Finite-key security analysis of quantum key distribution with imperfect light sources

Akihiro Mizutani*,[1] Marcos Curty,[2] Charles Ci Wen Lim,[3] Nobuyuki Imoto,[1] and Kiyoshi Tamaki[4]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[3] *Group of Applied Physics, University of Geneva, Geneva CH-1211, Switzerland*
[4] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*
* *mizutani@qi.mp.es.osaka-u.ac.jp*

Abstract.
In recent years, the gap between theory and practice in QKD has been significantly narrowed, particularly for QKD systems with arbitrarily flawed optical receivers. The status for QKD systems with imperfect light sources is however less satisfactory, in the sense that the resulting secure key rates are often overly-dependent on the quality of state preparation. This is especially the case when the channel loss is high e.g., the key rate significantly decreases with slight state preparation flaw [1] in the high-loss regime. Here, we derive security bounds for a wide class of realistic light sources and show that the bounds are also efficient in the presence of high channel loss. Our results strongly suggest the feasibility of long distance provably-secure communication with imperfect light sources.

Introduction.
Although state preparation flaws, such as multi-photon emissions or modulation errors in modulators for information-encoding, are common problems in QKD experiments, a few considerations have been made. The former problem can be solved by the use of the decoy state method, however, the latter does not have an adequate solution. In particular, it has been shown by Gottesman *et al* [1] that such inaccuracies in encoding can lead to very pessimistic secret key rates in the presence of high quantum channel loss. Very recently, a loss-tolerant QKD protocol has been proposed by Tamaki *et al* as a means to overcome typical encoding flaws in QKD systems [2]. For example, if the quantum states are encoded into the polarization degree-of-freedom of photons, an encoding flaw could be due to a misalignment in the wave-plate used to set the desired polarization. The loss-tolerant protocol is similar to the Bennett-Brassard 1984 (BB84) QKD scheme, but instead of considering all the four BB84 states, it uses only three of them. Interestingly, by considering statistics beyond those of the BB84 protocol, the resulting secret key rate is the same as the one of BB84's. More importantly, the secret key rate has the very nice property in that it is almost independent of encoding flaws. These results imply that the usual stringent demand on precise state preparation can be considerably relaxed and one only needs to know the prepared states. Additionally, it is useful to mention that most current BB84 QKD systems can easily switch to the loss-tolerant QKD protocol without much hardware modifications. In anticipation that the loss-tolerant QKD protocol will be widely implemented in the near future, we extend the security analysis in Ref. [2] to the finite-key regime, *i.e.*, we derive explicit bounds on the extractable secret key length (in [3], the authors have implemented the loss-tolerant protocol experimentally with careful verification of the qubit assumption used in the protocol. This paper also includes some finite-key analysis of the protocol. Unfortunately, however, its phase error rate estimation seems to be valid only against collective attacks). Furthermore, our bounds can be applied to a wide range of imperfect light sources—including typical cases whereby the intensity of the laser is fluctuating between a certain range. Also, the security bounds are obtained within the so-called universal-composable framework [4], and thus secret keys generated using these bounds can be applied to other cryptographic tasks like the one-time-pad. In order to investigate the feasibility of our results, we consider a QKD system model that borrows parameters from recent fiber-based QKD experiments. With this realistic model, our numerical simulations show that provably-secure keys can be distributed up to a fiber length of about 120 km, even when only 10^{11} signals are sent by Alice to Bob.

Assumptions on Alice and Bob's devices.
We consider that Alice's transmitter contains a laser source, an amplitude modulator and a phase modulator. See Fig. 1. The laser is single-mode and emits signals with a Poissonian photon number distribution. Also, we assume that Alice encodes the bit and the basis information in the relative phase $\theta_{\rm A}$ between a signal and a reference pulse, whose joint phase is perfectly randomized. Let us emphasize, however, that the security proof that we provide in this paper applies as well to other coding schemes like, for instance, the polarization or the time-bin coding schemes. Next we present the two types of imperfections that we consider for Alice's device.

