Secure quantum key distribution against pattern effects of optical pulse intensities

K. Yoshino,[1] M. Fujiwara,[2] K. Nakata,[3] A. Tomita,[3] and A. Tajima[1]
[1] NEC Corporation, Japan
[2] National Institute of Information and Communications Technology, Japan
[3] Hokkaido University, Japan

To realize highly secure communication, practical quantum key distribution (QKD) systems have been developed [1,2]. Although QKD theoretically guarantees ultimate security, device imperfections are inevitable. Therefore security analysis and implementation including the imperfections should be considered. In this paper, we focus on pattern effects of intensity modulation, which is one of the imperfections to consider. We analyze its impact on secure key rates and then propose a countermeasure, "decoy sifting" method.

For high-speed optics, modulation signals sometimes depend on previous electrical modulation patterns. This is called pattern effects. Figure 1 (a) shows an ideal electrical modulation signal to an optical intensity modulator. The electrical signal is rectangular, and voltages of hi-levels are always same. However, an actual signal is distorted due to the inhomogeneous frequency response of the electronics (Fig.1 (b)). Intensity of modulated optical signals are slightly changed depending on previous modulation. This is the pattern effects, which cause deviations of pulse intensities.

Intensity deviations influence the security of decoy state QKD. Commonly used three-state decoy QKD employs signal (S), decoy (D), and vacuum (V). Typical average photon number per pulse is 0.5, 0.2, 0, respectively. Intensity deviations of S and V are relatively small (around 1%) because the optical modulator is driven at the gradual slope near the top or bottom of the modulation curve. On the other hand, deviations of D is sometimes over 10% because of the steep slope at the middle of the curve.

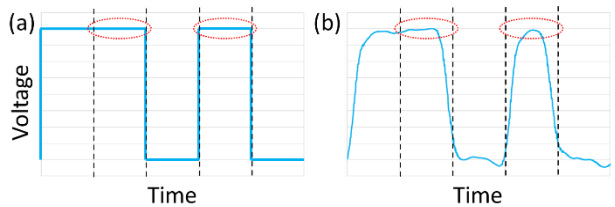

Fig.1: Modulation electric signals to an optical modulator. (a) Ideal case, (b) actual case.

To evaluate the impact of pattern effects, we estimated secret key rates considering intensity deviations of D. Results of deviations of 0~8% are shown in Fig.2 (a)~(e). We used finite-key security analysis in Ref. [3]. Intensity deviations are carefully introduced to minimize secret key rates. As a result, the key rates are significantly reduced.

To counter the pattern effects, we propose "decoy sifting" method; decoy pulses following D or V are discarded, and only ones following S are adopted. By discarding D with large deviations, pattern effects can be virtually eliminated. Using decoy sifting, secret key rates can recover to more than 90% of ones without pattern effects at 100km (Fig.2 (f)).

We focused on intensity deviations caused by pattern effects, which is one of considerable device imperfections. We analyze its impact on secure key rates, and propose a countermeasure "decoy sifting", which can almost completely cancel the key rate reduction due to the pattern effects.

This work was supported by ImPACT program.

----- References -----

[1] J. F. Dynes et al., Opt. Express 20, 16339 (2012).
[2] K. Yoshino et al., Opt. Express 21, 31395 (2013).
[3] C. C. W. Lim et al., Phys. Rev. A 89, 022307 (2014).

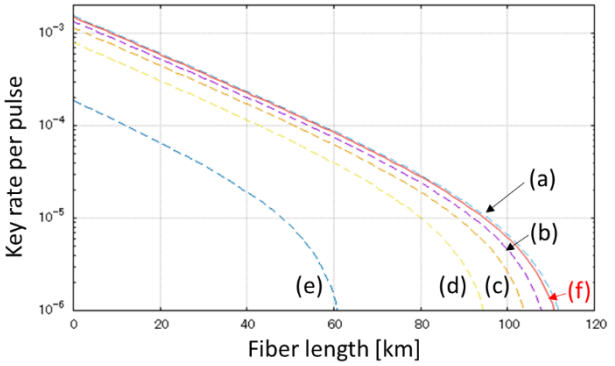

Fig.2: Key rates with decoy intensity deviations of 0% (a), 1% (b), 2% (c), 4% (d), 8% (e) (dashed lines), and with "decoy sifting" (f) (solid line).