Characterisation of state preparation uncertainty in quantum key distribution

Anqi Huang,[1] Akihiro Mizutani,[2] Hoi-Kwong Lo,[3,4,5] Vadim Makarov,[6,7,8] and Kiyoshi Tamaki[9]

[1] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*
[2] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[3] *Centre for Quantum Information and Quantum Control (CQIQC), Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*
[4] *Department of Physics, University of Hong Kong, Pokfulam, Hong Kong*
[5] *Quantum Bridge Technologies, Inc., 100 College Street, Toronto, Ontario M5G 1L5, Canada*
[6] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[7] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*
[8] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[9] *Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*

To achieve secure quantum key distribution, all imperfections in the source unit must be incorporated in a security proof and measured in the lab. Here we perform a proof-of-principle demonstration of the experimental techniques for characterising the source phase and intensity fluctuation in commercial quantum key distribution systems. We then apply the experimental results to the security proof that takes into account fluctuations in the state preparation and study the resulting secure key rates. Our characterisation methods pave the way for a future certification standard.

The loopholes in the source unit are the last obstacle to achieve security of quantum key distribution (QKD) in reality. The most effective solution to eliminate such security threat is to consider the practical imperfections of the source in the security model. The security proof of this loss-tolerant protocol [1] has been generalised to the case where Alice just has the knowledge of the intervals of the phase and intensity fluctuations of the coherent light source [2]. However, there is no methodology so far to characterise the fluctuation interval of the imperfect modulation in a practical QKD system [2].

Here we propose two methods of experimentally characterising fluctuation, one for phase and another for intensity. We apply each of them to a QKD system to obtain the intervals of phase and intensity fluctuation. By following the loss-tolerant protocol in Ref. 2, we treat the optical pulses that lie in this interval as untagged signals and the others as tagged signals. The probability that the optical pulses fall outside the interval is set at a certain small value. The secret key is then extracted from the untagged signals, and the information of the tagged signals is completely leaked to an eavesdropper.

To characterise the uncertainty of state preparation, the intervals of phase fluctuation are measured on a commercial plug-and-play QKD system Clavis2 from ID Quantique [3], and the intervals of intensity fluctuation are measured on a newer prototype QKD system running a decoy-state BB84 protocol with polarization encoding. The phase and intensity intervals are measured on two separate QKD systems because we have had no access to a QKD system that employs a phase-encoding loss-tolerant protocol with decoy-state method. However, the methodology of characterisation proposed in this work is general and applicable to the loss-tolerant QKD systems.

Experiment of phase characterisation. In order to study the methodology of fluctuation measurement and obtain the first data on the values of phase fluctuation interval in practical QKD systems, we conduct a proof-of-principle measurement to characterise it at the output of Alice in Clavis2 [3]. The latter's plug-and-play scheme [4] is quite suitable to measure the phase value, because it is inherently stable without active calibration. The assumptions, measurement setup, and characterisation procedure are described in detail in the appended full-length manuscript. The characterised distribution of phase fluctuation is shown in Fig. 1(a). Since the distribution fits well to Gaussian, we describe the real phase θ'_{A} by a mean value $\overline{\theta'_{\mathrm{A}}}$ and a standard deviation $\sigma_{\theta'_{\mathrm{A}}}$, listed in Table I.

Experiment of intensity characterisation. To demonstrate the method of characterising the intensity interval, we conduct a proof-of-principle experiment on another prototype BB84 QKD system that employs weak + vacuum decoy-state protocol [5] and polarization encoding. We measure the intervals for the signal, decoy, and vacuum state. The assumptions, measurement setup and characterisation procedure are described in detail in the appended full-length manuscript. The characterised distribution of intensity is shown in Fig. 1(b). Similarly to the phase distributions, the distributions of intensities are also nearly Gaussian, with their parameters listed in Table II. It is notable that, in theory, the vacuum state is zero. However, in practice, measurement is always affected by noise, so we obtain, in this particular instance, a small negative value.

