# Towards secure QKD with testable assumptions on modulation devices

Akihiro Mizutani,[1] Yuichi Nagamatsu,[1] Marcos Curty,[2] Hoi-Kwong Lo,[3] Koji Azuma,[4]
Rikizo Ikuta,[1] Takashi Yamamoto,[1] Nobuyuki Imoto,[1] and Kiyoshi Tamaki[4]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *EI Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[3] *Center for Quantum Information and Quantum Control, Dept. of Physics and Dept. of Electrical & Computer Engineering, University of Toronto, M5S 3G4 Toronto, Canada*
[4] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*

Quantum key distribution (QKD) is one of the most promising quantum information processing applications, and is now on the verge of global commercialization. Having said that, however, there are still some problems both theoretically and experimentally that need to be solved. One serious problem is to establish *practical security proofs* to bridge the gap between theory and practice. As QKD is physical cryptography, in the security proofs we have to assume some mathematical models for Alice and Bob's devices. However, if these models do not faithfully represent the physical properties of actual QKD devices, the security of the actual QKD systems is no longer guaranteed. In fact, such discrepancies between the device models in security proofs and the properties of the actual devices can be exploited by Eve to attack the source device [1, 2] and the detection unit [3]. Therefore, it is urgently required to establish security proofs based on practical devices for realizing secure communication.

QKD employs a source device and a detection unit, and we have to consider filling the gaps of both of them. Regarding the detection unit, thanks to the measurement-device-independent (MDI) QKD protocol [4], secure communication is possible without any assumption on the measurement device. That is, the gap in the detection unit is completely closed. However, assumptions on the source device are still necessary even in the MDI QKD protocol, and hence to accommodate source imperfections in security proofs is of vital importance. Unfortunately, security proofs with practical light sources are so far less satisfactory in the sense that only a few security proofs have accommodated realistic imperfections in the source device. The dominant imperfections in the source device are intensity and phase modulation errors (see Fig.1). Regarding the phase modulation errors, the GLLP analysis [5] showed that such an imperfection puts a severe limitation on the key rate as well as on the achievable distance. To solve this problem, the loss-tolerant (LT) protocol [6] has been proposed recently as a means to overcome typical phase modulation errors in the actual QKD systems. We have extended the original security proof in the asymptotic regime [6] to the finite-key regime [7], which is also an important issue in practical security proofs (see Table I for a review of recent finite-key analyses). In [6, 7], it was shown that if the probability distribution of the phase modulation error in a qubit space follows an identically and independent distribution (IID), such an imperfection does not have a significant influence on the resulting secret key rate even when the channel loss is high. Also, experimental demonstrations of the LT protocol have been done recently in both the prepare-and-measure setting [8] and the MDI setting [9].

A crucial problem in the previous proofs [6, 7] is that the IID assumption on the phase modulation errors can hardly be satisfied in the actual encoding devices, basically due to their time-dependent noises and correlations. Even if the error distribution follows IID in reality, it is impossible in finite time to verify whether or not the distribution is indeed IID for each pulse. Therefore, the error model in [6, 7] is not testable in the experiment, and it

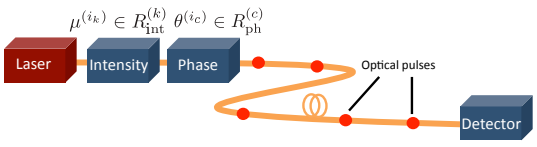


FIG. 1: Alice's source is composed of a laser source, an intensity modulator and a phase modulator.

| Ref. | Protocol | Source | Encoding flaws |
|---|---|---|---|
| [10, 11] | BB84 | Single-photon | No |
| [12–14] | BB84 | Coherent light | No |
| [7] | 3-state | Coherent light | IID phase, non-IID intensity |
| This work | 3-state | Coherent light | non-IID phase & intensity |

TABLE I: Review on recent finite-key analyses against coherent attacks. Refs. [10–14] assume that there are no encoding flaws in the source device, which cannot be guaranteed in practice. In our previous analysis [7], IID phase modulation errors and non-IID intensity fluctuation errors are accommodated. In this work [15, 16], we have generalized the source model assumed in [6], and we have accommodated non-IID properties in both phase and intensity modulators.

