Experimental quantum key distribution with source flaws and tight finite-key analysis

Feihu Xu, 1,∗ Shihan Sajeed, 2 Sarah Kaiser, 2 Zhiyuan Tang, 1 Li Qian, 1 Vadim Makarov, 2 and Hoi-Kwong Lo 1

1 Centre for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada
2 Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

(Dated: August 19, 2014)

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 secure in practice. Here, we perform an experiment that for the first time shows secure QKD with imperfect state preparations at long distances and achieves rigorous finite-key security bounds for decoy-state QKD against general quantum attacks in the universally composable framework. We implement both decoy-state BB84 and three-state protocol on top of a commercial QKD system and generate secure keys over 50 km standard telecom fiber based on a recent security analysis that is loss-tolerant to source flaws. Our work constitutes an important 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, 2]. Commercial systems have already appeared on the market and various QKD networks have been developed. The most important question in QKD is its security. This fact has finally been proven in a number of important papers [3–5] (see [2] for a review on this topic). 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, such as the photon-number-splitting attack [6]. Fortunately, the decoy-state method [7–9] 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 [10–14]. As a result, decoy-state method has become a standard technique in many current QKD implementations [15–21].

Until now, QKD experiments [10–21] have had three important drawbacks. First, in the key rate formula of all existing experiments, it is commonly assumed that the phase/polarization encoding is done perfectly. On one hand, the single-photon components of the four BB84 states are assumed to remain strictly inside a two-dimensional Hilbert space. We call this qubit assumption. In practice, no previous works have verified this assumption [10–21]. Note that an attack to exploit the higher dimensionality of state preparation has been proposed in [22]. On the other hand, the encoding devices are widely assumed to be perfect without modulation errors. This is a highly unrealistic assumption and may mean that the key generation is actually not proven to be secure in a real QKD experiment. What if we use a key rate formula that takes imperfect modulation into account? Standard Gottesman-Lo-Lütkenhaus-Preskill (GLLP) security proof [5] (see also [23, 24]) does allow one to do so. Unfortunately, the key rate will be reduced substantially because the GLLP formalism is very conservative and the resulting protocol is not loss-tolerant. Both key rate and distance will suffer greatly from the modulation errors [25]. This might be the major reason that previous experiments commonly ignored source flaws. We remark that source flaw is a serious concern in not only decoy-state BB84 but also measurement-device-independent QKD [17–21], quantum coin flipping [26, 27] and blind quantum computing [28].

Second, the security claims in most (if not all) of experiments [10–21] were made with the assumption that the eavesdropper (Eve) was restricted to particular types of attacks (e.g., collective attacks) or that the finite-key analysis was not rigorous (e.g., the security did not satisfy the universally composable security definition [29, 30]). Unfortunately, such assumptions cannot be guaranteed in practice. While Ref. [31] has reported an attempt implementing the rigorous finite-key analysis proposed in [32], a slight drawback is that both the theory and experiment assume a perfect single-photon source without decoy states. Very recently, Lim et al. provide, for the first time, tight and rigorous security bounds against general attacks for decoy-state QKD [33] (see also [34]). This analysis is built on a combination of the rigorous finite-key analysis of [32], and the novel finite-data analysis for the measurement-device-independent QKD method [35]. A QKD experiment that implements such a rigorous security analysis has yet to be completed.

∗Electronic address: feihu.xu@utoronto.ca
Third, the security analysis of previous experiments often relies on rotational symmetries [3–5]. Hence, four BB84 states are required for the estimation of the bit error rate and phase error rate. QKD protocols with three states, i.e., three-state protocols, have been proposed [36, 37], but to our knowledge, a decoy-state implementation of three-state protocol has not been reported in the literature.

In this paper, we perform a decoy-state QKD experiment that for the first time shows secure QKD with imperfect source at long distances. Our implementation is based on a novel proposal [38], which allows QKD protocols that are loss-tolerant to state-preparation flaws. We call it a loss-tolerant protocol. The key insight is that as long as the single-photon component remains a qubit (though, the devices that manipulate them can have modulation errors), Eve can not enhance state-preparation flaws by exploiting the channel loss. This is a reasonable assumption, as the source can be placed in Alice’s protected environment outside of Eve’s influence and Alice can in principle guarantee this assumption via quantifying her devices locally (see Appendix D).

On the theoretical side, our contributions are as follows. First, we perform a detailed analysis on the qubit assumption in a standard one-way phase-encoding system and have verified such assumption with high accuracy by using standard optical devices. Second, based on [33], we provide a rigorous finite-key analysis for the loss-tolerant protocol, thus making this protocol applicable in a real experiment. Third, we propose a method with finite number of decoy states in the loss-tolerant protocol.