The extracted intensity distributions are much wider relative to their mean values than the phase distributions. We attribute this to stochastic dynamic processes in Alice's gain-switched laser that generate energy noise (and timing jitter) of short pulses produced by it. As will

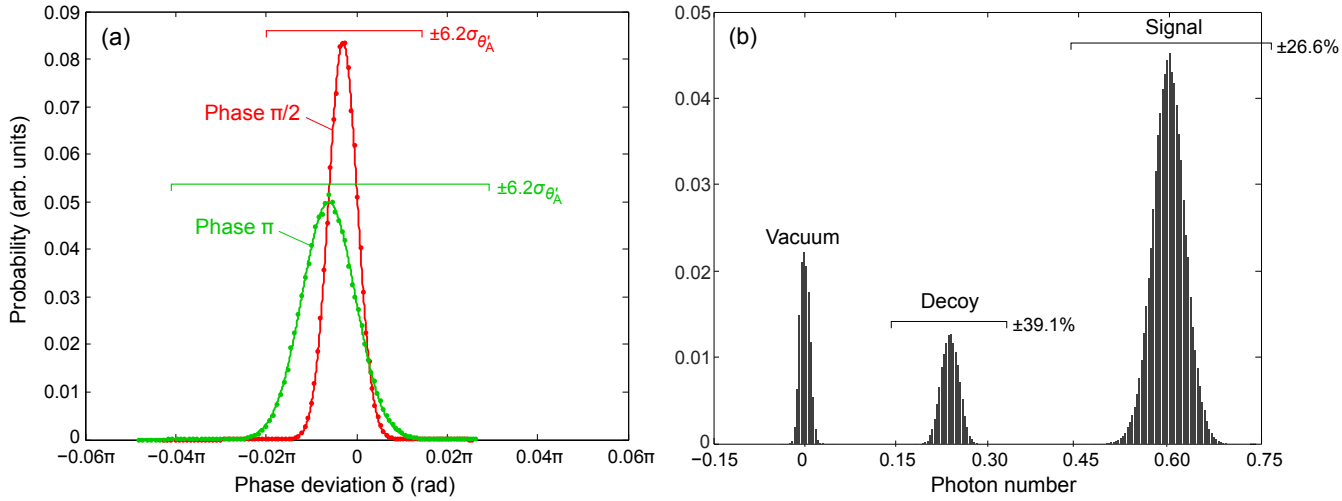

FIG. 1. Measured intervals. (a) Distributions of phases for different states. (b) Distributions of intensities for different states.

TABLE I. Parameters of Gaussian approximation of phase distributions.

Nominal phase θ_A	$\overline{\theta'_A}$	$\sigma_{\theta'_A}$
0	0	0
$\pi/2$	0.4970π	0.0028π
π	0.9939π	0.0057π

TABLE II. Parameters of Gaussian approximation of intensity distributions.

State	$\bar{\mu}$	σ_μ
Vacuum	-0.78×10^{-3}	0.0083
Decoy	0.236	0.0149
Signal	0.602	0.0258

be shown shortly, this leads to zero secure key rate with the available proof. This indicates that this simple gain-switched laser source may be unsuitable for secure QKD. Improvements to the source that reduce the laser's timing jitter might also reduce its energy noise and should be tested in future work.

Simulation of secret key rate. We employ the security proof and simulation technique proposed in Ref. 2 to calculate the secret key rate. We consider three cases: phase fluctuation only, intensity fluctuation only, and both phase and intensity fluctuation. The parameters commonly used in all these simulations are given in the appended full-length manuscript.