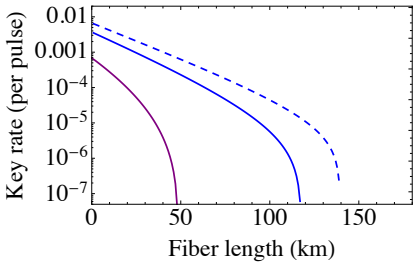


FIG. 2: Comparison in the secret key rate (per pulse) in logarithmic scale versus fiber length between our previous result [7] and our new result. These three curves show the case for $(r_k, \Delta\theta_c) = (0.05, 0)$. Regarding the two solid lines, the security parameter is $\epsilon_{\rm sec} = 10^{-10}$, and the right curve is for $N = 10^{12}$ based on our new result, and the left curve is for $N = 10^{14}$ based on the previous result [7]. The dashed line corresponds to the asymptotic case.

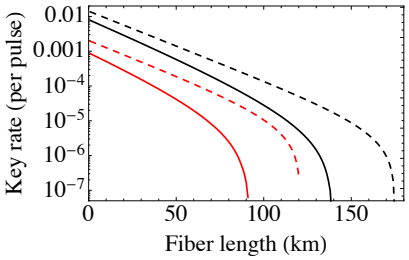


FIG. 3: Secret key rate (per pulse) in logarithmic scale versus fiber length. Regarding the solid lines, the security parameter is $\epsilon_{\rm sec} = 10^{-10}$, and the number of signals sent is $N = 10^{12}$. The right and left solid lines are for the case $(r_k, \Delta\theta_c) = (0, 0)$ and for the case $(r_k, \Delta\theta_c) = (0.03, 3\pi/180)$, respectively. The right and left dashed lines respectively show the case for $(r_k, \Delta\theta_c) = (0, 0)$ and $(0.03, 3\pi/180)$ with $N \to \infty$.

is not clear how to apply the security proof to guarantee the security of the actual QKD systems. Another important imperfection in the source device is due to intensity fluctuations. In the original decoy state method, stable control of intensity is required for better performance, and the effect of the fluctuation has to be taken into account into the security proof. In our previous work [7], we have accommodated this effect in the finite-key analysis. The assumption on the intensity fluctuation in [7] is that almost all the actual intensities lie in a certain interval. Note that there is no need to assume any particular distribution of the intensity fluctuation, and hence non-IID intensity modulation errors are accommodated. Unfortunately, with the mathematical methods used in [7], such an imperfection strongly limits the achievable secret key rate. More concretely, if one assumes an intensity fluctuation of $\pm 5\%$, we have that the achievable distance decreases down to 50km when Alice sends Bob $10^{14}$ signals (see Fig. 2). This strongly contrasts with the asymptotic result of 140km in the same situation, and constitutes a significant problem in practical security proofs. Therefore, we need to develop more efficient finite key analyses that takes into account intensity fluctuations.

Here, we solve these two significant problems on the practical source devices [15, 16]. Our first contribution is to establish a security proof based on potentially experimentally testable assumptions on the source device, which causes dominant imperfections. More specifically, we generalize the phase modulation errors in [6, 7] to accommodate non-IID phase modulation errors and prove the security against coherent attacks in the finite-key regime. The second contribution is to generalize the previous decoy-state method [7] to improve the performance under intensity fluctuation errors.

*Main results.*— Here, we first summarize all the assumptions we make on Alice's source. After that we describe our main results in detail.

(i) Assumptions on the sending states

Alice's sending states are in a single-mode and the photon number distributions follow a Poissonian distribution in any chosen basis, bit and intensity. Also, the joint phase between a signal and a reference pulse is randomized. Moreover, we assume that there are no side-channels in Alice's source.

(ii) Intensity of emitted light

We assume that the intensity of the emitted light lies in a certain interval except for error probability $\epsilon_{\rm int}^{(k)}$.

$$\Pr[|\{i_k|\mu^{(i_k)} \in R_{\rm int}^{(k)}\}| \geq N_k - \delta_{\rm int}^{(k)}] \geq 1 - \epsilon_{\rm int}^{(k)} \quad (1)$$

Here, $\mu^{(i_k)}$ denotes the intensity of the $i_k^{\rm th}$ coherent pulse when Alice selects the intensity $k \in \mathcal{K} = \{k_1, k_2, k_3\}$. $R_{\rm int}^{(k)}$ is a certain interval of the intensity. $N_k$ denotes the number of emitted light pulses with $k \in \mathcal{K}$, and $\delta_{\rm int}^{(k)}$ denotes the number of intensities that do not lie within the interval $R_{\rm int}^{(k)}$. $|*|$ denotes the cardinality of a set $*$.