Fourth, we show that QKD with three states gives almost the same key rate as BB84 in a practical setting with a reasonable data-rate. This is a reasonable assumption, as the source can be placed in Alice’s protected environment outside of Eve’s influence and Alice can in principle guarantee this assumption via quantifying her devices locally (see Appendix D). In addition to the decoy-state BB84, by modifying the commercial QKD system, we perform the first decoy-state experiment with only three encoding states.

II. THEORY

Three-state QKD: The loss-tolerant protocol works for both BB84 and three-state QKD. The three-state QKD [36, 37] runs almost the same as BB84 except that: i) Alice sends Bob only three pure states \(\{|0_z\}, |0_x\}, \{1_z\}\rangle\), where \(|i_j\rangle\) \((i \in \{0, 1\}\) and \(j \in \{Z, X\}\) denotes the state associated with bit “i” in \(j\) basis; ii) the rejected data (i.e., basis mismatch events) are used for the estimation of the phase error rate [39]. Based on the security analysis with biased basis choice, Alice and Bob can generate a secret key only from those instances where both of them select the \(Z\) basis [38].

Verify qubit assumption: The key point of the loss-tolerant protocol is the qubit assumption. If it holds, there is no side-channel for Eve to exploit to enhance the source flaws through channel loss [22, 38]. To guarantee this assumption, a phase-encoding system is required to have almost the same timing, spatial, spectral and polarization mode information for different encoding states. For a standard one-way phase-encoding system based on LiNbO3 phase modulator [11, 14, 15, 18, 19], 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 (see Appendix D for the details). For a two-way system, Alice can monitor the source and verify this assumption locally by using, for instance, the scheme proposed in [40].

Finite-key analysis: So far, unfortunately, the loss-tolerant protocol was only proven in the asymptotic case with infinitely long keys and an infinite number of types of decoy states, i.e., the legitimate users have unlimited resources [38]. Such an asymptotic case is impossible in practice. Here, to implement the loss-tolerant protocol, we extend it to a general practical setting with finite keys and finite decoy states. Our finite-key analysis is based on [33]. The \(\varepsilon_{\text{sec}}\)-secret key length in the \(Z\) basis is given by [33]

\[
\ell \geq s_{z,0}^L + s_{z,1}^L - s_{x,1}^U (\varepsilon_{x,1}) - \text{leak}_{\text{EC}} - 6 \log_2 \left(\frac{21}{\varepsilon_{\text{sec}}}\right) - \log_2 \left(\frac{2}{\varepsilon_{\text{cor}}}\right),
\]

(1)

where \(h(y) = -y \log_2 y - (1 - y) \log_2 (1 - y)\) is the binary entropy function; \(s_{z,0}^L, s_{z,1}^L \) and \(\varepsilon_{x,1}^U\) 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; \(\text{leak}_{\text{EC}} = n_{z,\mu} f_c (\varepsilon_z)\) is the size of the information exchanged during error-correction, where \(n_{z,\mu}\) and \(e_z\) denote respectively the gain counts for signal state and quantum bit error rate (QBER) and \(f_c \geq 1\) is the error correction inefficiency function; \(6 \log_2 \left(\frac{21}{\varepsilon_{\text{sec}}}\right)\) and \(\log_2 \left(\frac{2}{\varepsilon_{\text{cor}}}\right)\) are respectively the secrecy and correctness parameter. \(\ell\) quantifies the lower bound of final key length and the key rate is given by \(R^L = \ell / N\) with \(N\) denoting the total number of signals (optical pulses) sent by Alice. This key formula uses a security proof that is based on an uncertainty relation for smooth entropies [32] and it fulfills the composable security definition [29, 30].
Finite decoy-state protocol: In practice, \( s_{z,0}^L, s_{z,1}^L \) and \( e_{z,1}^U \) are estimated using the decoy-state method. Here, we propose a novel method for the estimation of the phase error rate \( e_{z,1}^U \). In our analysis, besides the signal state \( \mu \), we consider two additional decoy states, \( \nu \) and \( \omega \), where \( \mu, \nu \) and \( \omega \) are the mean photon numbers of weak coherent pulses and they satisfy \( \mu > \nu > \omega \geq 0 \). Hence, the intensity setting \( k \in \{ \mu, \nu, \omega \} \). The key novelty to estimate \( e_{z,1}^U \) is using the rejected detection counts [39], i.e., considering the detection events associated with single photons when Alice and Bob use different bases. The estimation result is shown in Eq. (A3) of Appendix A. \( s_{z,0}^L \) and \( s_{z,1}^L \) can be estimated using a method similar to [33], from the detection events \( n_{z,k} \) (see Appendix A for details).

