An efficient countermeasure against correlated intensity fluctuations in optical pulses on high-speed decoy BB84 QKD systems

A. Tomita*, K. Yoshino†, M. Fujiwara‡, T. Sumiya§, T. Sasaki§, K. Nakata*, A. Tajima†, M. Koashi§, M. Takeoka‡, and M. Sasaki‡

*Hokkaido University, †NEC Corporation, ‡ National Institute of Communication and Information Technology, § University of Tokyo, JAPAN

Continuing efforts have been made to develop practical quantum key distribution (QKD) systems on the installed fiber networks since early 2000s [1]. Recently, several groups have demonstrated high-speed QKD systems [2,3] with GHz-clock frequency working stably on the installed-fiber networks [4-7]. Along with the hardware development, an efficient key management protocol [7] has been implemented to construct a QKD platform to supply information-theoretically secure key for multiple applications. The QKD platform with high availability is expected to promote social deployment of the QKD technology.

Nevertheless, there remains an obstacle that makes the potential users hesitate to accept this emerging technology; they won’t innovate their secure communication systems unless convinced that a QKD system at hand is really secure. The deployment of QKD technology therefore requires security certification, test-and-measurement method, and security criteria, acceptable for non-experts. To this end, we re-examine the assumptions of security analysis to extract potential loopholes, and develop evaluation methods with devices available in common laboratories. We also improve the protocol to make it immune to the newly discovered imperfection.

Currently, we focus on the transmitter, because the quality of the transmitted photon states is crucial to security certification, and all the receiver imperfections can be circumvented in principle [8]. We have investigated phase correlation between pulses and intensity fluctuation in a gain-switched semiconductor laser. We here turns our attention to the intensity modulators (IM) in decoy QKD systems, which provide optical pulses with different mean photon numbers. Our concern is that electrical signal distortion, which occurs inevitably in band-width limited high-speed systems, may cause intensity correlation between the optical pulse as well as intensity fluctuation in individual pulses. This issue has arisen in decoy QKD systems, where the imperfect intensity control affects the photon number distribution and results in inaccurate estimation on eavesdropper’s information. In contrast, conventional digital optical communication systems work with intensity fluctuation and correlation, as long as threshold-based decision is successful. Investigating the accuracy of optical pulse intensities is thus important for security certification of decoy QKD systems. The intensity correlation is particularly crucial, because most of the security analysis assume independent and identically distributed (IID) pulses. The correlation hinders us from applying the security analysis with confidence.

In this contribution, we report the measurement of the intensity fluctuation of each optical pulse of a GHz-QKD system. We observed large modulation-pattern dependent intensity deviation. As an efficient countermeasure against the correlation, we propose a combination of pattern sifting (PS) and alternate key distillation (AKD) to recovers the IID assumption. We also propose a method, intensity sifting (IS), to limit the residual random intensity fluctuation to by discarding out-of-range pulses after the quantum communication.

Figure 1 shows a conceptual view of our QKD transmitter working with 1.24-GHz clock. We employ three-state decoy-BB84 protocol and time-bin coding. The QKD system uses a dual-electrode lithium niobate (LN) intensity modulator (IM) of 10 GHz bandwidth, driven by an electrical circuit designed for 10-Gbps digital optical communication. The pulse intensities are defined with phase shift φ_i (i=1,2) at each waveguide as $I_{out} = \cos^2[(\varphi_1 - \varphi_2)/2]\ I_{in}$: $(\varphi_1, \varphi_2) = (0,0)$ for "signal" (S), $(\pi, 0)$ for "vacuum" (V), and (π, ϕ) for "decoy" (D), where ϕ is determined with designed decoy intensity. In the following we define "Hi" voltage as V_π and V_ϕ for electrodes 1 and 2, respectively, and "Lo" as 0 for both.

