Experimental quantum key distribution with source flaws

Feihu Xu, Kejin Wei, Shihan Sajeed, Sarah Kaiser, Shihai Sun, Zhiyuan Tang, Li Qian, Vadim Makarov, and Hoi-Kwong Lo

Phys. Rev. A **92**, 032305 — Published 4 September 2015

DOI: 10.1103/PhysRevA.92.032305

Experimental quantum key distribution with source flaws

Feihu Xu,[1,*] Kejin Wei,[1,2] Shihan Sajeed,[3,4] Sarah Kaiser,[3,5] Shihai Sun,[6] Zhiyuan Tang,[1] Li Qian,[1] Vadim Makarov,[3,4,5] and Hoi-Kwong Lo[1]

[1]*Centre for Quantum Information and Quantum Control (CQIQC), Dept. of Electrical & Computer Engineering and Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[2]*School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3]*Institute for Quantum Computing (IQC), University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4]*Dept. of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[5]*Dept. of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[6]*College of Science, National University of Defense Technology, Changsha 410073, P.R.China*

Decoy-state quantum key distribution (QKD) is a standard technique in current quantum cryptographic implementations. Unfortunately, existing experiments have two important drawbacks: the state preparation is assumed to be perfect without errors and the employed security proofs do not fully consider the finite-key effects for general attacks. These two drawbacks mean that existing experiments are not guaranteed to be proven to be secure in practice. Here, we perform an experiment that for the first time shows secure QKD with imperfect state preparations over long distances and achieves rigorous finite-key security bounds for decoy-state QKD against coherent attacks in the universally composable framework. We quantify the source flaws experimentally and demonstrate a QKD implementation that is tolerant to channel loss despite the source flaws. Our implementation considers more real-world problems than most previous experiments and our theory can be applied to general discrete-variable QKD systems. These features constitute a step towards secure QKD with imperfect devices.

I. INTRODUCTION

Quantum key distribution (QKD), offering information-theoretic security in communication, has aroused great interest among both scientists and engineers [1]. The most important question in QKD is its security. This fact has finally been proven based on the laws of quantum mechanics [2, 3]. However, for real-life implementations that are mainly based on attenuated laser pulses, the occasional production of multi-photons and channel loss make QKD vulnerable to various subtle attacks [4]. Fortunately, the decoy-state method [5] has solved this security issue and dramatically improved the performance of QKD with faint lasers. Several experimental groups have demonstrated that decoy-state BB84 is secure and feasible under real-world conditions [6–12]. As a result, decoy-state method has become a standard technique in many current QKD implementations [13].

Until now, however, decoy state QKD experiments [6–13] have had two important drawbacks. The first one is that in the key rate formula of all existing experiments, it is commonly assumed that the phase/polarization encoding is done *perfectly* without errors. Thus, the state preparation is assumed to be basis-independent. That is, the density matrices for the two conjugate bases are assumed to be the same. This is a highly unrealistic assumption and may mean that the key generation is actually *not* proven to be secure in previous QKD experiments [6–13].

What if we use a key rate formula that takes imperfect encodings into account? Standard Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof [3] (see also [14]) does allow one to do so. Unfortunately, GLLP formalism is very conservative in assuming that the dimensionality of the prepared states is unbounded. Then, the eavesdropper (Eve) could perform an unambiguous-state-discrimination (USD) attack [15]. Consequently, the secret key rate will be reduced substantially (e.g., a commercial system is secure below 10 km fiber only). We remark that source flaw is a serious concern in not only decoy-state BB84 but also other quantum information processing protocols [16, 17].

To address the source flaw problem, Tamaki et al. put forward a theoretical proposal – loss-tolerant protocol [18] – that outperforms GLLP analysis significantly. The loss-tolerant protocol considers a realistic situation where the dimension of the prepared states is bounded to two (which we call a *qubit assumption*). Then, it is impossible for Eve to perform the USD attack. Eve's information can be bounded from the rejected-data analysis (i.e., using the basis-mismatch events to bound the phase error rate), proposed in [19]. Nevertheless, Ref. [18] is only valid in the asymptotic limit with unlimited resources. The practicality of the loss-tolerant protocol remains unknown.

Recently, though an elegant proposal has implied that Eve's information can be bounded without monitoring signal disturbance [20], source flaw was still not considered in the theory and experiment [21]. Therefore, all previous QKD experiments ignore the source flow problem, and all papers addressing this problem are theoretical. For these reasons, up till now, the feasibility of long-distance QKD implementations with imperfect encodings has remained undemonstrated.

The second drawback in previous experiments [6–13] is

*Electronic address: feihu.xu@utoronto.ca; Present address: Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

that the finite-key security claims were made with the assumption that Eve was restricted to particular types of attacks (e.g., collective attacks). Unfortunately, such assumptions cannot be guaranteed in practice. Very recently, based on the frameworks proposed in [22, 23], Hayashi et al. and Lim et al. independently provide, for the first time, tight and rigorous security bounds against general quantum attacks (i.e., coherent attacks) for decoy-state QKD [24, 25]. Nonetheless, a QKD experiment that implements such an advanced theory has yet to be completed.

In this work, we present the first experimental realization of the loss-tolerant protocol [18] and the finite-key analysis [24]. By modifying a commercial plug&play QKD system, we experimentally show that with imperfect source encodings, it is still able to perform secure QKD over long distances. In particular, with our security analysis, we successfully generate secure keys over different channel lengths, up to 50 km telecom fibers. In contrast, not even a single bit of secure key can be extracted with GLLP security proof. We note in passing that our experiment requires only three encoding states. Thus it can simplify conventional BB84 implementations[1]. Moreover, we study how to apply the finite-key analysis of [24, 25] in real implementations. For the first time, we generate secure keys that can be secure against coherent attacks in the universally composable framework [26]. Our implementation, security analysis and parameter estimation procedure can be applied to general discrete-variable QKD systems. Our results break new ground for future QKD experiments with imperfect sources.

The rest of this paper is organized as follows. We introduce the protocol in Sec. II. In Sec. III, we present the security analysis. In Sec. IV, we present the decoy-state analysis for parameter estimation. In Sec. V, we verify the qubit assumption. In Sec. VI, we present our experimental set up and experimental results. Finally, we conclude this paper in Sec. VII.

II. PROTOCOL

The loss-tolerant protocol is a general method that works not only for the standard BB84 protocol, but even for the three-state protocol [27] where there is a strong asymmetry between the two bases. The three-state QKD runs almost the same as BB84 except that: i) Alice sends Bob only three pure states $\{|0_z\rangle, |0_x\rangle, |1_z\rangle\}$, where $|i_j\rangle$ ($i \in\{0,1\}$ and $j \in\{\mathsf{Z}, \mathsf{X}\}$) denotes the state associated with bit "i" in j basis; ii) the rejected data (i.e., the detection events when Alice and Bob use different basis) are used for the estimation of the phase error rate [19].

Here we focus on the three-state protocol and consider an asymmetric coding, where the secret key is extracted only from the events whereby Alice and Bob both choose the Z basis. To implement the loss-tolerant protocol, we extend it to a general practical setting with finite keys and finite decoy states. The concrete description of the different steps of our protocol is presented in below.

a. Transmission Alice chooses a bit value uniformly at random, selects a basis choice $\lambda \in \{\mathsf{Z}, \mathsf{X}\}$ with probabilities $P_\lambda \in \{P_\mathsf{z}, P_\mathsf{x}\}$, and an intensity choice $k \in \{\mu, \nu, \omega\}$ ($\{$signal,decoy,vacuum$\}$) with probabilities $P_k \in \{P_\mu, P_\nu, P_\omega\}$. Finally, she prepares a phase-randomized weak coherent pulse, chosen from three states $\{|0_\mathsf{z}\rangle, |0_\mathsf{x}\rangle, |1_\mathsf{z}\rangle\}$, where $|i_\lambda\rangle$ denotes the state associated with bit "i" in λ basis, and sends it to Bob via the quantum channel.

b. Detection Bob chooses a basis from $\{\mathsf{Z}, \mathsf{X}\}$ with probabilities $\{P_\mathsf{z}, P_\mathsf{x}\}$ and measures the pulses. Then, he records the detection or non-detection, his basis choice and the measured bit value (for double clicks, he assigns a random bit value).

c. Basis reconciliation Alice and Bob announce their basis and intensity choices over an authenticated public channel. Then, they decide the number of the detected pulses (gain counts) $n_{\lambda,k}$, when both Alice and Bob use basis λ for intensity k.

d. Parameter estimation First, Alice and Bob announce the bit information for all the pulses that are detected in X by Bob. Second, they compute: (i) the number of error pulses $n_{e_\mathsf{x},k}$ where both Alice and Bob use X and they obtain the disagreement bit values; (ii) the number of basis-mismatch pulses $n_{i_\mathsf{x}|j_\mathsf{z},k}$ where Bob detects the pulse in X and obtains the bit value i, given that Alice prepares bit j in Z basis. Third, according to the formulas shown in Table I, they calculate $s^{\mathrm{L}}_{\mathsf{x},0}$, $s^{\mathrm{L}}_{\mathsf{x},1}$ and $e^{\mathrm{U}}_{\mathsf{x},1}$, which are the lower bound of vacuum events, the lower bound of single-photon events, and the upper bound of the phase error rate, associated with the single-photon events in Z basis, respectively.

e. Error correction and verification Alice and Bob reveal $\mathrm{leak}_{\mathrm{EC}} = n_{\mathsf{z},\mu} f_e h(e_{\mathsf{z},\mu})$ bit of information to perform an error correction step that can correct errors for the expected quantum bit error rate (QBER) e_z (f_e is the error correction inefficiency function that is chosen as 1.16 in this paper). To ensure that they share a pair of identical keys with $\varepsilon_{\mathrm{cor}}$-correct [23], they perform an error-verification step using two-universal hash functions that publishes $\lceil \log_2 1/\varepsilon_{\mathrm{cor}} \rceil$ bits of information [28].

f. Privacy amplification Using the results from steps d and e, Alice and Bob estimate the sacrificed bit length S_{PA} (see Eq. (1)) [24, 25] and apply an universal hash function to their corrected strings to produce the final secret key of length ℓ (see Eq. (2)).