Assumptions on Alice's apparatus.
1. *Intensity fluctuations.*
The fluctuation of the intensity of the emitted coherent light is typically due to the laser source and imperfec-

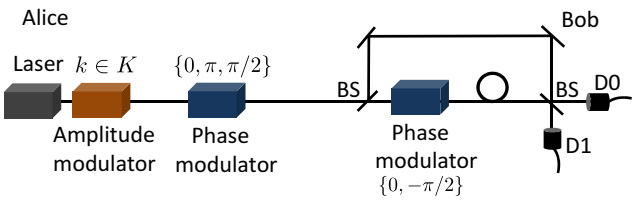

FIG. 1: In each trial, Alice's laser emits two consecutive coherent pulses representing the signal and the reference pulse. For this, she first uses an amplitude modulator to select the pulses' intensity $k \in K$. After that, she applies a phase shift $\{0, \pi, \pi/2\}$ to the signal pulse. On reception, Bob splits the received pulses into two beams and then applies a phase shift $\{0, -\pi/2\}$ to one of them. Also, he applies a one-pulse delay to one of the arms of the interferometer and then recombine the pulses at a 50:50 beamsplitter (BS). A "click" in detector D0 (D1) provides Bob the key bit $y' = 0$ ($y' = 1$).

tions in the amplitude modulator. Here we shall consider that Alice does not have a full description of the probability density function of the fluctuations, but she only knows their range [1]. That is, she knows that the intensity $k \in K = \{k_s, k_{d1}, k_{d2}\}$ of the emitted coherent light lies in an interval $k \in [k^-, k^+]$ except with error probability ϵ_{inten}, where $k^{+(-)}$ is the upper (lower) intensity. For simplicity, we shall assume that $\epsilon_{\text{inten}} = 0$. If $\epsilon_{\text{inten}} > 0$ this error probability can be directly taken into account through the security parameter. The intensities of the signal and reference pulses are $k^{\text{sig}} := kV$ and $k^{\text{ref}} := k(1-V)$ respectively, with $0 < V < 1$.

2. *Imperfect encoding of the bit and basis information.* In our protocol, Alice chooses the relative phase θ_A at random from $\{0, \pi/2, \pi\}$ to encode the bit and basis information. The phase $\theta_A \in \{0, \pi\}$ corresponds to the Z basis states which are selected with equal probability, and $\theta_A = \pi/2$ denotes the X basis state. Alice assigns a bit value $y = 0$ to $\theta_A \in \{0, \pi/2\}$ and a bit value $y = 1$ to $\theta_A = \pi$. Due to the misalignment of the optical system, however, the actual relative phase prepared by Alice may deviate from the desired angle θ_A by a factor $\Delta\theta_A$. Alice does not need to know the origin of the encoding errors $\Delta\theta_A$, but we assume that she knows the probability distribution $p(\Delta\theta_A)$ of $\Delta\theta_A$. Also, we assume that $p(\Delta\theta_A)$ is independently and identically distributed for each run of the protocol. Moreover, we consider that there are no side-channels in Alice's device.

Assumptions on Bob's apparatus.

[1] Note that in those scenarios where Alice knows the exact probability distribution of the fluctuations then the conventional decoy-state method can be directly applied.

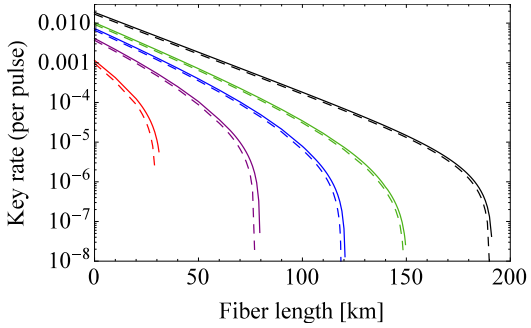

FIG. 2: (Color online) Secret key rate (per pulse) in logarithmic scale vs fiber length for the case with exact intensity control. The security parameter is $\epsilon_{\text{sec}} = 10^{-10}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = 9, 10, 11$ and 12 (from left to right). The rightmost two lines correspond to the asymptotic secret key rate with two decoy settings. The solid lines denote the case ξ=0 (*i.e.*, the perfect encoding scenario) while the dashed lines show the case ξ=0.147 (this error parameter is measured in an updated version of a commercial plug&play system (ID Quantique Clavis2) [3]). The experimental parameters are described in the main text.