The observed electric pulses applied to the IM was distorted from the ideal waveform due to the limited bandwidth of the circuit as shown in the inset of Fig. 1(a),(b). The effect continued for several hundred picoseconds, which caused the pulse intensity dependence on the pulse pattern. We applied complementary modulation to limit the pattern effect within two pulse periods. The binary modulation signals (Hi or Lo) in the first half of the pulse period was inverted (Lo or Hi) in the second half, as depicted in inset of Fig. 1(a). The complementary modulation reduces the pulse patterns for investigation to six: S→S, D→S, V→S, S→D, D→D, and V→D, where the second pulses are to be measured. We measured the inter-pulse intensity correlation from the individual pulse area obtained with a high-speed photo-receiver (9.3-GHz bandwidth) and an oscilloscope (8-GHz bandwidth). We observed up to -20 % deviation in D→D, and V→D patterns from S→D, whereas the S pulses shows small deviation of 0.6-2.1 % for all the three patterns.

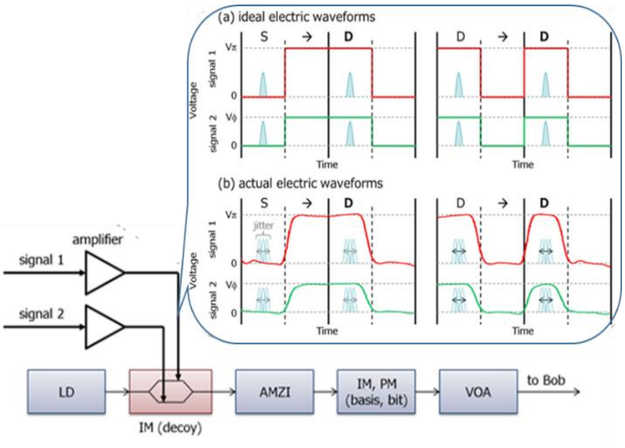
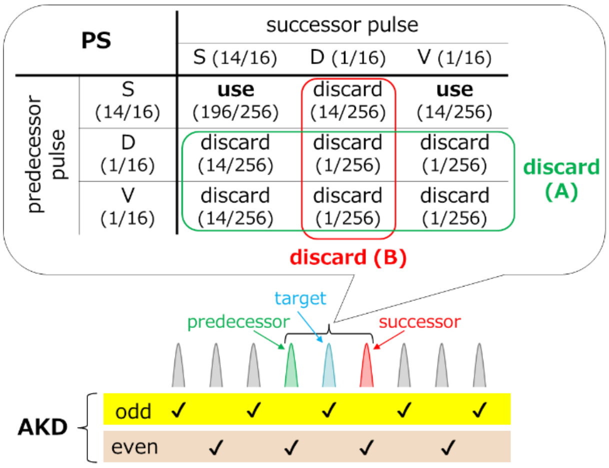


Fig. 1 Schematic view of a transmitter of a decoy BB84 QKD system.
(a) Ideal waveforms encoding signal (S) and decoy (D) with complementary modulation.
(b) Actual distorted waveforms

The pattern effect can be circumvented with pattern sifting (PS). The idea is simple; discarding particular modulation patterns that yield large intensity deviations. However, it is important the sifting rule should be independent of S, D, or V, otherwise sift itself may offer information on the intensity. The complementary modulation implies that the sifting rule should depend only on the states of the adjacent pulses. The intensity deviation can be suppressed by fixing predecessor pulse state to S and discarding the pulse whose successor is D. The latter rule reflects that D state intensity depends on the target pulse state. The rule is summarized as follows: (A) Discard the pulse, if its predecessor is in D- or V-state, (B) Discard the pulse, if its successor is in D-state. The correlation between the adjacent pulses can be disregarded effectively by alternate key distillation (AKD), where sifted keys are divided into odd-timing events and even-timing events according to the emission time stamps, and execute key distillation for each bit train. AKD works because pulse of odd (even) timing is independent of each other by applying the complementary modulation. The keys distillated individually can be combined because of the argument of the composability. The rules for PS and AKD are depicted in Fig. 2.