[1] For those free-space systems based on four laser diodes, one could simply keep one laser just as back-up in case certain laser fails, without any decrease in performance.

Definitions:

λ: basis-choice, $\lambda \in \{\mathsf{Z}, \mathsf{X}\}$.

k: intensity choice, $k \in \{\mu, \nu, \omega\}$ ({signal,decoy,vacuum}).

P_λ: probability choice for basis λ, $P_\lambda \in \{P_\mathsf{z}, (1-P_\mathsf{z})\}$.

P_k: probability choice for intensity k, $P_k \in \{P_\mu, P_\nu, P_\omega\}$.

δ_l: phase modulation errors for $l \in \{1,2,3\}$, see Eq.(6).

Measured quantities:

$n_{\lambda,k}$: the number of the detected pulses – both Alice and Bob use basis λ for intensity k.

$n_{e_\mathsf{x},k}$: the number of error pulses – both Alice and Bob use X for intensity k and they obtain the disagreement bit values.

$n_{i_\mathsf{x}|j_\mathsf{z},k}$: the number of basis-mismatch pulses – Bob detects the pulse in X and obtains the bit value i, given that Alice prepares bit j in Z for intensity setting k ($i,j \in \{0,1\}$).

Statistical fluctuations:

Δ: statistics [31], $\Delta(n_z,\varepsilon_1) = \sqrt{n_z/2\log(1/\varepsilon_1)}$.

$n^{\mathrm{U}}_{z,k}$: the upper bound of $n_{z,k}$, $n^{U}_{z,k} = n_{z,k} + \Delta(n_{z,k},\varepsilon_1)$.

$n^{\mathrm{L}}_{z,k}$: the lower bound of $n_{z,k}$, $n^{L}_{z,k} = n_{z,k} - \Delta(n_{z,},\varepsilon_1)$.

τ_n: n-photon-state probability, $\tau_n = \sum_{k\in\{\mu,\nu,\omega\}} P_k e^{-k} k^n/n!$.

Decoy-estimation results:

$s^{\mathrm{L}}_{z,0}$: the lower bound of vacuum events – Eq. (4).

$s^{\mathrm{L}}_{z,1}$; the lower bound of single-photon events – Eq. (5).

$e^{\mathrm{U}}_{\mathsf{x},1}$: the upper bound of the phase error rate – Eqs. (7).

TABLE I: Concrete descriptions and formulas for the parameter estimation.

III. SECURITY ANALYSIS

We first define the security criteria that we are using [29]. For some small errors, $\varepsilon_{\mathrm{cor}}, \varepsilon_{\mathrm{sec}} > 0$, we say that our protocol is $\varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}$-secure if it is $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret. The former is satisfied if the secret keys are identical except with a small probability $\varepsilon_{\mathrm{cor}}$. The latter is satisfied if $\|\rho_{\mathrm{AE}} - U_{\mathrm{A}} \otimes \rho_{\mathrm{E}}\|_1/2 \leq \varepsilon_{\mathrm{sec}}$ where ρ_{AE} is the classical-quantum state describing the joint state of $\mathbf{S}_{\mathrm{A}}$ and $\mathbf{E}$, U_{A} is the uniform mixture of all possible values of $\mathbf{S}_{\mathrm{A}}$. Importantly, this secrecy criterion guarantees that the protocol is universally composable: the pair of secret keys can be safely used in any cryptographic task [29].

The secrecy analysis is based on the framework of [23], which was extend to the case with decoy states [24]. We use the entropic uncertainty relations to establish bounds on the smooth min-entropy of the raw key conditioned on Eve's information. Conditional on passing the checks in the error-verification step, the sacrificed bit length S_{PA} [25] in privacy amplification (PA) is given by [24]

$$S_{\mathrm{PA}} = n_{z,\mu} - s^{\mathrm{L}}_{z,0} - s^{\mathrm{L}}_{z,1}[q - h\left(e^{\mathrm{U}}_{x,1}\right)] + 6\log_2\frac{26}{\varepsilon_{\mathrm{sec}}}, \quad (1)$$

where $h(x)$ is the binary entropy function, q is the maximum fidelity for states prepared in Z and X basis, which characterizes the quality of the source [23], and $\varepsilon_{\mathrm{sec}}$ is the secret level that can be guaranteed by PA (i.e., $\varepsilon_{\mathrm{sec}}$-secret [26]). $\{s^{\mathrm{L}}_{\mathsf{z},0}, s^{\mathrm{L}}_{\mathsf{z},1}, e^{\mathrm{U}}_{\mathsf{x},1}\}$ can be calculated from the measured quantities of $\{n_{\mathsf{z},k}, n_{e_\mathsf{x},k}, n_{i_\mathsf{x}|j_\mathsf{z},k}\}$, and the concrete formulas for such calculations are summarized in Sec. IV.

Finally, the $\varepsilon_{\mathrm{sec}}$-secret key length in the Z basis is given by

$$\ell \geq s^{\mathrm{L}}_{\mathsf{z},0} + s^{\mathrm{L}}_{\mathsf{z},1}[q - h\left(e^{\mathrm{U}}_{\mathsf{x},1}\right)] - \mathrm{leak}_{\mathrm{EC}} - 6\log_2\frac{26}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}, \quad (2)$$

with an overall security level $\varepsilon_{\mathrm{tot}} = \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}}$. Here, following the analysis in the Appendix B of [24], the secret level is given by

$$\varepsilon_{\mathrm{sec}} = 2\left[\alpha_2 + \alpha_3\right] + \overline{\nu} + 21\varepsilon_1. \quad (3)$$

To get the secret level given in Eq. (2), we set each error term to a common value ε, thus $\varepsilon_{\mathrm{sec}} = 26\varepsilon$.

With ℓ, the secret key rate (per optical pulse) is given by R^{L}=ℓ/N with N denoting the total number of signals (optical pulses) sent by Alice.

IV. PARAMETER ESTIMATION

Our decoy-state analysis for parameter estimation builds on [24]. Our new contribution is estimating the phase error rate $e^{\mathrm{U}}_{x,1}$ by incorporating source flaws. In decoy-state BB84, $e^{\mathrm{U}}_{x,1}$ is estimated from the counts in X basis [24]. In the loss-tolerant protocol [18], however, $e^{\mathrm{U}}_{x,1}$ is estimated from the rejected counts, i.e., considering the detection events associated with single photons when Alice and Bob use *different* bases. Moveover, our estimation focuses directly on the detection *counts* announced by Bob, which is different from previous analysis that is based on detection probabilities [5, 30]. The results are summarized in Table I.

A. Lower bounds of vacuum counts and single-photon counts

In original decoy-state method [5, 30], Alice first randomly chooses an intensity setting (signal state or decoy state) to modulate each laser pulse and then she announces her intensity choices after Bob's detections. One can imagine a *virtual* but equivalent protocol: *Alice has the ability to first send n-photon states and then she only decides on the choice of intensity after Bob has a detection.* Let $s_{z,n}$ be the number of detection counts observed by Bob given that Alice sends n-photon states in Z basis. Note that $\sum_{n=0}^{\infty} s_{z,n} = n_z$ is the total number of detections (gain counts). In the asymptotic limit with two decoy states, we have

$$\hat{n}_{z,k} = \sum_{n=0}^{\infty} P_{k|n} s_{z,n}, \ \forall k \in \{\mu,\nu,\omega\},$$

where $P_{k|n}$ is the conditional probability of choosing the intensity k given that Alice prepares an n-photon state. For finite-data size, from Hoeffding's inequality [31], the experimental measurement $n_{z,k}$ satisfies

$$|\hat{n}_{z,k} - n_{z,k}| \leq \Delta(n_z, \varepsilon_1),$$

with probability at least $1 - 2\varepsilon_1$, where $\Delta(n_z, \varepsilon_1) = \sqrt{n_z/2 \log(1/\varepsilon_1)}$ and $\hat{n}_{z,k}$ is the expected value of $n_{z,k}$. Note that our analysis considers the most *general* type of attack – joint attack – consistent with quantum memories. The above equation allows us to establish a relation between the asymptotic values and the observed statistics. Specifically,

$$\begin{aligned} \hat{n}_{z,k} &\leq n_{z,k} + \Delta(n_z, \varepsilon_1) = n^{\mathrm{U}}_{z,k}, \\ \hat{n}_{z,k} &\geq n_{z,k} - \Delta(n_z, \varepsilon_1) = n^{\mathrm{L}}_{z,k}, \end{aligned}$$

are respectively the upper and lower bound of the gain counts $n_{z,k}$ for a given intensity setting $k \in \{\mu, \nu, \omega\}$.