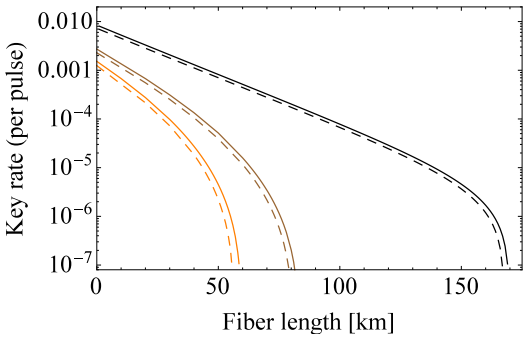

FIG. 3: (Color online) Secret key rate (per pulse) in logarithmic scale vs fiber length when the intensity fluctuation is 5%. The security parameter is $\epsilon_{\text{sec}} = 10^{-8}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = \{14, 15\}$ (from left to right). The rightmost two lines correspond to the asymptotic secret key rate with two decoy settings. The solid lines denote the case $\xi = 0$ (*i.e.*, the perfect encoding scenario) while the dashed lines show the case $\xi = 0.147$ (which is equivalent to a phase modulation error of 8.42°). The experimental parameters are described in the main text.

We consider that the detection efficiency of Bob's detectors is independent of his measurement basis choice. A phase value $\theta_B = 0$ ($\theta_B = -\pi/2$) corresponds to a device parameter to choose the Z (X) basis for the measurement. Also, like in the case of Alice, we consider that Bob uses an imperfect phase modulator that shifts the phase of the incoming signals. Furthermore, we assume that there are no side-channels in Bob's device.

Simulation of the key rate.
We show the simulation result for a fiber-based QKD sys-

tem. Alice chooses the intensity of the laser from the set $\{k_{\rm s}, k_{\rm d1}, k_{\rm d2}\}$, where we fix the intensity of the weakest decoy state to $k_{\rm d2} = 2\times 10^{-4}$. Also, we assume that Bob uses an active measurement setup with two single-photon detectors with detection efficiency $\eta_{\rm det} = 15\%$ and a dark count probability $p_{\rm d} = 5\times 10^{-7}$. The attenuation coefficient of the optical fiber is 0.2dB/km and its transmittance is $\eta_{\rm ch} = 10^{-0.2D/10}$ with D denoting the fiber length. The overall misalignment error of the optical system is fixed to be $e_{\rm mis} = 1\%$. In addition, we assume an error correction leakage $\lambda_{\rm EC} = f_{\rm EC} N_{\rm s} h(e_z)$, where e_z is the bit error rate of the sifted key whose size is $N_{\rm s}$. Moreover, for simplicity, we consider that the error correction efficiency of the protocol is a constant number $f_{\rm EC}$=1.16 which does not depend on the size of the sifted key. We model the imperfection of Alice's (Bob's) phase modulator as $\Delta\theta_{\rm A} = \xi\theta_{\rm A}/\pi$ ($\Delta\theta_{\rm B} = -\Delta\theta_{\rm A}$). Also, we consider that the intensity fluctuation of the laser source lies in the interval $[k^-, k^+]$ with $k^- = (1-r)k$ and $k^+ = (1+r)k$ for a fixed value r.