In conclusion, we have discovered, for the first time, modulation pattern dependent large intensity deviation, due to distortion of electric signals originated from the limited bandwidth of the electronics in a GHz-QKD system. The pattern effects emerge even 2.48 GHz (=1.24 GHz ×2) modulation by the devices compatible with 10 Gbps digital optical communication. The developed countermeasure, PS and AKD, which recovers the IID assumption common to most security proofs, yields reasonable key after 100-km transmission with the use of IS. The combination of PS, AKD and IS will provides simple and effective solution to wide range of high-speed QKD systems, where the signal distortion due to the limited bandwidth is frequently observed.

This work was partly supported by ImPACT Program (Cabinet Office, Government of Japan).



PS		successor pulse		
		S (14/16)	D (1/16)	V (1/16)
predecessor pulse	S (14/16)	use (196/256)	discard (14/256)	use (14/256)
	D (1/16)	discard (14/256)	discard (1/256)	discard (1/256)
	V (1/16)	discard (14/256)	discard (1/256)	discard (1/256)

Fig. 2. Summary of sifting rules in "pattern sifting (PS)" and pulse selection rules in "alternate key distillation (AKD)".
The numbers after S, D, and V show the typical values of the selection probability.
The number after use/discard shows the probability of each pulse pattern.

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**(1), 145–195 (2002).
2. J. F. Dynes, *et al.*, Opt. Express. **20**(15), 16339–16347 (2012).
3. K. Yoshino, *et al.*, Opt. Express **21**(25), 31395-31401 (2013).
4. C. Elliott, *et al.*, Proc. SPIE **5815**, 138–149 (2005); arXiv:quant-ph/0503058v2.
5. D. Stucki, *et al.*, New J. Phys. **13**(12), 123001, 1-18 (2011).
6. M. Peev, *et al.*, New J. Phys. **11**(7), 075001/1-37 (2009).
7. M. Sasaki, *et al.*, Opt. Express, **19**(11), 10387–10409 (2011).
8. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

Supplements

A Security proof of alternate key distillation

We will provide a brief proof of the security of the key after the alternate key distillation (AKD) and the pattern sifting (PS). To this end, we will analyze the sifted key from the even-indexed and pattern-sifted pulses and the odd-indexed and pattern-sifted pulses separately. We will apply an existing analysis of a standard decoy-state BB84 protocol to each set of pulses and obtain a final key by simply combining the outputs of these two analyses. If they were independent from each other, the security of the combined key could be understood as the usual argument of the universal composability. However, they are not independent, and we need to treat their dependence carefully.

To represent existing analyses of standard decoy-state BB84 protocols, we define $\mathbf{a}, \mathbf{n}$ and $\mathbf{\Lambda}$ as follows. $\mathbf{a}$ is a sequence whose element $a_i \in \{S, D, V\}$ represents the type (Signal, Decoy, or Vacuum, respectively) of the i-th pulse. $\mathbf{n}$ is a sequence whose element $n_i \in \{0, 1, \cdots\}$ represents the number of photons in the i-th pulse. $\mathbf{\Lambda}$ is a sequence whose element Λ_i represents the set of the other experimental outputs corresponding to the i-th pulse. Existing security proofs of standard decoy-state BB84 protocols usually consist of the following two parts. The first part (a) is to estimate a photon number distribution in a sifted key. This analysis relies on the assumption that the probability distribution $\Pr(\mathbf{a}, \mathbf{n})$ is written as $\prod_i f(a_i, n_i)$ with some function f, and $\mathbf{a}$ affects $\mathbf{\Lambda}$ only through $\mathbf{n}$, which can be represented as a Markov chain $\mathbf{a} \to \mathbf{n} \to \mathbf{\Lambda}$. The latter assumption corresponds to the understanding that the state emitted from the source does not depend on $\mathbf{a}$ once $\mathbf{n}$ is fixed. In existing analyses, we make a rule to determine quantities, such as a lower bound of the number of detections for single-photon signals, from $\mathbf{a}, \mathbf{\Lambda}$ and the form of f. To represent this process, we define Ω and Γ as the set of $(\mathbf{a}, \mathbf{n}, \mathbf{\Lambda})$ and a set of Ω which is consistent with the rule under an admissible failure probability ϵ_1, respectively. The part (a) guarantees that the failure probability of this process is smaller than ϵ_1, *i.e.* $\Pr(\Omega \notin \Gamma) < \epsilon_1$. The second part (b) is to prove that the protocol is ϵ_2-secure with a failure probability $\Pr(\Omega \notin \Gamma)$.