An analytical lower-bound on $s_{z,0}$ can be established by exploiting the structure of the conditional probabilities $P_{k|n}$ based on Bayes' rule: $P_{k|n} = \frac{P_k}{\tau_n} \frac{e^{-k} k^n}{n!}$, where $\tau_n = \sum_{k \in \{\mu,\nu,\omega\}} P_k e^{-k} k^n / n!$ is the probability that Alice prepares an n-photon state. Based on an estimation method in [30], we have

$$s^{\mathrm{L}}_{z,0} = \frac{\tau_0}{(\nu - \omega)} \left(\frac{\nu e^{\omega} n^{\mathrm{L}}_{z,\omega}}{P_\omega} - \frac{\omega e^{\nu} n^{\mathrm{U}}_{z,\nu}}{P_\nu} \right), \tag{4}$$

$$\begin{aligned} s^{\mathrm{L}}_{z,1} = \frac{\mu \tau_1}{\mu(\nu - \omega) - (\nu^2 - \omega^2)} \Bigg[& \frac{e^{\nu} n^{\mathrm{U}}_{z,\nu}}{P_\nu} - \frac{e^{\omega} n^{\mathrm{L}}_{z,\omega}}{P_\omega} \\ & + \frac{\nu^2 - \omega^2}{\mu^2} \left(\frac{s^{\mathrm{L}}_{z,0}}{\tau_0} - \frac{e^{\mu} n^{\mathrm{U}}_{z,\mu}}{P_\mu} \right) \Bigg]. \end{aligned} \tag{5}$$

$s^{\mathrm{U}}_{j_x|i_z,1}$ ($s^{\mathrm{L}}_{j_x|i_z,1}$) denotes the upper (lower) bound of single-photon events when Bob has detections associated with bit "j" in X basis, *given that* Alice sends a state of i_z with $i \in \{0, 1\}$.

$s^{\mathrm{L}}_{j_x|i_z,1}$ and $s^{\mathrm{L}}_{j_x|0_x,1}$ can be estimated equivalently by plugging $\{n^{\mathrm{L}}_{j_x|i_z,k}, n^{\mathrm{U}}_{j_x|i_z,k}\}$ and $\{n^{\mathrm{L}}_{j_x|0_x,k}, n^{\mathrm{U}}_{j_x|0_x,k}\}$ into Eqs. (4) and (5). $s^{\mathrm{U}}_{j_x|i_z,1}$ and $s^{\mathrm{U}}_{j_x|0_x,1}$ can be estimated by

$$\begin{aligned} s^{\mathrm{U}}_{j_x|i_z,1} &= \tau_1 \frac{n^{\mathrm{U}}_{j_x|i_z,\nu} - n^{\mathrm{L}}_{j_x|i_z,\omega}}{\nu - \omega}, \\ s^{\mathrm{U}}_{j_x|0_x,1} &= \tau_1 \frac{n^{\mathrm{U}}_{j_x|0_x,\nu} - n^{\mathrm{L}}_{j_x|0_x,\omega}}{\nu - \omega}. \end{aligned} \tag{11}$$

B. Upper bound of phase error rate

In the asymptotic case, we follow [18] to estimate the phase error rate. The details are shown in Appendix A. Here we extend [18] to the finite-key case.

We focus on phase encoding BB84 and assume $\{\delta_1, \delta_2, \delta_3\}$ to be Alice's phase modulation errors for $\{\pi/2, \pi, 3\pi/2\}$, thus the four BB84 imperfect states sent by Alice are given by

$$\begin{aligned} |\phi_{0_z}\rangle &= |0_z\rangle \\ |\phi_{1_z}\rangle &= \sin\delta_2 |0_z\rangle + \cos\delta_2 |1_z\rangle \\ |\phi_{0_x}\rangle &= \cos\delta_1 |0_x\rangle + \sin\delta_1 |1_x\rangle \\ |\phi_{1_x}\rangle &= \sin\delta_3 |0_x\rangle + \cos\delta_3 |1_x\rangle. \end{aligned} \tag{6}$$

After considering the finite-data analysis, $e^U_{x,1}$ is given by

$$e^{\mathrm{U}}_{x,1} = \frac{s^{vir,\mathrm{U}}_{0_x|1_x,1} + s^{vir,\mathrm{U}}_{1_x|0_x,1}}{s^{vir,\mathrm{L}}_{0_x|0_x,1} + s^{vir,\mathrm{L}}_{0_x|1_x,1} + s^{vir,\mathrm{L}}_{1_x|0_x,1} + s^{vir,\mathrm{L}}_{1_x|1_x,1}}. \tag{7}$$

Here

$$\begin{bmatrix} P_z s^{vir,\mathrm{U}}_{0_x|j_x,1} \\ P_z s^{vir,\mathrm{U}}_{1_x|j_x,1} \end{bmatrix} = B \times A^{-1} \begin{bmatrix} 2P_x s^{\mathrm{U}}_{j_x|0_z,1} \\ 2P_x s^{\mathrm{U}}_{j_x|1_z,1} \\ P_z s^{\mathrm{U}}_{j_x|0_x,1} \end{bmatrix}, \tag{8}$$

$$\begin{bmatrix} P_z s^{vir,\mathrm{L}}_{0_x|j_x,1} \\ P_z s^{vir,\mathrm{L}}_{1_x|j_x,1} \end{bmatrix} = B \times A^{-1} \begin{bmatrix} 2P_x s^{\mathrm{L}}_{j_x|0_z,1} \\ 2P_x s^{\mathrm{L}}_{j_x|1_z,1} \\ P_z s^{\mathrm{L}}_{j_x|0_x,1} \end{bmatrix}, \tag{9}$$

where P_z and P_x are the probabilities that Alice and Bob choose Z and X basis, $j \in \{0, 1\}$ and A and B are given by

$$\begin{aligned} A &= \begin{bmatrix} 1 & 1 & 0 \\ 1 & -\cos(2\delta_2) & \sin(2\delta_2) \\ 1 & \sin(2\delta_1) & \cos(2\delta_1) \end{bmatrix} \\ B &= \frac{1}{12} \begin{bmatrix} (1 + \sin\delta_2) & \sin\delta_2(1 + \sin\delta_2) & \cos\delta_2(1 + \sin\delta_2) \\ (1 - \sin\delta_2) & -\sin\delta_2(1 - \sin\delta_2) & -\cos\delta_2(1 - \sin\delta_2) \end{bmatrix}. \end{aligned} \tag{10}$$

λ	e_d	η_{Bob}	Y_0	f
1551.71 nm	2.35%	5.05%	4.01×10^{-5}	5 MHz

TABLE II: Parameters measured in ID-500 commercial QKD system, including laser wavelength λ, optical misalignment error e_d (the probability that a photon hits the erroneous detector), Bob's overall quantum efficiency η_{Bob}, dark count rate per pulse Y_0 for each detector and system repetition rate f.

V. VERIFYING QUBIT ASSUMPTION

The qubit assumption is normally required in the security proofs [1, 2] to simplify the analysis. With the qubit assumption, using large deviation techniques (e.g. quantum de Finetti theorem), one can show that effectively Eve can apply only the same super-operator on each transmitted qubit. This greatly simplifies the security proofs. In practice, however, *no* previous works have verified this assumption in practice. Note that a specific attack to exploit the higher dimensionality of state preparation has been proposed in [32]. Here we perform a comprehensive analysis to theoretically verify the qubit assumption (with high accuracy) in a practical QKD system, even with device imperfections. These results are shown in Appendix D.

VI. EXPERIMENT

We implement the protocol, presented in Sec. II, with a modified commercial ID-500 plug&play QKD system, manufactured by ID Quantique (see Fig. 1) [33, 34]. Nonetheless, we remark that our methods of parameter optimizations, finite key analysis, the quantification of phase modulation errors and the implementation can also be applied to standard QKD systems. Here, we use the plug&play QKD system simply as an example to illustrate our *general* methods.

A. Setup

The initial plug&play system employs the phase-coding QKD scheme and it works as follows (see Fig. 1) [34]. Bob first sends two laser pulses (i.e., signal and reference pulse) to Alice. Alice uses the reference pulse as a synchronization signal (detected by her classical photo-detector) to activate her phase modulator (PM). Then Alice modulates the phase of the signal pulse only, attenuates the two pulses to single photon level, and sends them back to Bob. Bob randomly chooses his measurement basis by modulating the phase of the returning reference pulse and detects the interference signals with his two single-photon detectors (SPDs).

Our modifications on top of ID-500 are as follows. To implement the decoy-state protocol, we add two acousto-optic modulators (AOMs, Brimrose) to achieve polarization-insensitive intensity modulation. AOM_1 – driven by a waveform with random patten generated from a function generator (FG_1, Agilent 88250A) – is used for the decoy modulation, while AOM_2 – driven by a fixed waveform generated from FG_2 – is used to compensate the phase shift caused by the frequency shift of the AOM [6]. To implement the three-state protocol, we adopt another FG, i.e., FG_3 in Fig. 1, to control Alice's phase modulator (PM). FG_1 and FG_3 are loaded with random numbers generated from a quantum random number generator [35]. We have measured the system parameters as shown in Table II.

