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

Feihu Xu,[1,*] Shihan Sajeed,[2] Sarah Kaiser,[2] Zhiyuan Tang,[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: April 26, 2014)

Decoy-state quantum key distribution (QKD) is the 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 novel 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) enables an unconditionally secure means of expanding secret keys between spatially separated honest parties [1, 2]. It offers information-theoretic security for communication in theory [3]. In reality, however, for 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. Fortunately, the decoy-state method [4–6] solves this security issue perfectly and dramatically improves the performance of QKD with faint lasers. Several experimental groups have demonstrated that decoy-state BB84 is secure and feasible under real-world conditions [7–9]. As a result, decoy-state method has become a standard technique in many current QKD implementations [10–13].

Before this work, unfortunately, previous QKD experiments [7–13] have 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*. One the one hand, the single-photon components of the four BB84 states are assumed to remain strictly in two dimensions of Hilbert space. We call this *qubit* assumption. In practice, none of previous works have verified this assumption. Note that an attack to exploit the higher dimensionality of state preparation has been proposed in [14]. 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 *insecure* 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 [3] 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. 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 [12, 13], quantum coin flipping [15] and blind quantum computing [16].

Second, the security claims made by most of experiments were obtained under the assumption that the eavesdropper (Eve) is restricted to particular types of attacks (*e.g.*, collective attacks) or that the finite-key analysis is not rigorous (*e.g.*, the security does not satisfy the universally composable security definition [17, 18]). Unfortunately, such assumptions cannot be guaranteed in practice. Although Ref. [19] reports an attempt implementing the rigorous finite-key analysis proposed in [20], both the theory and experiment assume a perfect signal-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 [21]. This analysis is based on a combination of a rigorous security proof [20] and a novel finite-data analysis for the decoy-state method [22]. However, a real-life implementation to demonstrate the feasibility of this analysis is still missing.

Third, the security analysis of previous experiments often relies on rotational symmetries [3]. Hence, four BB84 states are required for the estimation of the so-called bit error rate and phase error rate. QKD protocols with three states, *i.e.*, three-state protocols, have been proposed [23, 24], but to our knowledge, a decoy-state implementation of three-state protocol has not been reported in the literature.

II. RESULTS

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 [25], which allows QKD protocols that are loss-tolerant

*Electronic address: feihu.xu@utoronto.ca

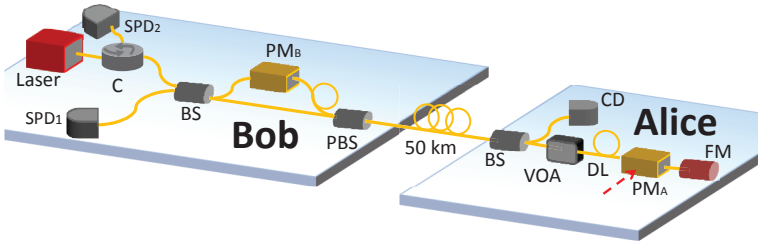

FIG. 1: **Setup.** Optical setup for ID-500 plug&play QKD system [26]. $\mathrm{SPD}_1/\mathrm{SPD}_2$, single-photon detector; C, circulator; $\mathrm{PM}_A/\mathrm{PM}_B$, phase modulator; BS, beam splitter; PBS, polarization beam splitter; CD, classical photo-detector; VOA, variable optical attenuator; DL, delay line; FM, Faraday mirror. PM_A randomly selects a phase from $\{0,\, \pi/2,\, \pi\}$ for the three-state experiment and from $\{0,\, \pi/2,\, \pi,\, 3\pi/2\}$ for the decoy-state BB84 experiment.

Parameter	Three-state	BB84
$s^L_{z,0}$	3.22×10^5	3.21×10^5
$s^L_{z,1}$	1.30×10^7	1.31×10^7
e_z	2.98%	2.89%
$e^U_{x,1}$	11.49%	6.01%
l	2.60×10^6	7.70×10^6
R^L	5.21×10^{-5}	1.54×10^{-4}

TABLE I: **Experimental results.** These values are obtained by plugging the raw counts into the decoy-state estimations (see Supplementary) and the key rate formula of Eq. (1).

to state-preparation flaws. We call it *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. It requires no side channel in the source. 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.