III. EXPERIMENT

System description: We perform a proof-of-principle experiment on top of a commercial ID-500 (manufactured by id Quantique) plug&play QKD system [42]. Our system employs the phase-coding QKD scheme and it works as follows (see Fig. 1). 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 signal (detected by her classical photo-detector) to activate her phase modulator (PM). Then Alice modulates the phase of the returning reference pulse and detects the interference signals with his two single-photon detectors (SPDs). To implement the decoy-state protocol, we use the variable optical attenuator (VOA) in Alice to generate signal state and decoy states [43]. We have measured the system parameters as shown in Table I.

Quantify modulation error: We first quantify the modulation error \( \delta \) in the source through calibrating Alice’s PM, a LiNbO\(_3\) waveguide based electro-optical modulator. \( \delta \) is defined as the difference between expected phase and actual phase. We find that in our ID-500 system, the voltage value \{0, 0.77, 1.59, 2.36\} V is used for the phase modulation \{0, \pi/2, \pi, 3\pi/2\}. With the statistical fluctuations, the modulation error is upper bounded by \( \delta \leq 0.127 \) (see Appendix B for details). Notice that \( \delta \) can also be estimated using the interference visibility or the extinction ratio of the PM [25]. In a system with an advanced phase-stabilized interferometer [44], the value of \( \delta \leq 0.062 \) corresponds to about 99.9\% visibility or 30 dB extinction ratio. We have also measured such error in an updated version of commercial plug&play system (ID Quantique Clavis2) and found that \( \delta \leq 0.147 \).

Implementation of loss-tolerant protocol: In our demonstration, we first implement the three-state decoy-state protocol over 50 km standard telecom fiber. The ID-500 system allows one to freely modify (via software) the four voltage values applied on Alice’s PM. In our implementation, we set Alice’s modulation voltage values to be \{0, 0.77, 1.59, 0.77\} V and thus operate Alice to send three encoding phases \{0, \pi/2, \pi\}, where the probability ratio for these three phases is 1 : 2 : 1 (with equal basis probability for the simplicity of implementation). We chose to operate the system for about 3 hours and send a total number of pulses \( N=5 \times 10^{10} \). Before the experiment, we performed a numerical simulation to optimize the implementation parameters. Our optimization routine is similar to [41], while the difference is that we use the rigorous finite-key security bounds (see Eq. (1)).
and the key rate formula of Eq. (1), the final secure key rate is:

\[ R = \frac{1}{2(e - \sum_{j=0}^{3} P_{j})} \]

where the key generation rate will hit zero at only about 10 km based on GLLP. The experimental data, we consider a conservative security parameter (the summation of all failure probabilities) \( \epsilon = 10^{-10} \). Finally, based on the three-state protocol, we got a QBER \( e_z = 2.98\% \) and a lower bound of secure key generation rate \( R^L = 5.21 \times 10^{-5} \) per pulse. About 2603 kbit 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 be against general attacks by Eve.

Next, we perform a similar experiment based on decoy-state BB84. Alice modulates her PM with a voltage value selected from \( \{0, 0.77, 1.59, 2.36\} \) V for each pulse, i.e., she randomly sends a state from \( \{0, \pi/2, \pi, 3\pi/2\} \) for each pulse. We also send a total number of signals \( 5 \times 10^{10} \) and use the same intensities and probabilities as the three-state implementation. We measure the raw counts in Fig. 2(d) and 2(e) and obtain the experimental results shown in the right column of Table II. Based on the loss-tolerant protocol (see Appendix C), the final secure key rate is \( R^L = 1.54 \times 10^{-4} \) per pulse. The key rate differences between BB84 and three-state protocol are mainly due to the finite-data statistics, which affects the estimation error on \( e_{\delta,1}^L \). We numerically find that if operating the experiment longer, say generating \( N = 10^{12} \), the key rate with three states is close to that with BB84. Notice that \( 10^{12} \) signals can be easily achieved within 20 min by using a relatively high speed system such as 1 GHz repetition rate [14, 15].

As a comparison to previous security analysis (e.g., GLLP), with the source flaws \( \delta = 0.127 \), 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 based on GLLP [5, 25].

To simplify our implementation, we adopt equal basis probability, i.e., \( P_2 = P_X = 0.5 \), and assume that the basis choice is independent of the intensities.