B. Quantifying modulation error

System	θ	$D_{1,\theta}$	$D_{2,\theta}$	$\bar{\delta}_\theta$
ID-500	0	630	867678	-
	$\pi/2$	456735	444336	0.013
	π	856245	4744	0.134
	$3\pi/2$	464160	436962	0.030
Clavis2	0	727	1075320	-
	$\pi/2$	546724	527735	0.023
	π	1111574	6990	0.145
	$3\pi/2$	566813	531417	0.037

TABLE III: Raw counts and modulation errors for Alice's phase modulator in ID-500 and Clavis2 commercial plug&play systems. $D_{1,\theta}$ ($D_{2,\theta}$) represents the detections counts of SPD_1 (SPD_2). $\bar{\delta}_\theta$, given by Eq. (12), is the upper bound of modulation error for a given phase θ.

We quantify the modulation error δ_θ in the source through calibrating Alice's PM, a LiNbO_3 waveguide based electro-optical modulator, on two plug&play QKD systems – ID 500 and Clavis2 [34]. δ_θ is defined as the difference between the actual phase and the expected phase $\theta \in \{0, \pi/2, \pi\ 3\pi/2\}$. We find that in ID-500, the voltages $\{0, 0.30V_m, 0.62V_m, 0.92V_m\}$ modulate the expected phases $\{0, \pi/2, \pi\ 3\pi/2\}$, where $V_m \approx 3.67$ V is a maximal value allowed on Alice's PM. The calibration process is as follows. Alice is directly connected to Bob with a short fiber (about 1 m), Alice scans the voltages applied to her PM, Bob sets his own PM at a fixed unmodulated phase $\{0\}$ and records the detection counts of his two SPDs. These counts are denoted by $D_{1,\theta}$ and $D_{2,\theta}$. The detections counts on ID-500 and Clavis2 are shown in Table III.

In ID-500, to quantify δ_θ, we first determine the detector efficiencies (η_{d1}, η_{d2}) and the dark count rates ($Y_{0,d1}$, $Y_{0,d2}$) for Bob's two SPDs and find that $\eta_{d1} = 5.05\%$ and $\eta_{d2} = 4.99\%$ and $Y_{0,d1} \approx Y_{0,d2} = 4.01 \times 10^{-5}$. In Table III, $D_{1,0}$ quantifies the amount of global misalignment between Alice and Bob (i.e. the summation of the dark counts and the imperfect visibility). This global misalignment can increase QBER, but it is irrelevant to bound Eve's information in the loss-tolerant protocol [18]. Only the relative orientation between the three states prepared by Alice quantifies the source flaws that can be potentially exploited by Eve. Hence, we subtract $D_{1,0}$ in the quantification of δ_θ. In our analysis of the statistics, we use Hoeffding's inequality [31] to guarantee the definition of

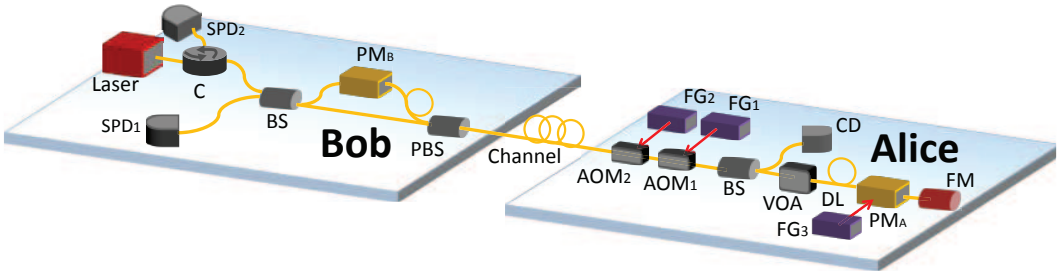

FIG. 1: (Color online) Experimental setup. SPD_1/SPD_2, single-photon detector; C, circulator; PM_A/PM_B, phase modulator; BS, beam splitter; PBS, polarization beam splitter; CD, classical photo-detector; VOA, variable optical attenuator; AOM_1/AOM_2, acousto-optic modulator; FG, function generator; DL, delay line; FM, Faraday mirror. PM_A randomly selects a phase from $\{0, \pi/2, \pi\}$ for the three-state modulations. AOM_1 randomly modulates the intensity of each pulse to be either signal state level or decoy state level, while AOM_2 compensates the phase shift due to AOM_1.

composable security. The upper bound of δ_θ is given by:

$$\delta_\theta \leq \bar{\delta}_\theta = |\theta - 2\arctan(\sqrt{\frac{((D_{1,\theta}+\Delta(D_{1,\theta},\varepsilon))-(D_{1,0}-\Delta(D_{1,0},\varepsilon)))/\eta_{d1}}{((D_{2,\theta}-\Delta(D_{2,\theta},\varepsilon))-(D_{1,0}+\Delta(D_{1,0},\varepsilon)))/\eta_{d2}}})|, \tag{12}$$

where $\Delta(D_{i,\theta},\varepsilon)$=$\sqrt{D_{i,\theta}/2\log(1/\varepsilon)}$ (with $i \in \{0,1\}$) [31]. In general, if $Y_{0,d1} \neq Y_{0,d2}$ in a practical system, in Eq. (12), we can use $D_{i,\theta}$ to subtract the dark counts of detector d_i. Here, we choose a failure probability $\varepsilon = 10^{-10}$ (i.e. a confidence level $1 - 2 \times 10^{-10}$). The upper bounds of δ_θ are shown in Table III. From this table, the error δ in ID-500 is upper bounded by the case of δ_π, i.e., $\delta \leq \bar{\delta}_\pi = 0.134$.

Using the same method for Clavis2, we find that δ is upper bounded by $\delta \leq \bar{\delta}_\pi = 0.145$. Notice that δ can also be estimated using the interference visibility or the extinction ratio of the PM [36]. In a system with an advanced phase-stabilized interferometer [37], the value of $\delta \leq 0.062$ corresponds to about 99.9% visibility or 30 dB extinction ratio.

C. Numerical evaluation

With δ_θ and the parameters in Table II, Fig. 2 shows the simulation results, where we choose the total number of pulses N=5 $\times$ 10^{10} and the security level ε_{tot}=10^{-10}. We use the model, proposed in [30], to simulate the virtual data. For comparison, this figure also includes the key rate for the decoy-state BB84 based on the GLLP security analysis (See Sec. I of SM for the model). The power of our security analysis is explicitly shown by the fact that GLLP delivers a key rate that decreases rapidly when δ increases. The maximal tolerant distance is about 9 km for our QKD system. Our security analysis, however, can substantially outperform GLLP. Our QKD set up can be made secure over 60 km and the secure key rate is almost the same as the case without source flaws. Using simulation, we also determine the implementation parameters

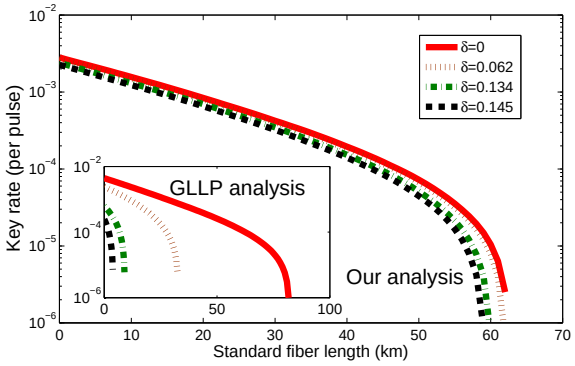

FIG. 2: (Color online) Practical key rates with parameters of Table II, N=5 $\times$ 10^{10} and ε_{tot}=10^{-10}. The main figure is for our analysis, while the inset figure is for the decoy-state BB84 with the GLLP security analysis. With GLLP, the maximal distance for our ID-500 system is about 9 km (green dashed-dotted curve in the inserted figure). In contrast, our analysis can substantially outperform GLLP in that the ID-500 system can be made secure over 60 km and the secure key rate is almost the same as the case without considering source flaws (i.e., assuming δ=0).

to achieve the optimal system performance. The optimized parameters are shown in Table IV.

D. Experimental results

In our demonstration, we implement the loss-tolerant protocol in the finite-key regime over standard fibre lengths (L)

Channel		Parameters						Estimation			Performance		
L (km)	Attn (dB)	N	μ	ν	P_μ	P_ν	P_z	$s^L_{\mathsf{z},0}$	$s^\mathrm{L}_{\mathsf{z},1}$	$e^\mathrm{U}_{\mathsf{x},1}$	$e_{\mathsf{z},\mu}$	l	R^L
5	1.4	7.84×10^{9}	0.41	0.05	0.64	0.27	0.70	7.40×10^{4}	3.02×10^{7}	6.28%	2.67%	1.06×10^{7}	1.40×10^{-3}
20	4.5	7.84×10^{9}	0.37	0.06	0.40	0.50	0.60	6.15×10^{4}	6.58×10^{6}	8.67%	2.74%	8.07×10^{5}	1.03×10^{-4}
50	10.5	5.23×10^{10}	0.55	0.06	0.74	0.18	0.50	3.36×10^{5}	1.33×10^{7}	8.46%	2.98%	1.07×10^{6}	2.14×10^{-5}

TABLE IV: **Implementation parameters and experimental results.** N is the total number of pulses sent by Alice. P_μ, P_ν are the probabilities to choose different intensities. P_z is the probability to choose the Z basis. ω equals about 0.001 for 5 and 50 km experiments, and it equals about 0.003 for 20 km experiment. The estimation results are obtained by plugging the experimental counts into the decoy-state estimation equations (see Table I). The key rate is obtained from Eq. (2).

