respectively), assuming the same error model specified in Fig. 5. The BB84 coherent-state protocol in Refs. [12] and [20] is also the non-phase-randomization protocol, in which Alice only prepares the first four states of our six-coherent-protocol to send to Bob and with $\mu_1 = \mu_2$. The curves plotted in Ref. [12] are from the quantum coin method and Ref. [20] is from the SDP method. As compared with the protocol in Ref. [20], two additional test states are included in our protocol to give better characterization of the quantum system between Alice and Bob. Thus, a tighter bound on Eve's information could be obtained.

Moreover, through the optimization, we observe that the secret key rate is optimized when $\mu_1 = \mu_2 = \mu_3$ and $\theta_1 = \theta_2 = \pi/2$. This is expected since $\mu_1 = \mu_2 = \mu_3$ corresponds to larger overlaps between the six coherent states, which implies that it is more challenging for Eve to distinguish them; meanwhile, $\theta_1 = \theta_2 = \pi/2$ provides more characterization of the test basis (B_1), thus resulting in a higher secret key rate. Therefore, in practice, one only has

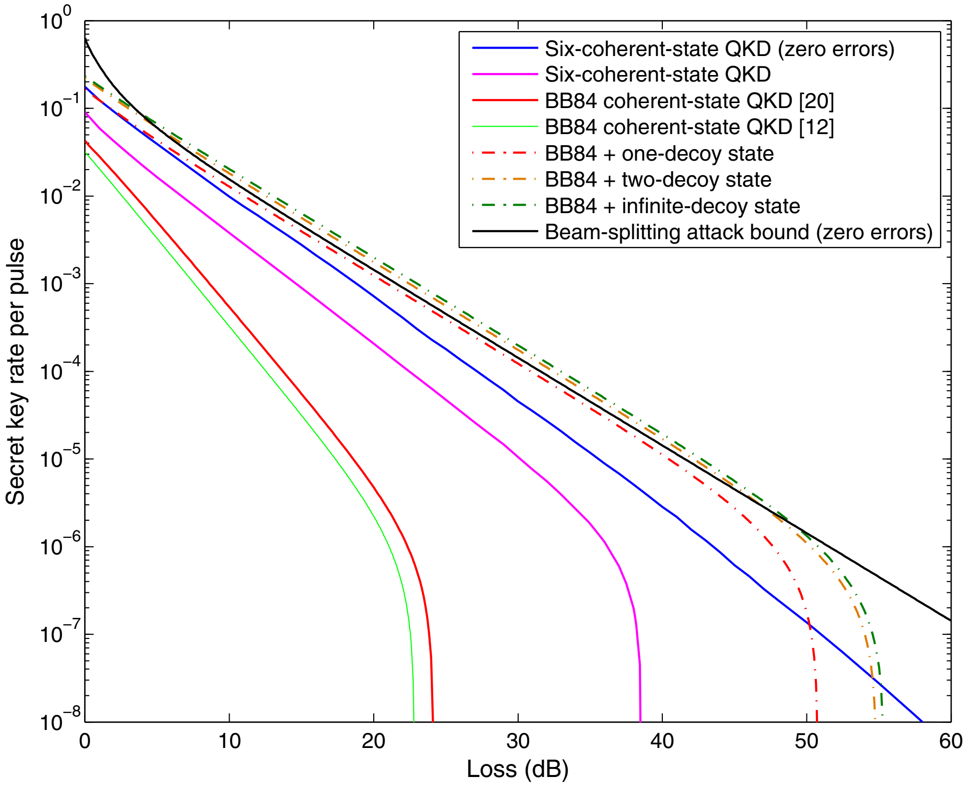


FIG. 6. For the key rate simulation, we assume a detector dark count rate of $p_{\text{DC}} = 10^{-7}$ and a misalignment error rate of $\varepsilon = 2\%$. The zero errors mean that the dark count rate and misalignment error are set to zero. The comparison is based on the same error model and same experiment parameters. The protocol of BB84 plus decoy technology we consider here comes from Ref. [34]. The one-decoy scenario of Ref. [34] and our six-coherent-state protocol both have two key states and four test states. Also, we have fewer test states compared to the two or infinite decoy states BB84 protocol. The optimization is carried out with the MATLAB package YALMIP [38] and the SDP solver SEDUMI [39].

TABLE II. The optimized intensities.