Case 1. Phase fluctuation only. We apply the experimental values of phase fluctuation from Table I. The signal and decoy intensities are optimised at each fiber length. The simulation results are shown in Fig. 2(a), which shows that secure key can be produced between Alice and Bob over more than 100 km of fiber with 10^{13} pulses sent, when the phase fluctuation only is considered. To see how much phase noise the system can tolerate, we have also run the simulation with an artificially increased fluctuation, which shows that the system keeps producing secret key until $\sim 2\sigma_{\theta'_A}$.

Case 2. Intensity fluctuation only. Because the measured intensity fluctuation is way too large for the secret key to be produced, we simulate performance of a system that has a fraction of the measured intensity fluctuation. This estimates how much the source has to be improved. We calculate the key rates with intensity fluctuation but no phase fluctuation under the following two scenarios. (a) The mean photon numbers are fixed and taken from the experimental results (Table II) but fluctuation interval is set to be ±0.5% or ±1% of $\bar{\mu}$. The resulting key rates are shown in Fig. 2(b). (b) The mean photon numbers are optimised for each fiber length and fluctuation interval is also set to be ±1% of $\bar{\mu}$. The results are shown in Fig. 2(c).

In scenario (a), while without the imperfection the distance reaches 90 km, a moderate amount of fluctuation of just ±0.5% (±1%) reduces it to 30 km (17 km). This high sensitivity to the fluctuation is attributed to our using the fixed mean photon numbers of the states. Remarkably, the fluctuation interval measured in the QKD system (Table II) is very large, ±39.1% of $\bar{\mu}$ for the decoy and ±26.6% of $\bar{\mu}$ for the signal state (corresponding to $\pm 6.2\sigma_\mu$). The hardware should thus be drastically improved to accommodate the available security proof. In scenario (b), optimising the mean photon numbers of the decoy and signal allows to tolerate the intensity fluctuation much better. The key rate at a short distance is not significantly reduced and the maximum transmission distance only decreases by about 13 km. For the same fluctuation interval of ±1%, the maximum distance reaches 123 km versus 17 km with the fixed photon numbers. This is a significant advantage.