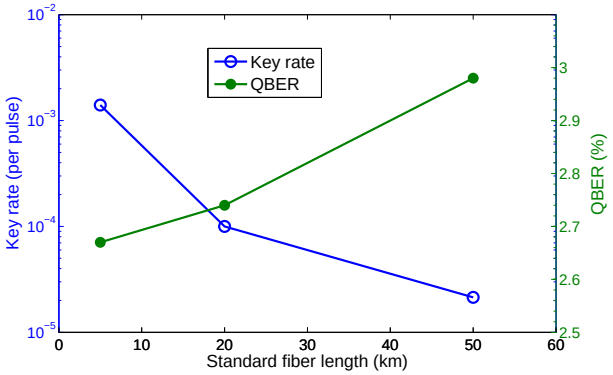

FIG. 3: (Color online) Experimental secret key rates (blue circle) and QBERs (green dot) over fibre lengths of 5, 20 and 50 km.

of 5, 20 and 50 km. In the 5 and 20 km experiments, we performed a real decoy-state QKD implementation with optimized parameters. We use FG1 to randomly modulate the signal and decoy states and use FG3 to randomly modulate the three states of $\{|0_z\rangle, |0_x\rangle, |1_z\rangle\}$. In the 50 km experiment, we removed the two AOMs due to their high loss (over 3 dB each) and used the VOA in Alice to modulate the decoy intensities for a proof of concept decoy-state modulation.

Our measurement and post-processing are different from previous experiments in that we directly measure the detection *counts* instead of the so-called gains (i.e., probabilities) [6–12], and we also record the basis-mismatch counts. In the 5 km and 20 km experiments, we chose to operate the system for a few hours and collected about 75 sets of data, with each set of about 104.5 million pulses, which corresponds to a total number of pulses $N = 7.84\times10^{9}$. In the 50 km experiment, we collected about 500 sets of data and sent a total number of $N = 5.23\times10^{10}$ pulses. The details of the experimental counts are shown in Appendix C.

In our analysis of experimental data, we consider a security level $\varepsilon_{tot} = 10^{-10}$. With δ_θ, we find that $q = 0.79$. By plugging the experimental counts into the decoy-state estimations and using Eq. (2), we obtain the experimental results listed in Table IV and Fig. 3. The system's QBER is below 3%. Based on the loss-tolerant analysis, a secure key rate (per optical pulse) of 1.40×10^{-3} was generated at 5 km, while at 50 km it was 2.14×10^{-5}. Given the 5 MHz repetition rate, the key rates per second are 7 kbps and 107 bps respectively. Over 1 kilobit of unconditionally secure keys are exchanged between Alice and Bob. The security of these keys considers source flaws and satisfies the composable security definition, and it can withstand general attacks by Eve. With state-of-the-art high speed QKD system working at GHz repetition rate, our loss-tolerant analysis can easily enable a key rate of megabit per second.

As a comparison to previous security analysis (e.g., GLLP [3]), with the source flaw δ=0.134, no matter how many decoy states we choose or how large the data size we use, the key generation rate will hit zero at only about 10 km. That is, at 20 km and 50 km, using previous GLLP security proof, not even a single bit could be shared between Alice and Bob with guaranteed security. This means that if considering source flaws in previous long-distance decoy-state experiments [6–13], the key generation might *not* be proven to be secure. In contrast, our analysis can easily achieve high secure key generation rate over long distances even in the presence of source flaws.

VII. CONCLUSION:

We have demonstrated decoy-state QKD with imperfect state preparations and employed tight finite-key security bounds with composable security against coherent attacks. Our experiment demonstrates that the perfect state-preparation assumption can be removed, and it is still able to perform QKD over long distances. In our paper, we ignore certain imperfections in the source such as the intensity fluctuations of signal/decoy states, which have a small effect and can be taken care of using previous result [25]. Moreover, it will be interesting to consider the source flaw problem in the new protocol of [20]. Future research can also combine our results with measurement-device-independent QKD [16] to remove the security loopholes both in the source and in the detectors.

Acknowledgments

We thank O. Bedroya, M. Curty, M. Jiang, C. Lim, N. Lütkenhaus, M. Legré, X Ma, G. Ribordy, and particularly M. Lucamarini and K. Tamaki, for valuable discussions. Support from NSERC, the CRC program, Connaught Innovation fund, Industry Canada, the OGS Visa award, Air Force Office of Scientific Research (AFOSR), CryptoWorks21, US Of-

fice of Naval Research, Mike & Ophelia Lazaridis Fellowship, the National Natural Science Foundation of China (Grant No. 61178010 and No. 11304391) and the China Scholarship Council (No. 201406470051) is gratefully acknowledged.

Notes added: After posting an earlier version of our work [38], we noticed a paper, which addresses the finite-key effect of the loss-tolerant protocol [39]. In contrast to our present manuscript, that paper is strictly theoretical.

Appendix A: Phase error rate in the asymptotic case

We follow [18] to estimate the phase error rate. To make our paper self-contained, we presented the main results from [18] in this section. For simplicity, we consider three pure states, described in Eq. (6). The density matrices for the three states $|\phi_{0_z}\rangle$, $|\phi_{1_z}\rangle$, $|\phi_{0_x}\rangle$, are:

$$\rho_{0_z} = |\phi_{0_z}\rangle\langle\phi_{0_z}| = (I+\sigma_z)/2, \tag{A1}$$

$$\begin{aligned}\rho_{1_z} = |\phi_{1_z}\rangle\langle\phi_{1_z}| &= \begin{bmatrix} \sin^2\delta_2 & \sin\delta_2\cos\delta_2 \\ \sin\delta_2\cos\delta_2 & \cos^2\delta_2 \end{bmatrix} \\ &= \frac{1}{2}I - \frac{1}{2}\cos(2\delta_2)\sigma_z + \frac{1}{2}\sin(2\delta_2)\sigma_x,\end{aligned} \tag{A2}$$

$$\begin{aligned}\rho_{0_x} = |\phi_{0_x}\rangle\langle\phi_{0_x}| &= \frac{1}{2}\begin{bmatrix} 1+\sin(2\delta_1) & \cos(2\delta_1) \\ \cos(2\delta_1) & 1-\sin(2\delta_1) \end{bmatrix} \\ &= \frac{1}{2}I + \frac{1}{2}\sin(2\delta_1)\sigma_z + \frac{1}{2}\cos(2\delta_1)\sigma_x,\end{aligned} \tag{A3}$$

Here $\sigma_{x,y,z}$ denote Pauli matrices and I is identity matrix. The equivalent entanglement states between Alice and Bob are [18]

$$\begin{aligned}|\Psi_z\rangle &= (|0_z\rangle|\phi_{0_z}\rangle + |1_z\rangle|\phi_{1_z}\rangle)/\sqrt{2} \\ |\Psi_x\rangle &= |0_x\rangle|\phi_{0_x}\rangle.\end{aligned} \tag{A4}$$

Let $Y^{\omega}_{s_\beta,j_\alpha}$ with $\omega \in \{Z,X\}$ and $s,j \in \{0,1\}$ denote the joint probability that Alice (Bob) obtains a bit value j (s) conditional on the state preparation of $|\Psi_\omega\rangle$ and her (his) basis choice α (β), then the joint probabilities for different states are [18]:

$$\begin{aligned}Y^z_{s_x,0_z} &= \frac{2}{6}Tr[D_{sx}\sigma^z_{B,0_z}] = \frac{1}{6}Tr[D_{sx}\rho_{0_z}] \\ &= (q_{s_x|I} + q_{s_x|z})/6,\end{aligned} \tag{A5}$$

where $\sigma^z_{B,0_z} = Tr_A[|0_z\rangle\langle 0_z| \otimes I|\Psi_z\rangle\langle\Psi_z|] = \frac{1}{2}|\phi_{0_z}\rangle\langle\phi_{0_z}|$, and $q_{s_x|(I,x,z)} = Tr[D_{s_x}\sigma_{I,x,z}]/2$;

$$\begin{aligned}Y^z_{s_x,1_z} &= \frac{2}{6}Tr[D_{sx}\sigma^z_{B,1_z}] = \frac{1}{6}Tr[D_{sx}\rho_{1_z}] \\ &= [q_{s_x|I} - \cos(2\delta_2)q_{s_x|z} + \sin(2\delta_2)q_{s_x|x}]/6,\end{aligned} \tag{A6}$$

where $\sigma^z_{B,1_z} = Tr_A[|1_z\rangle\langle 1_z| \otimes I|\Psi_z\rangle\langle\Psi_z|] = \frac{1}{2}|\phi_{1_z}\rangle\langle\phi_{1_z}|$;

$$\begin{aligned}Y^x_{s_x,0_x} &= \frac{1}{6}Tr[D_{sx}\sigma^x_{B,0_x}] = \frac{1}{6}Tr[D_{sx}\rho_{0_x}] \\ &= [q_{s_x|I} + \sin(2\delta_1)q_{s_x|z} + \cos(2\delta_1)q_{s_x|x}]/6,\end{aligned} \tag{A7}$$

where $\sigma^x_{B,0_x} = Tr_A[|0_x\rangle\langle 0_x| \otimes I|\Psi_x\rangle\langle\Psi_x|] = \frac{1}{2}|\phi_{0_x}\rangle\langle\phi_{0_x}|$.