![FIG. 2: Experimental raw counts.](image)

(a) (b) (c) (d) (e)

TABLE II: Experimental results. These values are obtained by plugging the raw counts (Fig. 2) into the estimation equations shown in Appendix A and the key rate formula of Eq. (1).

| Parameter | Three-state | BB84 |
|-----------|-------------|------|
| \( s_{0,0}^L \) | \( 3.22 \times 10^5 \) | \( 3.21 \times 10^5 \) |
| \( s_{0,1}^L \) | \( 1.30 \times 10^7 \) | \( 1.31 \times 10^7 \) |
| \( e_z \) | 2.98% | 2.89% |
| \( e_{\delta,1}^L \) | 11.49% | 6.01% |
| \( l \) | \( 2.60 \times 10^6 \) | \( 7.70 \times 10^6 \) |
| \( R^L \) | \( 5.21 \times 10^{-5} \) | \( 1.54 \times 10^{-4} \) |
FIG. 3: Decoy-state QKD with source flaws in a practical setting. The simulation is conducted with parameters in Table I, $N = 5 \times 10^{10}$ and $\epsilon = 10^{-10}$. The main figure is for the three-state protocol based on our security analysis, while the inserted figure is for the decoy-state BB84 protocol based on GLLP security analysis (see Appendix C 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 $\delta$ increases. The maximal tolerant distance is about 9 km for our QKD system (green dashed-dotted curve in the inserted figure). In contrast, our analysis can substantially outperform GLLP and it is loss-tolerant to source flaws. Our QKD set-up 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 $\delta = 0$).

In other words, at 50 km, not even a single bit could be shared between Alice and Bob with guaranteed security with previous GLLP security proof. This means that if considering source flaws in previous long-distance decoy-state experiments [10–16], the key generation might be not proven to be secure. In contrast, our analysis with the loss-tolerant protocol can easily achieve high secure key generation rate over long distances even in the presence of source flaws.

IV. DISCUSSION

Numerical simulation: With $\delta$ and the parameters in Table I, we perform a simulation to numerically study our security analysis in a practical setting. Fig. 3 shows the simulation results, where similar to our experiment, we use $N = 5 \times 10^{10}$ and $\epsilon = 10^{-10}$. For comparison, this figure also includes the key rate for the decoy-state BB84 based on the GLLP security analysis (See Appendix C 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 $\delta$ increases. The maximal tolerant distance is about 9 km for our QKD system. This is because GLLP considers the worst case scenario where losses can increase the fidelity flaw [5, 25]. Our security analysis, however, can substantially outperform GLLP and it is loss-tolerant to source flaws. 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.

Conclusion: We have demonstrated decoy-state QKD with imperfect state preparations and employed tight finite-key security bounds in our implementation. Our work constitutes an important step towards secure QKD with imperfect devices in practice. 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 [45]. Also, we assume that there is no unwanted information leakage from the source. How to protect the source outside of Eve’s active influence will be a subject for future investigations. Furthermore, it will be interesting to work out a refined security proof that include all possible (small) imperfections and side channels in the source and extend our results to MDI-QKD [17]. Thus, one can solve the problem of not only imperfect source but also remove all loopholes in the detection system. This may incubate the first practical side-channel-free QKD.

V. ACKNOWLEDGMENTS

We thank M. Curty, C. Lim, M. Legrê and G. Ribordy for valuable discussions. Support from NSERC, the CRC program, Connaught Innovation fund and Industry Canada is gratefully acknowledged. F. Xu thanks Shahid U.H. Qureshi Memorial Scholarship and the OGS Visa award for the support. S. S. and S.K. acknowledge support from CryptoWorks21, US Office of Naval Research and Mike & Ophelia Lazaridis Fellowship.
Appendix A: Decoy-state analysis for three-state protocol

Our decoy-state analysis builds on [33], which discusses the decoy-state BB84. Our new contribution is estimating the phase error rate $e_{x,1}^U$. In decoy-state BB84, $e_{x,1}^U$ is estimated from the counts in $X$ basis [33]. In three-state protocol, however, $e_{x,1}^L$ is estimated from the rejected counts, i.e., considering the detection events associated with single photons when Alice and Bob use different bases. Notice also that our estimation focuses directly on the detection counts announced by Bob, which is different from previous analysis that is based on detection probabilities [8, 9].