	Loss (dB)	0	10	20	30	40	50	55
Zero error	μ_1	0.23	0.09	0.08	0.07	0.04	0.03	0.02
($p_{\mathrm{DC}} = 0, \varepsilon = 0$)	μ_4	0.0005	0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
	Loss (dB)	0	10	20	30	38		
With error	μ_1	0.14	0.06	0.03	0.02	0.01		
($p_{\mathrm{DC}} = 10^{-7}, \varepsilon = 2\%$)	μ_4	0.0005	0.0005	0.0005	0.0005	0.0005		

to modulate the amplitude between two levels (μ_1 and μ_4), which makes our protocol highly practical and suitable for high-speed implementation. The optimized values of $\mu_1 = \mu_2 = \mu_3$ and μ_4 are given in Table II. These values decrease as the loss increases.

For completeness, we also plot the secret key rate, obtained using the decoy-state method, of the protocol in Ref. [34] that is based on time-bin encoding of phase-randomized coherent states. The asymptotic secret key rate is estimated using the formula given in Ref. [40], without taking into account the statistical corrections of finite-length keys. Considering the same simulation parameters (i.e., total loss, misalignment error, and dark count rate), the plot of the secret key rate against loss of the decoy-state QKD protocol is shown in Fig. 6. The comparison shows that the secret key rate of our protocol is comparable to that of the one-decoy-state protocol in the low-loss regime. Specifically, the key rates differ by only 1 order of magnitude in the region when the loss is less than 25 dB. For further comparison, we also simulate the optimized secret key rates of the BB84 protocol with two decoy states and an infinite number of decoy states, and our protocol still shows appreciable performance in the short-distance regime.

IV. CONCLUSION

In conclusion, on the one hand, phase randomization is a critical assumption made in the analysis of most coherent state QKD protocols and any deviation from preparing perfectly phase-randomized coherent states may pose serious threats of a security breach. On the other hand, existing analysis on non-phase-randomized coherent states is overly pessimistic and yields secret key rates that are inferior to alternative protocols based on the decoy-state method. In this paper, we present and analyze the security of a six-coherent-state phase-encoding QKD protocol based on non-phase-randomized coherent states. Our analysis requires fewer assumptions on both the quantum state preparation and measurement processes as it relies solely on the overlaps of the code states as well as the observed statistics. Simulating with a realistic experimental model (dark count rate of 10^{-7} and misalignment error of 2%), our protocol can tolerate a total loss of up to 38 dB, which is much higher than previous works. Moreover, we observe that the secure key rates of our protocol are comparable with the BB84 decoy-state protocol in the low loss regime. In addition to the improved key rates, our protocol only requires the modulation of six relative phases and two amplitudes, which is easy to implement. Hence, we show that one could implement coherent state QKD without performing phase randomization and yield comparable key rates with other known protocols.

We note that there are also other QKD protocols that are based on the transmission of coherent states. For example, coherent one-way (COW) and differential phase shift (DPS) protocols are two such protocols. These protocols differ from the six-coherent-state protocol in that the receiver now performs joint measurements on consecutive signals, due to the need to measure the coherence between two nonempty coherent states. However, the key rates and transmission distances of these protocols are known to be limited, especially when compared against the case with phase randomization [41–44]. For COW protocols, the key is encoded into the arrival time of the coherent signals. It has been shown that the key rate is much lower than the six-coherent-state protocol when analyzed with the same SDP method [20]. For DPS protocols, the key is encoded into the relative phases between the adjacent pulses, and read out by the coherent measurement of two adjacent pulses using an imbalanced Mach-Zehnder interferometer. The security analysis of DPS is so far restricted to nondemolition measurement or the photon number resolving and key rate is typically lower than 80 km [42–44]. It would be interesting to investigate the security DPS QKD based on the same SDP method, namely, without trusted measurements in the future.

ACKNOWLEDGMENTS

We would like to thank Hugo Zbinden and Goh Koon Tong for the valuable comments and careful reading of the manuscript. This research is supported by the National Research Foundation (Singapore), the Ministry of Education (Singapore), the National University of Singapore, the Asian Office of Aerospace Research and Development, and the National Natural Science Foundation of China (Grants No. 61572081 and No. 61672110). Li Liu kindly acknowledges support from the China Scholarship Council.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2001).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[4] H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).

[5] W. Y. Hwang, Quantum key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[6] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[7] X. B. Wang, Beating the Photon-number-splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[8] M. Dušek, M. Jahma, and N. Lütkenhaus, Unambiguous state discrimination in quantum cryptography with weak coherent states, Phys. Rev. A **62**, 022306 (2000).