Theory: 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, building on [25], we propose a finite decoy-state method for QKD with three states and show that QKD with three states gives almost the same key rate as BB84 in a practical setting with a reasonable data-set. The three-state scheme can simplify conventional BB84 implementations, especially for those based on four laser sources [8, 11], where one could keep one laser just as back-up in case certain laser fails, without any decrease in performance. Third, based on [21], we provide a rigorous finite-key analysis for the loss-tolerant protocol, thus make this protocol applicable in a practical setting. The $\varepsilon_{\mathrm{sec}}$-secret key length in the Z basis is given by [21]

$$\ell \geq s^L_{z,0} + s^L_{z,1} - s^L_{z,1} h\left(e^U_{x,1}\right) - \mathrm{leak}_{\mathrm{EC}} - 6\log_2\frac{21}{\varepsilon_{\mathrm{sec}}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}, \quad (1)$$

where $h(y)$=$-y\log_2 y-(1-y)\log_2(1-y)$ is the binary entropy function; $s^L_{z,0}$, $s^L_{z,1}$ and $e^U_{x,1}$ are, respectively, the lower bound of vacuum events, the lower bound of single-photon events, and the upper bound of the phase error rate for single-photon events in Z basis, which can be estimated using the decoy-state method [21]; $\mathrm{leak}_{\mathrm{EC}} = n_{z,\mu} f_e h(e_z)$ 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 $f_e \geq 1$ is the error correction inefficiency function; $6\log_2\frac{21}{\varepsilon_{\mathrm{sec}}}$ and $\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}$ are respectively the secrecy and correctness parameter. ℓ quantifies the lower bound of key length and the key rate is given by R^L=ℓ/N with N denoting the total number of signals (pulses) sent by Alice. This key formula uses the min-entropy security proof [20] and fulfills the composable security definition [17, 18].

Experiment: On the experimental side, with a commercial ID-500 plug&play QKD system [26] (see Fig. 1), we perform the first decoy-state QKD demonstration considering source flaws. We quantify these flaws experimentally and include them in the key rate formula. We find that in ID-500 system, the voltage value $\{0,\, 0.77,\, 1.59,\, 2.36\}$ V is used for the phase modulation $\{0,\, \pi/2,\, \pi,\, 3\pi/2\}$ and the modulation error $\delta \leq 0.127$. We have also measured such error in an updated version of commercial plug&play system (IDQ Clavis2) and found that $\delta \leq 0.147$.

Based on the loss-tolerant protocol, we successfully generate secure keys over 50 km standard telecom fiber. Meanwhile, we for the first time apply the tight decoy-state finite-key analysis [21] in a real-life implementation and generate keys that are secure against general attacks in the universally composable framework. Furthermore, 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.

In the implementation of the three-state protocol, 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 $1:2:1$. We chose to operate the system for about 3 hours and send a total number of pulses N=5×10^{10}. Before the experiment, we performed a numerical optimization [10]

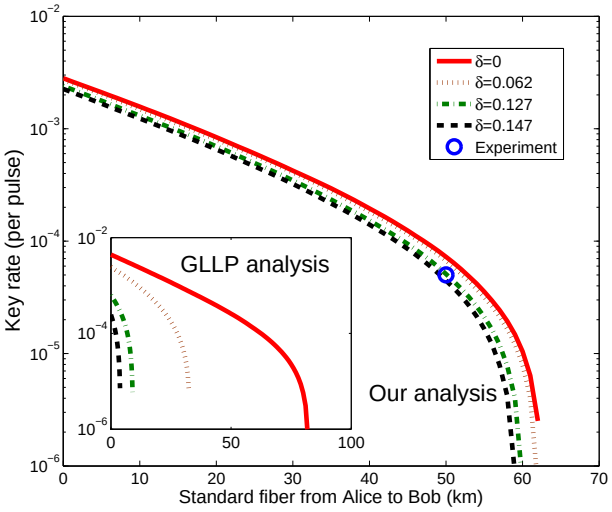

FIG. 2: Decoy-state QKD with source flaws in a practical setting. The main figure is for the three-state protocol based on our security analysis, while the inserted figure is for the decoy-state BB84 protocol based on GLLP security analysis. The power of our security analysis is explicitly shown by the 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 (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 δ=0).

on the implementation parameters. The experimental results are listed in Table I. Based on the three-state (BB84) protocol with our loss-tolerant security analysis, we got a QBER 2.98% (2.89%) and a lower bound of secure key generation rate 5.21×10^{-5} (1.54×10^{-4}) per pulse, and about 2603 (7700) kbit of unconditionally secure keys are exchanged between Alice and Bob.