(iii) Relative phase of emitted light

We assume that the relative phase of the emitted light lies in a certain interval except for error probability $\epsilon_{\rm ph}^{(c)}$.

$$\Pr[|\{i_c|\theta^{(i_c)} \in R_{\rm ph}^{(c)}\}| \geq N_c - \delta_{\rm ph}^{(c)}] \geq 1 - \epsilon_{\rm ph}^{(c)} \quad (2)$$

Here, $\theta^{(i_c)}$ denotes the $i_c^{\rm th}$ relative phase between two consecutive coherent pulses when the bit and basis information is $c \in \mathcal{C} = \{0_Z, 1_Z, 0_X\}$. $R_{\rm ph}^{(c)}$ is a certain interval of the relative phase. $N_c$ denotes the number of emitted pulses with $c \in \mathcal{C}$, and $\delta_{\rm ph}^{(c)}$ denotes the number of phases that do not lie within the interval $R_{\rm ph}^{(c)}$.

The assumptions (ii) and (iii) on the intensity and the phase modulations mean that each intensity and relative phase generated almost surely lies inside a particular interval, which can be potentially guaranteed in the actual experiments. Importantly, given the intervals $R_{\rm int}^{(k)}$ and $R_{\rm ph}^{(c)}$, we do not need to care anymore about the particular distributions of the phase and the intensity for each trial,

and arbitrary correlations among phases and intensities are allowed.

Based on these three assumptions, we prove the security against coherent attacks in the finite-key regime. More specifically, we establish the estimation method for Eve's leaked information accommodating the dominant imperfections. As for the intensity fluctuation problem, the main innovation of this work is the generalization of the "intensity post-selection method" [12] to accommodate the intensity fluctuation (see Appendix D in the supplementary material for detail). As a result, we have obtained significant improvements over the previous result [7] (see Fig. 2). Moreover, the generalization of the previous proofs with IID phase modulation errors [6, 7] to non-IID phase modulation errors (see Appendix E in the supplementary material for detail) has a significant importance on the practical security of QKD because it enables us to realize secure communication with realistic phase modulators (see Fig. 3).

We now briefly discuss the simulation results of the key generation rate for a fiber-based QKD system. For simulation purposes, we assume the following experimental parameters [14]: the attenuation coefficient of the optical fiber is 0.2dB/km, and the detection efficiency and dark count probability of the single-photon detectors are, respectively, $\eta_{\rm det} = 10\%$ and $p_{\rm d} = 6 \times 10^{-7}$. The channel transmittance is given by $\eta_{\rm ch} = 10^{-0.2l/10}$ with $l$ denoting the fiber length. Also, the overall misalignment error of Bob's apparatus is assumed to be 1%. In addition, we assume an error correction leakage equal to $f_{\rm EC}|Z_{\rm tot}|h(e_Z)$, where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$, $|Z_{\rm tot}|$ is the number of detection events when Alice and Bob select the $Z$ basis, and $e_Z$ is the bit error rate of the sifted key. For simplicity, we assume an error correction efficiency $f_{\rm EC} = 1.16$ that is independent of the size of $|Z_{\rm tot}|$. In addition, we assume the phase interval $R_{\rm ph}^{(c)}$ as $[\theta_c - \Delta\theta_c, \theta_c + \Delta\theta_c]$ for a fixed value $\Delta\theta_c$ with $\theta_{0_Z} = 0, \theta_{1_Z} = \pi$ and $\theta_{0_X} = \pi/2$. Also, we assume the intensity interval $R_{\rm int}^{(k)}$ as $[(1-r_k)k, (1+r_k)k]$ for a fixed value $r_k$. Further, we assume $\delta_{\rm ph}^{(c)} = \delta_{\rm int}^{(k)} = \epsilon_{\rm ph}^{(c)} = \epsilon_{\rm int}^{(k)} = 0$ for all $k \in \mathcal{K}$ and $c \in \mathcal{C}$ for simplicity of the analysis.