Eqs. (A5)-(A7) can be rewritten as

$$\begin{aligned}\begin{bmatrix} Y^z_{s_x,0_z} \\ Y^z_{s_x,1_z} \\ Y^x_{s_x,0_x} \end{bmatrix} &= \frac{1}{6}\begin{bmatrix} Y^z_{s_x|0_z} \\ Y^z_{s_x|1_z} \\ Y^x_{s_x|0_x} \end{bmatrix} = \frac{1}{6}\begin{bmatrix} 1 & 1 & 0 \\ 1 & -\cos(2\delta_2) & \sin(2\delta_2) \\ 1 & \sin(2\delta_1) & \cos(2\delta_1) \end{bmatrix}\begin{bmatrix} q_{s_x|I} \\ q_{s_x|z} \\ q_{s_x|x} \end{bmatrix} \\ &\equiv \frac{1}{6}A\begin{bmatrix} q_{s_x|I} \\ q_{s_x|z} \\ q_{s_x|x} \end{bmatrix}.\end{aligned} \tag{A8}$$

Here $Y^z_{s_x|0_z}$ denotes the conditional probability that Bob obtains bit s in basis x given that Alice sends 0_z. The same definition is applied to $Y^z_{s_x|1_z}$ and $Y^x_{s_x|0_x}$. Note that all these quantities can be measured *directly* in experiment.

To estimate the phase error rate, we consider a *virtual* protocol: Alice first prepares $|\Psi_z\rangle$ and then both Alice and Bob measure systems A and B in the X basis [18]. The joint probabilities of the virtual states $Y^{z,vir}_{s_x,j_x}$ are:

$$\begin{aligned}Y^{z,vir}_{s_x,0_x} &= \frac{1}{12}Tr[D_{s_x}\sigma^{z,vir}_{B,0_x}] = \frac{1}{3}[(1+\sin\delta_2)q_{s_x|I} + \sin\delta_2(1+\sin\delta_2)q_{s_x|x} + \cos\delta_2(1+\sin\delta_2)q_{s_x|x}], \\ Y^{z,vir}_{s_x,1_x} &= \frac{1}{12}Tr[D_{s_x}\sigma^{z,vir}_{B,1_x}] = \frac{1}{3}[(1-\sin\delta_2)q_{s_x|I} - \sin\delta_2(1-\sin\delta_2)q_{s_x|x} - \cos\delta_2(1-\sin\delta_2)q_{s_x|x}].\end{aligned} \tag{A9}$$

Eq. (A9) can be rewritten as

$$\begin{bmatrix} Y^{z,vir}_{s_x,0_x} \\ Y^{z,vir}_{s_x,1_x} \end{bmatrix} = \frac{1}{12} \begin{bmatrix} (1+\sin\delta_2) & \sin\delta_2(1+\sin\delta_2) & \cos\delta_2(1+\sin\delta_2) \\ (1-\sin\delta_2) & -\sin\delta_2(1-\sin\delta_2) & -\cos\delta_2(1-\sin\delta_2) \end{bmatrix} \begin{bmatrix} q_{s_x|I} \\ q_{s_x|z} \\ q_{s_x|x} \end{bmatrix} \equiv B \begin{bmatrix} q_{s_x|I} \\ q_{s_x|z} \\ q_{s_x|x} \end{bmatrix}. \tag{A10}$$

Combining it with Eq. (A8), we can obtain the rate of virtual states based on experimental results, which is

$$\begin{bmatrix} Y^{z,vir}_{s_x,0_x} \\ Y^{z,vir}_{s_x,1_x} \end{bmatrix} = B \times A^{-1} \begin{bmatrix} Y^{z}_{s_x|0_z} \\ Y^{z}_{s_x|1_z} \\ Y^{x}_{s_x|0_x} \end{bmatrix}. \tag{A11}$$

Finally the phase error can be estimated by

$$e_x = \frac{Y^{z,vir}_{1_x,0_x} + Y^{z,vir}_{0_x,1_x}}{Y^{z,vir}_{0_x,0_x} + Y^{z,vir}_{1_x,0_x} + Y^{z,vir}_{0_x,1_x} + Y^{z,vir}_{1_x,1_x}}. \tag{A12}$$

The extended result of Eq. (A12) for the finite-data case is presented in Eq. (4) of the main text.

Appendix B: GLLP security analysis with source flaws

We discuss the standard GLLP security analysis for BB84 with source flaws [3, 36], which is used for our simulation of Fig. 2.

Based on GLLP for imperfect sources, the ε_{sec}-secret key length is similar to the key formula (i.e. Eqn. (1)) in main-text, except for the phase error rate, which includes the correction due to basis-dependent flaws and is revised to [3]

$$\bar{e}^U_{x,1} \leq e^U_{x,1} + 4\Delta' + 4\sqrt{\Delta' e^U_{x,1}} + \epsilon_{ph} \tag{B1}$$

Here, Δ', called the balance of a quantum coin [3, 36], quantifies the basis-dependent flaws of Alice signals associated with single-photon events. Δ' is given by [3]

$$\begin{aligned} \Delta' &\leq \frac{\Delta}{Y_1} \\ \Delta &= \frac{1 - F(\rho_z, \rho_x)}{2} \end{aligned} \tag{B2}$$

where Y_1 (typically called the yield of single photons [5, 30]) is the frequency of successful detections associated with single-photons; $F(\rho_z, \rho_x)$ is the fidelity of the density matrices for the Z and X basis. Using Eq. (6), we can easily calculate $F(\rho_z, \rho_x)$ given $\{\delta_1, \delta_2, \delta_3\}$. In our QKD system, with $\{\delta_1, \delta_2, \delta_3\}$ upper bounded by 0.127, we have $F(\rho_z, \rho_x)$=$1-1.9\times10^{-3}$. So, from Eq. (B2), Δ=9.45×10^{-4}.

In GLLP analysis, the imperfect fidelity $F(\rho_z, \rho_x)$ can in principle be enhanced by Eve via exploiting the channel loss, which is clearly shown in Eq. (B2), i.e., Δ is enhanced to Δ'. Combined with the decoy-state estimations discussed in [24], we can derive the key length and obtain the inset curves in Fig. 2.

Appendix C: Experimental counts

In Table V, we list the raw experimental counts for each distance. Note that, in the experiment results,

$$\begin{aligned} n_{1_x|0_x,k} &= n_{e_x,k}, \\ n_{0_x|0_x,k} &= n_{x,k} - n_{e_x,k}. \end{aligned}$$

In the 5 and 20 km experiments, we collected about 75 sets of data, with each set of about 104.5 million pulses sent out by Alice. This corresponds to a total number of pulses $N = 7.84\times10^9$. In the 50 km experiment, we collected about 500 sets of data and sent a total number of $N = 5.23\times10^{10}$ pulses. The experimental gain counts ($n_{z,k}$, $n_{x,k}$), error counts ($n_{e_z,k}$, $n_{e_x,k}$) and rejected counts ($n_{0_x|z,k}$, $n_{1_x|z,k}$) are listed in the Table.

Appendix D: Qubit assumption and its verification

We verify the qubit assumption, i.e., that the four BB84 states remain in two dimensions. This assumption is commonly made in various QKD protocols including decoy-state BB84 and MDI-QKD. We focus on a standard *one-way phase-encoding* system, which has been widely implemented in experiments [7, 10–12]. In this system, $LiNbO_3$ waveguide-based phase modulator (PM) is commonly used to encode/decode phase information. Fig. 4 illustrates the schematic of such PM [40]. For commercial products, see [41]. To guarantee the qubit assumption, Alice's PM is supposed to have the same timing, spectral, spatial and polarization mode information for different BB84 states. We find that timing and spatial information can be easily guaranteed without any additional devices, while spectral and polarization information can also be guaranteed with standard low-cost optical devices such as wavelength filter and polarizer. Therefore, based on standard devices, we can verify the qubit assumption with high accuracy. We remark that our method serves as a specific example to practically verify the qubit assumption. In future, it will be interesting to work towards constructing a more general theory on the verification of the qubit assumption.

In the following, we discuss timing, spectral, spatial and polarization properties for different encoding phases.