In original decoy-state method [8, 9], 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 [46], 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,

$$
\hat{n}_{z,k} \leq n_{z,k} + \delta(n_z, \varepsilon_1) = n_{z,k}^U,
$$

$$
\hat{n}_{z,k} \geq n_{z,k} - \delta(n_z, \varepsilon_1) = n_{z,k}^L,
$$

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: $P_{k|n} = \frac{P_n e^{-k n}}{\tau_n}$, where $\tau_n = \sum_{k \in \{\mu, \nu, \omega\}} P_k e^{-k n}/n$ is the probability that Alice prepares an $n$-photon state. Based on an estimation method in [41], we have

$$
s_{z,0}^L = \frac{\tau_0}{(\nu - \omega)} \left( \frac{\nu e^\omega n_{z,\omega}^L}{P_\omega} - \frac{\omega e^\nu n_{z,\nu}^L}{P_\nu} \right), \quad (A1)
$$

$$
s_{z,1}^L = \frac{\mu n_{z,\mu}^L}{\mu(\nu - \omega) - (\nu^2 - \omega^2)} \left[ \frac{e^\nu n_{z,\nu}^L}{P_\nu} - \frac{e^\omega n_{z,\omega}^L}{P_\omega} + \frac{\nu^2 - \omega^2}{\mu^2} \left( \frac{s_{z,0}^L}{\tau_0} - \frac{e^\nu n_{z,\nu}^L}{P_\nu} \right) \right]. \quad (A2)
$$

Different from [33], the phase error rate $e_{x,1}^U$ in a three-state protocol is estimated using the rejected data analysis [38]:

$$
e_{x,1}^U = \frac{2P_x s_{0|x,1}^U + P_z s_{1|x,1}^U - s_{0|x,1}^L}{2P_x s_{1|x,1}^L}, \quad (A3)
$$

where $P_x$ ($P_z$) is the probability that Alice/Bob selects $X$ ($Z$) basis; $s_{0|x,1}^U$ denotes the upper bound of single-photon events when Bob has detections associated with bit “0” in $X$ basis, given that Alice sends a state in $Z$ basis; $s_{1|x,1}^U$, $s_{0|x,1}^L$, $s_{1|x,1}^L$, $s_{0|x,1}^L$ has the similar meaning. $s_{0|x,1}^L$ and $s_{1|x,1}^L$ can be estimated equivalently by plugging $n_{0|x,1}^L$ ($n_{0|x,1}^U$) and $n_{1|x,1}^L$ ($n_{1|x,1}^U$) into Eqs. (A1) and (A2) to replace $n_{z,k}^U$ ($n_{z,k}^L$), $s_{0|x,1}^U$ and $s_{1|x,1}^U$ can be estimated by

$$
s_{0|x,1}^U = \tau_1 \frac{n_{0|x,1}^U - n_{0|x,1}^L}{\nu - \omega},
$$

$$
s_{1|x,1}^U = \tau_1 \frac{n_{1|x,1}^U - n_{1|x,1}^L}{\nu - \omega}.
$$
We discuss the calibration methods and measurement results for the modulation error $\delta$ of Alice’s phase modulator (PM) in two ID Quantique commercial plug&play systems. The calibration process is as follows. Alice is directly connected to Bob with a short fiber (about 1 m); Bob keeps sending optical pulses out and 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\(^2\). The counts for Alice’s different phase modulations are denoted by $D_{1,\theta}$ and $D_{2,\theta}$. We find that in ID-500 system, the voltages $\{0, 0.30V_m, 0.62V_m, 0.92V_m\}$ give the phase modulations $\{0, \pi/2, \pi, 3\pi/2\}$, where $V_m \approx 2.57\text{ V}$ is a maximal value allowed on Alice’s PM. The detections counts of ten measurements for $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ are shown in Table III.

In ID-500 system, to quantify the modulation errors $\delta_\theta$ for $\theta \in \{\pi/2, \pi, 3\pi/2\}$, we first determine the detector efficiency and dark counts for Bob’s two SPDs and find that $\eta_{d1} = 5.05\%$ and $\eta_{d2} = 4.99\%$ and the dark count rate for the two SPDs are almost the same as $Y_{0,d1} \approx Y_{0,d2} = 4.01 \times 10^{-5}$. Notice that when Alice’s PM applies a $\{0\}$ phase, $D_{1,0}$ (i.e., 630 in Table III) quantifies the summation of the dark counts and imperfect visibility of the system (due to imperfect optical alignment). Ignoring finite data statistics temporarily, the modulation error can be written as:

$$\delta_\theta = |\theta - 2\arctan(\sqrt{(D_{1,\theta} - D_{1,0})/\eta_{d1})/\sqrt{(D_{2,\theta} - D_{1,0})/\eta_{d2})}|$$

where $\theta \in \{\pi/2, \pi, 3\pi/2\}$.