To apply an existing analysis to our experiment, we need to pay attention to the pattern effect, which causes that the i-th type a_i affects n_{i+1} as well as n_i. Although it disturbs the form of $\Pr(\mathbf{a}, \mathbf{n})$ and prevents us to apply (a) to our experiment, the dependence of the pairs (a_i, n_i) has a sequential order which means a Markov chain $(a_1, n_1) \to (a_2, n_2) \to (a_3, n_3) \to \cdots$. It means that the pairs (a_i, n_i) for even indices become independent if we fix the pairs (a_i, n_i) for the odd indices. It can be written as $\Pr(\mathbf{a}^{\mathrm{even}}, \mathbf{n}^{\mathrm{even}} | \mathbf{a}^{\mathrm{odd}}, \mathbf{n}^{\mathrm{odd}}) = \prod_j f_{2j}\left(a_{2j}, n_{2j}\right)$, where the superscripts "even" and "odd" represent the restriction on the even-indexed elements and the odd-indexed elements, respectively. The forms of functions f_{2j} depend on $\mathbf{a}^{\mathrm{odd}}$ and $\mathbf{n}^{\mathrm{odd}}$ and are not necessarily identical because of the pattern effect. If we fix $2j$ to be an index surviving the pattern sifting, $f_{2j}\left(a_{2j}, n_{2j}\right)$ is equal to $f(a_{2j}, n_{2j})$, where f is the function assumed in (a). Even under the pattern effect, the state emitted from the source does not depend on $\mathbf{a}$ once $\mathbf{n}$ is fixed. It also holds if we restrict their indices. Then, we obtain a Markov chain $\mathbf{a}^{\mathrm{even,ps}} \to \mathbf{n}^{\mathrm{even,ps}} \to \mathbf{\Lambda}^{\mathrm{even,ps}}$ under given $\mathbf{a}^{\mathrm{odd}}$ and $\mathbf{n}^{\mathrm{odd}}$, where "ps" in the superscript represents the restriction on the indices surviving the pattern sifting. Since the assumptions required for (a) are satisfied in the even-indexed and pattern-sifted elements, we can apply (a) to them and obtain $\Pr(\Omega^{\mathrm{even,ps}} \notin \Gamma \mid \mathbf{a}^{\mathrm{odd}}, \mathbf{n}^{\mathrm{odd}}) < \epsilon_1$, Since the same goes for the odd-indexed and pattern-sifted elements, we can use the union bound to obtain $\Pr(\Omega^{\mathrm{even,ps}} \notin \Gamma \vee \Omega^{\mathrm{odd,ps}} \notin \Gamma) < 2\epsilon_1$. This means that the failure probability of predicting the photon number distributions in the elements surviving the pattern sifting can be bounded.

From $\mathbf{a}^{\mathrm{even}}$ and $\mathbf{a}^{\mathrm{odd}}$, we know which elements survive the pattern sifting. For the even-indexed and pattern-sifted elements, we perform a standard decoy-state BB84 protocol. The part (b) guarantees that this protocol is ϵ_2-secure with a failure probability $\Pr(\Omega^{\mathrm{even,ps}} \notin \Gamma)$. The same holds for the protocol using the odd-indexed and pattern-sifted elements. From a similar argument of the universal composability, we find that a protocol that combines two keys of these two protocols is $2\epsilon_2$-secure with a failure probability $\Pr(\Omega^{\mathrm{even,ps}} \notin \Gamma \vee \Omega^{\mathrm{odd,ps}} \notin \Gamma)$. As a consequence, it means that our protocol is $2(\epsilon_1 + \epsilon_2)$-secure.