1. Temporal-spectral mode

Temporal mode: Fig. 4 shows the schematic of the phase modulation based on $LiNbO_3$ crystal. When phase modulator

Distance	$n_{z,\mu}$	$n_{z,\nu}$	$n_{z,\omega}$	$n_{x,\mu}$	$n_{x,\nu}$	$n_{x,\omega}$
5km	7.84×10^7	2.23×10^6	2.60×10^4	7.17×10^6	4.08×10^5	4.70×10^3
20km	8.09×10^6	1.50×10^6	2.71×10^4	3.40×10^6	6.31×10^5	1.36×10^4
50km	2.01×10^7	6.94×10^5	4.81×10^4	2.06×10^6	7.10×10^5	4.82×10^4
	$n_{e_{z,\mu}}$	$n_{e_{z,\nu}}$	$n_{e_{z,\omega}}$	$n_{e_{x,\mu}}$	$n_{e_{x,\nu}}$	$n_{e_{x,\omega}}$
5km	1.01×10^6	6.40×10^4	6.80×10^3	1.32×10^5	1.25×10^4	1.76×10^3
20km	2.22×10^5	6.13×10^4	6.78×10^3	5.67×10^4	2.68×10^4	2.65×10^3
50km	5.98×10^5	8.46×10^4	2.28×10^4	6.40×10^5	8.89×10^4	2.23×10^4
	$n_{0_x\|0_z,\mu}$	$n_{0_x\|0_z,\nu}$	$n_{0_x\|0_z,\omega}$	$n_{1_x\|0_z,\mu}$	$n_{1_x\|0_z,\nu}$	$n_{1_x\|0_z,\omega}$
5km	3.83×10^6	2.47×10^5	3.30×10^3	4.16×10^6	2.32×10^5	2.40×10^3
20km	1.36×10^6	2.39×10^5	4.56×10^3	1.34×10^6	2.2×10^5	4.59×10^3
50km	0.57×10^7	1.63×10^5	1.10×10^4	0.56×10^7	1.76×10^5	1.26×10^4
	$n_{0_x\|1_z,\mu}$	$n_{0_x\|1_z,\nu}$	$n_{0_x\|1_z,\omega}$	$n_{1_x\|1_z,\mu}$	$n_{1_x\|1_z,\nu}$	$n_{1_x\|1_z,\omega}$
5km	3.83×10^6	2.46×10^5	3.31×10^3	4.15×10^6	2.32×10^5	2.41×10^3
20km	1.37×10^6	2.38×10^5	4.57×10^3	1.34×10^6	2.21×10^5	4.60×10^3
50km	0.58×10^7	1.62×10^5	1.11×10^4	0.56×10^7	1.77×10^5	1.25×10^4

TABLE V: **Experimental raw counts.**

(PM) modulates different phases, the electrical-optical effect inside the $LiNbO_3$ waveguide changes the principal refractive index n_z. At first sight, it might appear that the timing information is indeed changed for different phase modulations. However, we will show that such change is so small that it can be neglected.

According to the EM theory in $LiNbO_3$ waveguide, the relations among the principal refractive index n_z, the group refractive index n_g and the extraordinary refractive index n_e are given by [40]

$$\begin{aligned} n_g &= n_z + \omega_0 \frac{dn_z(\omega)}{d\omega}|_{\omega_0} \\ n_z &= n_e - \frac{1}{2} n_e^3 r_z \frac{V}{d} \end{aligned} \tag{D1}$$

where ω_0 is the central frequency of the optical field, r_z is the electro-optical coefficient along z axis, V is the voltage applied onto the crystal, and d is the thickness of the crystal. Thus the timing difference Δt between $\{0\}$ and phase modulation $\{\pi\}$ is given by

$$\Delta t = [\frac{1}{2} n_e^3 r_z \frac{V_\pi}{d} + \frac{3}{2} n_e^2 r_z \frac{V_\pi}{d} \omega_0 \frac{dn_e(\omega)}{d\omega}|_{\omega_0}] \frac{l_0}{c} \tag{D2}$$

where $V_\pi = \frac{\chi_0 d}{n_e^2 r_z l_0}$ is the half-wave voltage that provides a phase modulation $\{\pi\}$ [40], l_0 is the length of the crystal and c is the speed of light.

For a typical $LiNbO_3$ crystal working in the telecom wavelength $\chi_0 \sim 1550$ nm, it is well known that the relation between n_e and λ_0 is given by [42]

$$n_e^2 = 1 + \frac{2.980\lambda_0^2}{\lambda_0^2 - 0.020} + \frac{0.598\lambda_0^2}{\lambda_0^2 - 0.067} + \frac{8.954\lambda_0^2}{\lambda_0^2 - 416.08} \tag{D3}$$

Notice that in a waveguide based PM, one has to use the effective index, i.e., n_{eff}, to include the waveguide effect. We remark however that, for $LiNbO_3$ material, n_{eff} and n_e are almost the same [43]. Hence, by plugging Eq. (D3) into Eq. (D2), we have $\Delta t \approx 4\times10^{-6}$ ns. In a QKD implementation, the optical pulse is typically around 1 ns width [7–9] or 0.1 ns [10–12], thus $\Delta t \ll 0.1$ ns. Assuming that the optical pulse is Gaussian, Δt corresponds to a fidelity of $F(\rho^0, \rho^\pi) \approx 1 - 10^{-8}$ between $\{0\}$ and $\{\pi\}$. Therefore, timing remains (almost) the same for different phase modulations.

Spectral mode: First, in a standard one-way system, Alice can locally synchronize the devices so that the optical pulse passes through Alice's PM in the middle of the electrical modulation signal (flat response). Hence, the optical pulse experiences a correct modulation *without* spectral change [46, 47]. In a two-way system, Alice can monitor the timing information between the signal and reference pulse to guarantee the correct modulation and defend against side-channel attacks [46, 47]. Second, to guarantee single spectral mode from the output of a laser, one can use a standard wavelength filter. For instance, a recent QKD experiment used an off-the-shelf wavelength filter with a full-width at the half maximum (FWHM) of $\Delta\nu$ =15 GHz for a different purpose [12]. In this case, given a Gaussian pulse with FWHM $\Delta t = 0.1$ ns in the time domain [12], it is quite close to the lower bound of time-bandwidth product [40], i.e., $\Delta t \times \Delta\nu \geq \frac{2ln2}{\pi}$. Wavelength filters with narrow bandwidth have already been widely available on the market [44]. Hence, single spectral mode can be guaranteed with high accuracy by using a wavelength filter.

2. Spatial mode

For a standard single-mode fiber (SMF), the core diameter is around 10 um. Theory and experiments have already confirmed that a SMF in the telecom wavelength rejects all high-order modes and conducts only one fundamental trans-

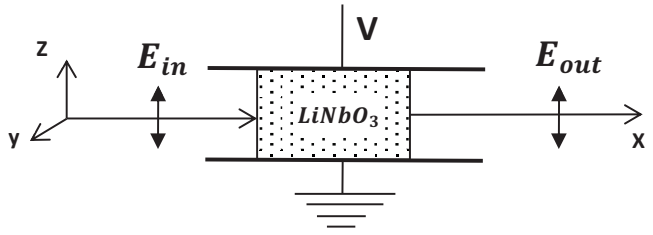

FIG. 4: Schematic of an electro-optic phase modulator based on $LiNbO_3$ crystal [40]. Commercial products can be seen in [41]. The double-headed arrows show the direction of polarization of the optical beam. The crystal is cut in a configuration so that the applied electrical field (voltage) is along the direction of the principal (z) axis. To take the advantage of the largest electro-optical coefficient in the z axis, an optical beam is propagating along the x axis, with the direction of polarization parallel to the z axis.

verse mode [45]. The cutoff wavelength of a standard SMF is about 1260 nm [2]. Using the software of BeamPROP, we have also performed a numerical simulation with a standard multimode fiber propagating into a SMF. The results show that after only about one millimeter, SMF rejects almost all high-order modes. The high-order modes decay exponentially, thus after about ten millimeters, there is no high-order component left (less than 10^{-10} proportion). Notice that, the input of a standard commercial PM usually has a certain length of pigtail fiber (about one meter) [41]. Therefore, the single mode assumption on spatial mode can be easily guaranteed in practice.

3. Polarization mode

The input of a commercial PM is normally a pigtail of polarization maintaining fiber [41], which can ensure that the input polarization is perfectly aligned with the principal axis of PM. Experimentally, before this polarization maintaining fiber, one can use a fiber polarization beam splitter (PBS) to reject other polarization modes. A standard PBS has about 30 dB extinction ratio. In the following, we discuss the error due to this finite extinction ratio (30 dB). Ideally, if the PBS has infinite extinction ratio, the input state is perfectly aligned with the principal axis (z axis in Fig. 4) and Alice modulates the four BB84 states as

$$|\phi_j\rangle = \frac{1}{\sqrt{2}}(e^{ij\frac{\pi}{2}}|S_z\rangle + |R_z\rangle),$$

where $j \in\{0, 1, 2, 3\}$ denotes the four BB84 states and $|S_z\rangle$ ($|R_z\rangle$) denotes the signal (reference) pulse with polarization along z axis. However, due to the finite extinction ratio of PBS, the signal and reference pulse are expressed as

$$|S\rangle = \alpha|S_y\rangle + \beta|S_z\rangle,$$
$$|R\rangle = \alpha|R_y\rangle + \beta|R_z\rangle,$$

where $|S_y\rangle$ denotes the polarization component along y axis. For 30 dB extinction ratio, $\alpha^2 \approx 0.001$. Thus Alice's imperfect modulations can be described by

$$|\phi'_j\rangle = \frac{1}{\sqrt{2}}(\alpha e^{ij\frac{\pi}{6}}|S_y\rangle + \beta e^{ij\frac{\pi}{2}}|S_z\rangle + \alpha|R_y\rangle + \beta|R_z\rangle, \tag{D4}$$

where we assume that the relative modulation magnitude ratio between the polarization aligned with the principal axis (z axis) and the orthogonal polarization (y axis in Fig. 4) is 1:3 [40, 46]. Using three new bases $\{|e_1\rangle, |e_2\rangle, |e_3\rangle\}$, Eq. (D4) can be written as (similar to [32])

$$|\phi'_j\rangle = \frac{1}{\sqrt{2}}(\alpha\beta(e^{ij\frac{\pi}{6}} - e^{ij\frac{\pi}{2}})|e_1\rangle + (\alpha^2 e^{ij\frac{\pi}{6}} + \beta^2 e^{ij\frac{\pi}{2}})|e_2\rangle + |e_3\rangle), \tag{D5}$$