[9] S. H. Sun, M. Gao, M. S. Jiang, C. Y. Li, and L. M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, Phy. Rev. A **85**, 032304 (2012).

[10] Y. L. Tang, H. L. Yin, X. Ma, C. H. F. Fung, Y. Liu, H. L. Yong, T. Y. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan, Source attack of decoy-state quantum key distribution using phase information, Phy. Rev. A **88**, 022308 (2013).

[11] H. P. Yuen, Quantum amplifiers, quantum duplicators and quantum cryptography, Quantum Semiclassic. Opt. **8**, 939 (1996).

[12] H. K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quant. Inf. Comput. **7**, 431 (2007).

[13] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Robust random number generation using steady-state emission of gain-switched laser diodes, Appl. Phys. Lett. **104**, 261112 (2014).

[14] T. Kobayashi, A. Tomita, and A. Okamoto, Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser, Phys. Rev. A **90**, 032320 (2014).

[15] Y. Zhao, B. Qi, and H. K. Lo, Experimental quantum key distribution with active phase randomization, Appl. Phys. Lett. **90**, 044106 (2007).

[16] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, Nat. Photon. **9**, 832 (2015).

[17] S. H. Sun, F. Xu, M. S. Jiang, X. C. Ma, H. K. Lo, and L. M. Liang, Effect of source tampering in the security of quantum cryptography, Phys. Rev. A **92**, 022304 (2015).

[18] Z. Cao, Z. Zhang, H. K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, New J. Phys. **17**, 053014 (2015).

[19] S. H. Sun and L. M. Liang, Experimental demonstration of an active phase randomization and monitor module for quantum key distribution, Appl. Phys. Lett. **101**, 071107 (2012).

[20] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks, npj Quantum Inf. **5**, 17 (2019).

[21] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phy. Rev. A **84**, 010302(R) (2011).

[22] J. Bowles, M. T. Quintino, and N. Brunner, Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-measure Scenario with Independent Devices, Phys. Rev. Lett. **112**, 140407 (2014).

[23] Y. K. Wang, S. J. Qin, X. Wu, F. Gao, and Q. Y. Wen, Reduced gap between observed and certified randomness for semi-device-independent protocols authors, Phys. Rev. A **92**, 052321 (2015).

[24] E. Woodhead and S. Pironio, Secrecy in Prepareand-measure Clauser-horne-shimony-holt Tests with a Qubit Bound, Phys. Rev. Lett. **115**, 150501 (2015).

[25] T. V. Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patron, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[26] D. Rusca, T. V. Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Practical self-testing quantum random number generator based on an energy bound, available on line https://arXiv.org/abs/1904.04819 (2019).

[27] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[28] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley and Sons, New York, 2006), 2nd ed.

[30] M. Christandl, R. König, and R. Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

[31] F. Dupuis, O. Fawzi, and R. Renner, Entropy accumulation, available on line https://arxiv.org/abs/1607.01796 (2016).

[32] R. A. Horn and C. R. Johnson, in *Matrix Analysis* (Cambridge Univ. Press, Cambridge, 2013), 5th ed., Chap. 7, p. 654.

[33] H. Inamori, N. Lütkenhaus, and D. Mayers, Unconditional security of practical quantum key distribution, Eur. Phys. J. D **41**, 599 (2007).

[34] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M. J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure Quantum key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[35] K. Tamaki, M. Curty, G. Kato, H. K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A. **90**, 052314 (2014).

[36] H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent Quantum key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[37] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H. K. Lo, Experimental quantum key distribution with source flaws, Phys. Rev. A **92**, 032305 (2015).

[38] J. Löfberg, in *IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508)* (IEEE, Taipei, Taiwan, 2004), p. 284.

[39] J. F. Sturm, Using SEDUMI 1.02, a MATLAB toolbox for optimization over symmetric cones, Optim. Method Softw. **11**, 625 (1999).

[40] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[41] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, Security of Distributed-phase-reference Quantum key Distribution, Phys. Rev. Lett. **109**, 260501 (2012).

[42] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature **509**, 475 (2014).

[43] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nat. Photon. **9**, 827 (2015).

[44] Y. Hatakeyama, A. Mizutani, G. Kato, N. Imoto, and K. Tamaki, Differential-phase-shift quantum-key-distribution protocol with a small number of random delays, Phys. Rev. A **95**, 042301 (2017).