In our analysis of the statistics, we use standard error analysis following [41]. The upper bound of $\delta_\theta$ is thus given by:

$$\delta_\theta \leq \delta_\theta = |\theta - 2\arctan(\sqrt{(D_{1,\theta} + n_\alpha\sqrt{D_{1,\theta}} - (D_{1,0} - n_\alpha\sqrt{D_{1,0}}))/\eta_{d1})/\sqrt{(D_{2,\theta} - n_\alpha\sqrt{D_{2,\theta}} - (D_{1,0} + n_\alpha\sqrt{D_{1,0}}))/\eta_{d2})}|,$$

where $n_\alpha$ denotes the number of standard deviations one chooses for statistical fluctuation analysis. Here, we choose $n_\alpha = 7$, which corresponds to a failure probability about $\epsilon = 10^{-10}$. The upper bounds of $\delta_\theta$ are shown in Table III. From this table, the error $\delta$ in ID-500 system is upper bounded by the case of $\delta_{3\pi/2}$, i.e., $\delta \leq \delta_{3\pi/2} = 0.127$.

Using the same method in Clavis2, we find that $\delta$ is upper bounded by $\delta \leq \delta_{3\pi/2} = 0.147$.

Appendix C: GLLP security analysis with source flaws

We discuss the standard GLLP security analysis for BB84 with source flaws [5, 25], which is used for our simulation of Fig.3. 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

\[
\begin{align*}
|\phi_{0_z}\rangle &= |0_z\rangle \\
|\phi_{1_z}\rangle &= \sin \delta_2|0_z\rangle + \cos \delta_2|1_z\rangle \\
|\phi_{0_x}\rangle &= \cos \delta_1|0_x\rangle + \sin \delta_1|1_x\rangle \\
|\phi_{1_x}\rangle &= \sin \delta_3|0_x\rangle + \cos \delta_3|1_x\rangle
\end{align*}
\]

\(^2\) In our calibration, we assume that phase $\{0\}$ modulation is error-free. Our method could easily be generalised to the case when $\{0\}$ phase modulation has an error.
Based on GLLP for imperfect sources, the $e_{\sec}$-secret key length is similar to Eqn. 1, except for the phase error rate, which includes the correction due to basis-dependent flaws and is revised to [5]

$$e_{x,1}^U \leq e_{x,1}^U + 4\Delta' + 4\sqrt{\Delta' e_{x,1}^U} + \epsilon_{ph}$$

(C2)

Here, $\Delta'$, called the balance of a quantum coin [5, 25], quantifies the basis-dependent flaws of Alice signals associated with single-photon events. $\Delta'$ is given by [5]

$$\Delta' \leq \frac{\Delta}{Y_1}$$

$$\Delta = \frac{1 - F(\rho_z, \rho_x)}{2}$$

(C3)

where $Y_1 = \frac{\delta_{x,1}}{\sigma_{x,1}}$ (typically called the yield of single photons [8]) 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. (C1), 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 $F(\rho_z, \rho_x)=1 - 1.9 \times 10^{-3}$. So, from Eq. (C3), $\Delta = 9.45 \times 10^{-4}$.

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. (C3), i.e., $\Delta$ is enhanced to $\Delta'$. Combined with the decoy-state estimations discussed in [33], we can derive the key length and obtain the insert curves in Fig. 3.

In contrast, based on the loss-tolerant protocol [38], as long as the single-photon component remains a qubit, Eve can not enhance state-preparation flaws. Thus, in our implementation of decoy-state BB84, we use $\Delta = \Delta'$ in our key length estimation, i.e., the experimental results for BB84 in Table II.

Appendix D: Qubit assumption

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 [11, 14, 15, 47]. 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 [48]. For commercial products, see [49]. To guarantee the qubit assumption, Alice’s PM is supposed to have the same timing, spectral, spatial and polarization 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. In the following, we discuss timing, spectral, spatial and polarization properties for different encoding phases.

Temporal-spectral mode

Temporal mode: Fig. 4 shows the schematic of the phase modulation based on LiNbO$_3$ crystal. When phase modulator (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 [48]

$$n_g = n_z + \omega_0 \frac{dn_z(\omega)}{d\omega}\bigg|_{\omega_0}$$
$$n_z = n_e - \frac{1}{2} n_e^3 \frac{V}{d}$$

where $\omega_0$ 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 $\Delta t$ between $\{0\}$ and phase modulation $\{\pi\}$ is given by

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

where $V_\pi = \frac{\lambda_0 d}{n_e^2 r_z l_0}$ is the half-wave voltage that provides a phase modulation $\{\pi\}$ [48], $l_0$ is the length of the crystal and $c$ is the speed of light.