As a comparison to previous security analysis, with the source flaws δ=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 [3]. In other words, at 50 km, not even a single bit could be shared between Alice and Bob with guaranteed security. This means that the key generation might be actually *insecure* in previous long-distance decoy-state experiments [7–11] if considering source flaws. In contrast, our analysis can easily achieve high secure key generation rate over long distances in the presence of source flaws.

Simulation: We perform a simulation to numerically study our security analysis in a practical setting. Fig. 2 shows the simulation results, where similar to our experiment, we use N=5×10^{10} and ϵ=10^{-10}. For comparison, this figure also includes the key rate for the decoy-state BB84 based on the GLLP security analysis. 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. This is because GLLP considers the worst case scenario where losses can increase the source flaw [3]. 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.

More details can be seen in the Supplementary Material. Supplementary Material is unpublished results and confidential.

[1] Gisin, N. *et al*. *Rev. Mod. Phys.* **74**, 145–195 (2002).
[2] Scarani, V. *et al*. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
[3] Gottesman, D., Lo H.-K., Lütkenhaus, N. & Preskill, J. *Quant. Inf. Comput.* **4**, 325 (2004).
[4] Hwang, W.-Y. *Phys. Rev. Lett.* **91**, 057901 (2003).
[5] Lo, H.-K., Ma, X. & Chen, K. *Phys. Rev. Lett.* **94**, 230504 (2005).
[6] Wang, X.-B. *Phys. Rev. Lett.* **94**, 230503 (2005).
[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] Dixon, A., Yuan, Z., Dynes, J., Sharpe, A., & Shields, A. *Opt. Exp.* **16**, 1879018979 (2008).
[10] Lucamarini, M. *et al*. *Opt. Express* **21**, 2455024565 (2013).
[11] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S. & Weinfurter H. *Nat. Photon.* **7**, 382386 (2013).
[12] Lo, H.-K. Curty, M. & Qi, B. *Phys. Rev. Lett.* **108**, 130503 (2012).
[13] Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I., & Tittel, W. *Phys. Rev. Lett.* **111**, 130501 (2013).
[14] Sun, S.-H., Jiang, M.-S. & Liang, L.-M. *Phys. Rev. A* **83**, 062331 (2011).
[15] Berlín, G., Brassard, G., Bussiéres, F., Godbout, N., Slater, J. A., & Tittel, W. *Nat. Commun* **2**, 561 (2011).
[16] Dunjko, V., Kashefi, E., & Leverrier, A. *Phys. Rev. Lett.* **108**, 200502 (2012).
[17] Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J. *Theory of Cryptography*, 386-406, Springer (2005).
[18] Renner, R. & König, R. *Theory of Cryptography*, 407425, Springer (2005).
[19] Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. *Nat. Commun* **2**, 2363 (2013).
[20] Tomamichel, M., Lim, C. C.-W., Gisin, N. & Renner, R. *Nat. Commun* **3**, 634 (2012).
[21] Lim, C. C.-W., Curty, M., Walenta, N. Xu, F. & Zbinden, H. *Phys. Rev. A* **89**, 022307 (2014).
[22] Curty, M., Xu, F., Cui, W., Lim, C. C.-W., Tamaki, K. & Lo, H.-K. (to be published in *Nat. Commun.*) Preprint arXiv: 1307.1081 (2013).
[23] Boileau, C., Tamaki, K., Batuwantudawe, J., Laflamme, R. & Renes, J. *Phys. Rev. Lett.* **94**, 040503 (2005).
[24] Fung, C.-H. F. & Lo, H.-K. *Phys. Rev. A* **74**, 042342 (2006).
[25] Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Preprint arXiv: 1312.3514 (2013).
[26] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. *New J. Phys.* **4**, 41 (2002).