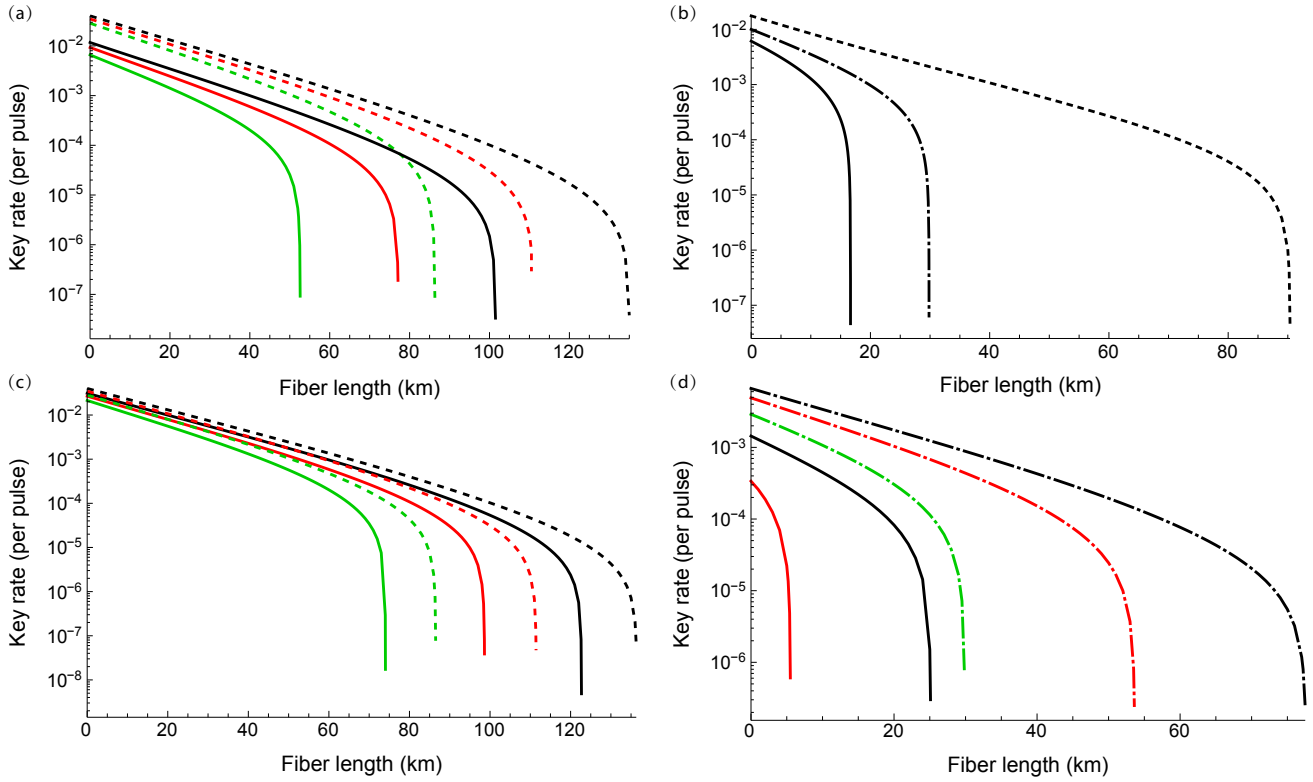

FIG. 2. Simulated key rates with (a) only phase fluctuation, (b) only phase fluctuation with fixed mean photon numbers, (c) only phase fluctuation with optimised mean photon numbers, and (d) both phase and intensity fluctuations. The number of pulses sent by Alice is 10^{13} for black lines, $10^{12.5}$ for red (dark grey) lines, and 10^{12} for green (light grey) lines. Dashed lines are for an ideal source. Other-styled lines are for sources with fluctuations, as detailed in main text.

Case 3. Phase and intensity fluctuation. We combine the phase-only and intensity-only fluctuation into one simulation. The result is shown in Fig. 2(d). Combining the phase and intensity fluctuation introduces some drop in the key rate and maximum distance. For example, with only ±1% intensity fluctuation, the maximum distance is 123 km for $N_{\text{sent}} = 10^{13}$ [black solid line in Fig. 2(c)], however when the phase fluctuation is added it drops to 78 km [black dash-dotted line in Fig. 2(d)]. When the intensity fluctuation is increased to ±3% [solid lines in Fig. 2(d)], the key rate and maximum distance decay rapidly, and no key is produced for the lowest $N_{\text{sent}} = 10^{12}$. This shows that controlling the intensity fluctuation in the QKD hardware is crucial, at least with the security proof currently available [2].

To summarise, we have proposed and experimentally demonstrated methodology for characterising source fluctuation in phase and intensity in QKD. We have then applied our characterisation results to the security proof of the three-state, loss-tolerant protocol [2]. The fluctuations lead to a significant reduction in the key rate and maximum transmission distance in fiber. In fact, the intensity fluctuation we measured is so large that the proof predicts no key. There is a room for improvement in the source hardware, especially to reduce its intensity fluctuation. Likewise the security proof and details of the QKD protocol might be improved to give a higher key rate at the same fluctuation. This may be helped by knowing the distribution of fluctuation (such as the Gaussian distribution we measured) [6]. The development of security proofs for other QKD protocols that incorporate source fluctuation is desirable. This characterisation methodology is a necessary element in the upcoming formal security standards and certification of QKD.

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

[2] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, and K. Tamaki, npj Quantum Inf. **5**, 8 (2019).

[3] Clavis2 specification sheet, `http://marketing.idquantique.com/acton/attachment/11868/f-00a0/1/-/-/-/-/Clavis%20QKD%20Datasheet.pdf`, visited 16 January 2018.

[4] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

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

[6] X. Sixto, V. Zapatero, and M. Curty, (manuscript in preparation).