For a typical LiNbO$_3$ crystal working in the telecom wavelength $\lambda_0 \sim 1550$ nm, it is well known that the relation between $n_e$ and $\lambda_0$ is given by [50]

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

Notice that in a waveguide based PM, one has to use the effective index, i.e., $n_{e,eff}$, to include the waveguide effect. We remark however that, for LiNbO$_3$ material, $n_{e,eff}$ and $n_e$ are almost the same [51]. Hence, by plugging Eq. (D3) into Eq. (D2), we have $\Delta t \approx 4 \times 10^{-6}$ ns. In a QKD implementation, the optical pulse is typically around 1 ns width [11–13] or 0.1 ns [14, 15, 47], thus $\Delta t < 0.1$ ns. Assuming that the optical pulse is Gaussian, $\Delta t$ corresponds to a fidelity of $F(\rho^0, \rho^\pi) \approx 1 - 10^{-5}$ 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 [52, 53]. 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 [52, 53]. 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 [47]. In this case, given a Gaussian pulse with FWHM $\Delta t = 0.1$ ns in the time domain [47], it is quite close to the lower bound of time-bandwidth product [48], i.e., $\Delta t \times \Delta \nu \geq \frac{2\lambda_0^2}{\Delta \nu}$. Wavelength filters with narrow bandwidth have already been widely available on the market [54]. Hence, single spectral mode can be guaranteed with high accuracy by using a wavelength filter.

**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 mode [55]. Using the software of BeamPROP, we have also performed a numerical simulation with a standard multi-mode 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) [49]. Therefore, the single mode assumption on spatial mode can be easily guaranteed in practice.

**Polarization mode**

The input of a commercial PM is normally a pigtail of polarization maintaining fiber [49], 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

$$|\phi_i\rangle = \frac{1}{\sqrt{2}} (e^{i\frac{\pi}{4}} |S_z\rangle + |R_z\rangle),$$
where \( j \in \{0, 1, 2, 3\} \) denotes the four BB84 states and \(|S_y\rangle (|R_z\rangle)\) 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

\[
|\phi'_j\rangle = \frac{1}{\sqrt{2}}(\alpha e^{ij\frac{\pi}{2}}|S_y\rangle + \beta e^{ij\frac{\pi}{2}}|S_z\rangle + \alpha|R_y\rangle + \beta|R_z\rangle),
\]

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 \([48, 52]\). Using three new bases \(|e_1\rangle, |e_2\rangle, |e_3\rangle\), Eq. (D4) can be written as (similar to \([22]\))

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

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 \(|\phi'_j\rangle\), \(F(\rho|\phi_j\rangle, \rho|\phi'_j\rangle) = tr(\sqrt{\sqrt{\rho|\phi_j\rangle\langle\phi_j|}\sqrt{\rho|\phi'_j\rangle\langle\phi'_j|}})\), 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] Gisin, N. et al. Quantum cryptography. Rev. Mod. Phys. 74, 145–195 (2002).
[2] Scarani, V. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301–1350 (2009).
[3] Lo, H.-K. & Chau, H. Unconditional security of quantum key distribution over arbitrarily long distances. Science 283, 2050 (1999).
[4] Shor, P. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85, 441–444 (2000).
[5] Gottesman, D., Lo H.-K., Lütkenhaus, N. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. Quant. Inf. Comput. 4, 325 (2004).
[6] Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. Limitations on practical quantum cryptography. Phys. Rev. Lett. 85, 1330–1333 (2000).
[7] Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. 91, 057901 (2003).
[8] Lo, H.-K., Ma, X. & Chen, K. Decoy State Quantum Key Distribution. Phys. Rev. Lett. 94, 230504 (2005).
[9] Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. Phys. Rev. A 94, 230503 (2005).
[10] Zhao, Y., Qi, B., Ma, X., Lo, H.-L. & Qian L. Experimental quantum key distribution with decoy states. Phys. Rev. Lett. 96, 070502 (2006).
[11] Rosenberg, J. et al. Long-distance decoy-state quantum key distribution in optical fiber. Phys. Rev. Lett. 98, 010503 (2007).
[12] Schmitt-Manderbach, T. et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys. Rev. Lett. 98, 010504 (2007).
[13] Peng, C.-Z. et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. Phys. Rev. Lett. 98, 010505 (2007).
[14] Dixon, A., Yuan, Z., Dynes, J., Sharpe, A., & Shields, A. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Opt. Exp. 16, 1879018979 (2008).
[15] Lucamarini, M. et al. Efficient decoy state quantum key distribution with quantified security. Opt. Exp. 21, 2455024565 (2013).
[16] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S. & We infurter H. Air-to-ground quantum communication. Nat. Photon. 7, 382386 (2013).
[17] Lo, H.-K. Curty, M. & Qi, B. Measurement-deviceindependent quantum key distribution. Phys. Rev. Lett. 108, 130503 (2012).
[18] Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I., & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. Phys. Rev. Lett. 111, 130501 (2013).
[19] Liu, Y. et al. Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. 111, 130502 (2013).
[20] Silva, T. F. da, Vitoroti, D., Xavier, G., Amaral, G. do, Temporão & Weid, J. von der Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys. Rev. A 88, 052303 (2013).
[21] Tang, Z., Liao, Z., Xu, F., Qi, B., Li, Q. & Lo, H.-K. Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. Phys. Rev. Lett. 112, 190503 (2012).
[22] Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Passive faradaymirror attack in a practical two-way quantum-key-distribution system. Phys. Rev. A 83, 062331 (2011).
[23] Marøy, Ø., Lydersen, L. and Skaar, J. Security of quantum key distribution with arbitrary individual imperfections. *Phys. Rev. A* **82**, 032337 (2010).