In these conditions, we simulate the secret key generation rate for a fixed value of the correctness coefficient $\epsilon_{\rm c} = 10^{-15}$. For this, we perform a numerical optimization of the resulting secure key rate over the free parameters $p_z, p_{k_{\rm s}}, p_{k_{\rm d1}}, k_{\rm s}$ and $k_{\rm d1}$, where p_z is the probability that Alice (Bob) selects the Z basis, $p_{k_{\rm s}}$ is the probability that Alice selects the signal setting and $p_{k_{\rm d1}}$ is the probability that Alice selects the first decoy setting.

A. Key generation rate for the exact intensity control case.

The resulting secret key rate for this scenario, *i.e.* when $r = 0$, is shown in Fig. 2. The security parameter is $\epsilon_{\rm sec} = 10^{-10}$ and the total number of signals sent by Alice is $N = 10^s$ with $s = 9, 10, 11$ and 12. We consider two possible cases: $\xi = 0$ (*i.e.*, the perfect encoding case) and $\xi = 0.147$, which is equivalent to a phase modulation error of 8.42°. For comparison, Fig. 2 also includes the asymptotic secret key rate (*i.e.,* the key rate in the limit of infinitely large keys) with two decoy settings.

As a result, we find that the effect of state preparation flaws on the key generation rate is almost negligible. Also, we have that if the total number of signals sent by Alice is about $N = 10^{12}$, Alice and Bob can exchange secret keys over 150 km both when $\xi = 0$ and $\xi = 0, 147$.

B. Key generation rate for the intensity-fluctuation case.

We also evaluate the resulting secret key rate when the laser source suffers from intensity fluctuations. We study the case for $r = 0.05$. The result is shown in Fig. 3. Here we consider that $N = \{10^{14}, 10^{15}\}$, and the term ξ takes again the values $\xi = 0$ and $\xi = 0.147$. The security parameter is $\epsilon_{\rm sec} = 10^{-8}$ in Fig. 3.

For comparison, Fig. 3 also shows the asymptotic secret key rate when Alice and Bob use two decoy settings. In this asymptotic case, we find that the degradation on the achievable key rate, when compared to the scenario $r = 0$, is only about 20 km.

In the finite-key regime, however, we obtain that the presence of intensity fluctuations seems to strongly limit the key generation rate if Alice and Bob do not know their probability distribution but only know the interval where the fluctuations lie in. The main technical reason for this behavior seems to be the fact that Azuma's inequality [5] has a relatively slow convergence speed when compared to the Chernoff bound [6] and the Multiplicative Chernoff bound [7].

Conclusion.

In summary, we have provided explicit security bounds for the loss-tolerant QKD protocol in the finite-key regime. On the application front, our results constitute an important step towards practical QKD with imperfect light sources, in that the resulting security performance is robust against encoding inaccuracies like, for instance, optical misalignment. Furthermore, our results take into account intensity fluctuations in the light source, which is a common experimental fact. Our results highlight the importance of the stable control of the intensity modulator as well as the need for a precise estimation of its intensity, which is not often sufficiently emphasized in the experiments.

Acknowledgements.

AM acknowledges support from the JSPS Grant-in-Aid for Scientific Research(A) 25247068. MC thanks the Galician Regional Government (program "Ayudas para proyectos de investigacion desarrollados por investigadores emergentes", and consolidation of Research Units: AtlantTIC), and the Spanish Government (project TEC2014-54898-R) for financial support. KT acknowledges support from the National Institute of Information and Communications Technology (NICT) of Japan (Project "Secure Photonic Network Technology" as part of Project UQCC) and the ImPACT program.

[1] Gottesman D *et al* 2004 *Quantum Inf. Comput.* **4** 325
[2] Tamaki K *et al* 2014 *Phys. Rev. A* **90** 052314
[3] Xu F *et al* 2014 arXiv:1408.3667
[4] Müller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[5] Azuma K 1967 *Tohoku Math. J.* **19** 357
[6] Chernoff H 1952 *Ann. Math. Sat.* **23** pp.493-507
[7] Curty M *et al* 2014 *Nature Commun.* **5** 3732