Hence, the four imperfect states is spanned to three dimensions in Hilbert space, i.e., the information encoded by Alice is not only in the time-phase mode but also in the polarization mode. However, for 30 dB extinction ratio, we find that it is almost impossible for Eve to attack the system, because the fidelity between $|\phi_j\rangle$ and $|\phi'_j\rangle$, $F(\rho^{|\phi_j\rangle}, \rho^{|\phi'_j\rangle}) = tr\sqrt{\sqrt{\rho^{|\phi_j\rangle}}\rho^{|\phi'_j\rangle}\sqrt{\rho^{|\phi_j\rangle}}}$, is about $1 - 10^{-7}$ for $j \in\{0, 1, 2, 3\}$. This shows that the imperfect states are highly close to the perfect BB84 states. Most importantly, one can derive a refined security proof to include this small imperfection into the secure key rate formula, which will be a subject of future investigation.

[1] N. Gisin *et al*. *Rev. Mod. Phys.* **74**, 145–195 (2002); V. Scarani *et al*, *Rev. Mod. Phys.* **81**, 1301–1350 (2009); H.-K. Lo, M. Curty, K. Tamaki, *Nat. Photon.* **8**, 595 (2014).

[2] D. Mayers, J. of the ACM 48, 351 (2001); H.-K. Lo and H. Chau, *Science* **283**, 2050 (1999); P. Shor, J. Preskill, *Phys. Rev. Lett.* **85**, 441–444 (2000).

[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, *Quant. Inf. Comput.* **4**, 325 (2004).

[4] B. Huttner, N. Imoto, N. Gisin and T. Mor, *Phys. Rev. A*, **51**, 1863 (1995); G. Brassard, N. Lütkenhaus, T. Mor, B. Sanders, *Phys. Rev. Lett.* **85**, 1330–1333 (2000).

[5] W.-Y. Hwang *Phys. Rev. Lett.* **91**, 057901 (2003); H.-K. Lo, X. Ma, K. Chen *Phys. Rev. Lett.* **94**, 230504 (2005); X.-B. Wang *Phys. Rev. Lett.* **94**, 230503 (2005).

[6] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, L. Qian *Phys. Rev. Lett.* **96**, 070502 (2006).

[7] D. Rosenberg, J. *et al*. *Phys. Rev. Lett.* **98**, 010503 (2007).

[8] Schmitt-Manderbach, T. *et al*. *Phys. Rev. Lett.* **98**, 010504 (2007).

[9] Peng, C.-Z. *et al*. *Phys. Rev. Lett.* **98**, 010505 (2007).

[10] Dixon, A., Yuan, Z., Dynes, J., Sharpe, A., & Shields, A. *Opt. Exp.* **16**, 1879018979 (2008).

[11] Lucamarini, M. *et al*. *Opt. Exp.* **21**, 2455024565 (2013).

[12] Patel, K. A. *et al*. *Appl. Phys. Lett.* **104**, 051123 (2014).

[13] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter *Nat. Photon.* **7**, 382 (2013); J.-Y. Wang, J.-Y.*et al*.

Nat. Photon. **7**, 387 (2013); B. Frohlich *et al*. *Nature* **501**, 69 (2013); A. Rubenok, J.A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel *Phys. Rev. Lett.* **111**, 130501 (2013); Y. Liu, *et al*. *Phys. Rev. Lett.* **111**, 130502 (2013); T. Ferreira da Silva, *et al*. *Phys. Rev. A* **88**, 052303 (2013); Z. Tang, *et al*. *Phys. Rev. Lett.* **112**, 190503 (2014); Y. L. Tang, *et al*. *Phys. Rev. Lett.* **113**, 190501 (2014).

[14] Ø. Marøy, L. Lydersen, J. Skaar *Phys. Rev. A* **82**, 032337 (2010); E. Woodhead, S. Pironio *Phys. Rev. A* **87**, 032315 (2013).

[15] M. Dušek, M. Jahma, N. Lütkenhaus *Phys. Rev. A* **62**, 022306 (2000).

[16] H.-K. Lo, M. Curty, B. Qi *Phys. Rev. Lett.* **108**, 130503 (2012); M. Curty, *et al. Nat. Commun.* **3**, 634 (2014); F. Xu, M. Curty, B. Qi, H.-K. Lo *IEEE JSTQE* **21**, 3, 6601111 (2015).

[17] G. Berlín, *et al*. *Nat. Commun* **2**, 561 (2011); A. Pappa, *et al*. *Nat. Commun* **5**, 3717 (2014); V. Dunjko, E. Kashefi, A. Leverrier *Phys. Rev. Lett*. **108**, 200502 (2012).

[18] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, K. Azuma *Phys. Rev. A* **90**, 052314 (2014).

[19] S. M. Barnett, B. Huttner, S. Phoenix *J. Mod. Opt*. **40**, 2501 (1993).

[20] T. Sasaki, Y. Yamamoto, M. Koashi *Nature* **509**, 475 (2014); Z. Zhang, X. Yuan, Z. Cao, X. Ma *arXiv:1505.02481* (2015).

[21] J.-Y. Guan *et al*. *Phys. Rev. Lett.* **114**, 180502 (2015)

[22] M. Hayashi, T. Surumaru *New J. Phys.* **9**, 093014 (2011).

[23] M. Tomamichel, C. C.-W. Lim, N. Gisin,R. Renner *Nat. Commun.* **3**, 634 (2012).

[24] C. C.-W. Lim, M. Curty, N. Walenta, F. Xu, H. Zbinden, *Phys. Rev. A* **89**, 022307 (2014).

[25] M. Hayashi, R. Nakayama *New J. Phys.* **16**, 063009 (2014).

[26] M. Ben-Or, M. Horodecki, D.-W. Leung, D. Mayers, J. Oppenheim *Theory of Cryptography*, 386-406, Springer (2005); R. Renner, R. König *Theory of Cryptography*, 407425, Springer (2005); Renner, R. Security of quantum key distribution, Ph.D. thesis, ETH Zurich (2005).

[27] J. C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, J. M. Renes *Phys. Rev. Lett.* **94**, 040503 (2005); C.-H. F. Fung, H.-K. Lo *Phys. Rev. A* **74**, 042342 (2006).

[28] M. N. Wegman and J. L. Carter, *New hash functions and their use in authentication and set equality*, J. Comput. Syst. Sci. **22**, 265 (1981).

[29] Renner, R. Security of quantum key distribution, Ph.D. thesis, ETH Zurich (2005).

[30] X. Ma, B. Qi, Y. Zhao, H.-K. Lo *Phys. Rev. A* **72**, 012326 (2005)

[31] Hoeffding, W. *J. Amer. Statist. Assoc.* **58**, 13–30 (1963).

[32] S.-H. Sun, M.-S. Jiang, L.-M. Liang *Phys. Rev. A* **83**, 062331 (2011).

[33] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden *New J. Phys.* **4**, 41 (2002).

[34] ID Quantique: http://www.idquantique.com/

[35] F. Xu, *et al. Opt. Express* **20**, 12366 (2012).

[36] Tamaki, K., Lo, H.-K., Fung, C.-H. F. & Qi, B. *Phys. Rev. A* **85**, 042307 (2012).

[37] Honjo, T., Inoue, K., & Takahashi, H. *Opt. Lett.* **23**, 2797 (2004).

[38] F. Xu, *et al.* arXiv:1408.3667v2 (2015).

[39] A. Mizutani, *et al.* arXiv:1504.08151 (2015).

[40] Yariv, A. & Yeh, P. *Oxford University Press* (2007).

[41] For instance, EO-space: http://www.eospace.com; JDSU: http://www.jdsu.com

[42] Zelmon, D. E., Small, D. L. & Jundt, D. *Journal of the Optical Society of America B* **14**, 3319 (1997).

[43] Suhara, T. & Fujimura, M. *Springer* **11**, (2003).

[44] http://www.afwtechnologies.com.au; http://www.yenista.com

[45] Mynbaev, D. K. & Scheiner, L. L. Fiber-optic communications technology. Prentice Hall (2001).

[46] Xu, F., Qi, B., & Lo, H.-K. *New J. Phys.* **12**, 113026 (2012).

[47] Jiang, M.-S., Sun, S.-H., Li, C.-Y. & Liang, L.-M. *Journal of Modern Optics* **61**, 147 (2014).