[24] Wootters, W. K., and Zurek, W. H. Experimental verification of quantum nondemolition measurement. *Phys. Rev. Lett.* **41**, 228 (1978).

[25] Marquardt, C., Lacki, J., Nunn, C. P., Lagoute, R. and Clark, J. R. Quantum teleportation with a single photon. *Nature* **467**, 73 (2010).

[26] Sasaki, K., Ishino, A., Takeoka, M., and Takei, K. Quantum key distribution with a phase modulator. *Phys. Rev. A* **85**, 042307 (2012).

[27] Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. Experimental quantum key distribution with finite-key security analysis for noisy channels. *Nat. Commun.* **2**, 2363 (2013).

[28] Lim, C. C.-W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).

[29] Hayashi, M. & Nakayama, R. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths. *New J. Phys.* **16**, 063009 (2014).

[30] Barnett, S. M., Bruno H., Simon J. P. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *Nat. Commun.* **3**, 634 (2012).

[31] Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. Experimental quantum key distribution with finite-key security analysis for noisy channels. *Nat. Commun.* **2**, 2363 (2013).

[32] Tomamichel, M., Lim, C. C.-W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).

[33] Lim, C. C.-W., Curty, M., Walenta, N. Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).

[34] Hayashi, M. & Nakayama, R. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths. *New J. Phys.* **16**, 063009 (2014).

[35] Curty, M., Xu, F., Cui, W., Lim, C. C.-W., Tamaki, K. & Lo, H.-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **3**, 634 (2014).

[36] Boileau, C., Tamaki, K., Batsuwardaw, J., Laflamme, R. & Renes, J. Unconditional security of a three state quantum key distribution protocol. *Phys. Rev. Lett.* **94**, 040503 (2005).

[37] Fung, C.-H. F. & Lo, H.-K. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Phys. Rev. A* **74**, 042342 (2006).

[38] Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. Preprint arXiv: 1312.3514 (2013).

[39] Barnett, S. M., Bruno H., Simon J. P. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *J. Modern Optics* **40**(12) (1993): 2501-2513.

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

[41] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug&play system. *Phys. Rev. A* **74**, 042342 (2006).

[42] We perform a proof-of-principle decoy-state implementation, in which Alice modulates different intensities via her VOA without randomization. This method has been widely used in decoy-state experiments (see for instance [18, 20]). It is straightforward to implement a general modulation via adding another intensity modulator by following [10].

[43] Horodecki, R., Horodecki, P., Horodecki, M. & Ruskai, M. B. Quantum and classically correlated states. *Commun. Math. Phys.* **240**, 387 (2003).

[44] Barnett, S. M., Tiefenbacher, S., Tittel, W. Quantum communication with continuous variable systems. *Phys. Rev. Lett.* **81**, 2913 (1998).

[45] Wang, X.-B., Peng, C.-Z., Zhang, J., Yang, L. & Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **77**, 042311 (2002).

[46] Hoeffding, W. Probability inequalities for sums of bounded random variables. *Journal of the American statistical association* **49**, 25 (1954).

[47] Patel, K. A. et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl. Phys. Lett.* **104**, 051123 (2014).

[48] Yariv, A. & Yeh, P. Photonics: Optical electronics in modern communications. Oxford University Press (2007).

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

[50] Zelmon, D. E., Small, D. L. & Jundt, D. Infrared corrected Sellmeier coefficients for congruently grown lithium niobate and 5 mol.% magnesium oxidized lithium niobate. *Journal of the Optical Society of America B* **14**, 3319 (1997).

[51] Suhara, T. & Fujimura, M. Waveguide nonlinear-optic devices. *Springer* **11**, (2003).

[52] Xu, F., Qi, B., & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12**, 113026 (2012).

[53] Jiang, M.-S., Sun, S.-H., Li, C.-Y & Liang, L.-M. Frequency shift attack on 'plug-and-play' quantum key distribution systems. *Journal of Modern Optics* **61**, 147 (2014).

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

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