With these parameters, we simulate the secret key generation rate $R := \ell/N$ for a fixed value of the correctness and secrecy parameters $\epsilon_{\rm c} = \epsilon_{\rm s} = 10^{-10}$. Here, $\ell$ and $N$ denote the secret key length and the number of emitted pulses by Alice, respectively (see Appendix C in the supplementary material for the derivation of $\ell$). For this, we perform a numerical optimization for $R$ over the free parameters $p_Z$, $p_{k_1}, p_{k_2}, k_1$ and $k_2$, where we fix the weakest decoy state to $k_3 = 2 \times 10^{-4}$. $p_Z$ and $p_k$ denote the probability of choosing the $Z$ basis and the intensity $k \in \mathcal{K}$, respectively. In Fig. 3, we show the resulting secret key rate with a phase modulation error of $\pm 3\pi/180$rad and intensity fluctuation of $\pm 3\%$. The left solid curve is for $N = 10^{12}$, and the left dashed line is for $N \to \infty$. For comparison, we plot the curves for the ideal case ($r_k = \Delta\theta_c = 0$). The right solid and right dashed lines are for $N = 10^{12}$ and $N \to \infty$, respectively. This result strongly suggests the feasibility of long distance secure communication with imperfections of $\pm 3\pi/180$rad phase modulation error and $\pm 3\%$ intensity fluctuation. In Fig. 2, to see how the intensity fluctuation alone affects the performance, we plot the key generation rate assuming the intensity fluctuation only. The two left curves show that the achievable distance of our new result is more than double than that in [7]. From this, we observe the dramatic improvement over the previous result [7].

*Conclusions.*— In this work, we establish a security proof based on potentially testable assumptions on the phase and the intensity modulations, which cause dominant imperfections in the source devices. As a result of our security proof, even if a realistic phase fluctuation of $\pm 3\pi/180$rad and intensity fluctuation of $\pm 3\%$ occur, we show that long distance secure communication is possible with reasonable times of signal transmission. Our result constitutes a significant step toward realizing secure quantum communication with practical devices.

*Acknowledgements.*—NI acknowledges support from the MEXT/JSPS KAKENHI Grant Number 16H02214. MC acknowledges support from the Galician Regional Government (program "Ayudas para proyectos de investigación desarrollados por investigadores emergentes" EM2014/033, and consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2014-54898-R. HKL acknowledges financial support from NSERC, CFI, ORF and the US Office of Naval Research (ONR). This work is in part funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Govement of Japan).

[1] S. Sajeed *et al*, Phys. Rev. A **91**, 032326 (2015).
[2] S.-H. Sun *et al*, Phys. Rev. A **92**, 022304 (2015).
[3] L. Lydersen *et al*, Nature Photon. **4**, 686 (2010).
[4] H.-K. Lo *et al*, Phys. Rev. Lett. **108**, 130503 (2012).
[5] D. Gottesman *et al*, Quant. Inf. Comput. **4**, 325 (2004).
[6] K. Tamaki *et al*, Phys. Rev. A **90**, 052314 (2014).
[7] A. Mizutani *et al*, New J. Phys. **17**, 093011 (2015).
[8] F. Xu *et al*, Phys. Rev. A **92**, 032305 (2015).
[9] Z. Tang *et al*, Phys. Rev. A **93**, 042308 (2016).
[10] M. Tomamichel *et al*, Nature Commun. **3**, 634 (2012).
[11] M. Hayashi *et al*, New J. Phys. **14**, 093014 (2012).
[12] M. Curty *et al*, Nature Commun. **5**, 3732 (2014).
[13] M. Hayashi *et al*, New J. of Phys. **16**, 063009 (2014).
[14] C. C. W. Lim *et al*, Phys. Rev. A **89**, 022307 (2014).
[15] Y. Nagamatsu *et al*, Phys. Rev. A **93**, 042325 (2016).
[16] A. Mizutani, M. Curty, H.-K. Lo, K. Azuma, R. Ikuta, T. Yamamoto, N. Imoto and K. Tamaki, in preparation.