The remaining problem is that there exist independent fluctuations in the mean photon number of the coherent state after AKD and PS in our experiment. We need generalize a security proof for a standard decoy-state BB84 protocol to accommodate it. It can be done by extending a function $f(a, n)$ to a set of functions satisfying a condition about intensity fluctuations. Since our argument in this section depends only on the dependence of $\Pr(\mathbf{a}, \mathbf{n})$ on $\mathbf{a}$ and $\mathbf{n}$, this extension does not affect the argument in this section.

B Simulation

We will provide a finite-length analysis considering random distributions. After PS, the pulse intensity may fluctuate because of pulse jitter or electrical noise in electrical circuits. The residual fluctuation is random, so that we can safely treat it by extending conventional security analysis. The reason is following: PS and AKD can treat the effect of the correlated intensity deviations due to the pattern effect, and provide effectively IID bit string for key generation. The resultant IID bit string allows us to analyze its security with conventional method.

We measured pulse intensities for 100,000 samples of signal and decoy pulses. Average intensity of signal pulses was normalized to one, and we evaluate standard deviations of $S \rightarrow \mathbf{S}$ and $S \rightarrow \mathbf{D}$, where the second pulse was the measurement target. Then we calculated the ratios of standard deviations to average intensities, which referred as normalized standard deviation used as an index of the intensity fluctuation. We obtained the values $\sigma_S = 3.2$ % and $\sigma_D = 7.0$ % for signal and decoy, respectively.

We expanded the theory of Lim, *et al.*[1], to include the effects of the intensity distribution. We set the upper and lower limits of the intensity; the mean photon numbers of the states stay equiprobably within the range defined with relative fluctuation δ_i as $[\mu_i(1-\delta_i), \mu_i(1+\delta_i)]$, where $i = S, D,$ and V. We put the mean photon numbers to the equations of ref. to be the most advantageous to Eve, that is, to yield the smallest final key rate. Since a usual probability distribution takes the maximum value at the expectation value and decreases with the deviation, the equiprobable distribution will yield a pessimistic estimation. The range can be defined experimentally by monitoring pulse intensities with a high-speed photodetector and discarding out-of-range pulses after quantum communication completed. We call this procedure "intensity sifting (IS)."

We estimated the secure key rate under intensity fluctuations caused by pattern effects and random distribution. Probability that pulse intensity being out of the range was calculated assuming normal distribution. Note that other probability distribution will yield different key rate, but it never affect the security of the protocol. Results for several values of the intensity range from 0.2σ to 0.8σ are shown in Fig. B.1.

[1] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**(2), 022307 (2014).

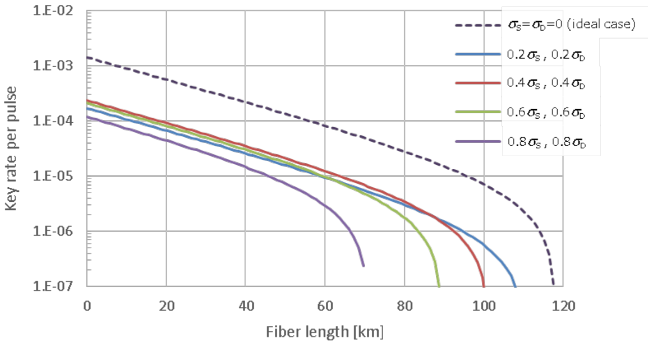


Figure B.1: Simulation of the final key rate considering intensity fluctuation caused by pattern effects and random noise. Intensity range δ_i was set between $0.2\sigma_i$ and $0.8\sigma_i$.