Quantum key distribution with an efficient countermeasure against intensity fluctuations in optical pulses

K. Yoshino[1], M. Fujiwara[2], K. Nakata[3], T. Sumiya[4], T. Sasaki[4], M. Takeoka[2], M. Sasaki[2],
A. Tajima[1], M. Koashi[4] and A. Tomita[3]
[1] NEC Corporation, [2] National Institute of Information and Communications Technology,
[3] Hokkaido University, [4] The University of Tokyo, Japan

Quantum key distribution (QKD) allows two distant parties to share information-theoretically secure keys, and GHz-clocked QKD systems have already been realized [1,2]. However, it has been pointed out that high-speed systems might have intensity correlation between optical pulses due to the limited bandwidth of driving devices [3]. Depending on preceding modulation pattern, slightly different "High" (or "Low") electric signals are applied to the modulator (so-called "pattern effect", Fig.1), and correlated deviation of optical intensity arises. Such an inter-pulse correlation violates the assumption of most security proofs. As a countermeasure, we propose a simple and effective method [4]. In practice, however, there remain uncorrelated fluctuations due to thermal noise or timing jitter. Here, using additional method considering such random fluctuations, we estimate secure key rate.

Our method consists of three parts, "pattern sifting (PS)", "alternate key distillation (AKD)" and "intensity sifting (IS)". In the case of 3-state decoy QKD (using signal "S", decoy "D" and vacuum "V"), there are 9 patterns corresponding to adjacent intensity selection. PS discards the patterns with large intensity deviation in the post-processing, and AKD treats odd/even number pulses independently to remove correlations between neighboring pulses (Fig.2). IS discards the pulses with out-of-range intensity due to uncorrelated fluctuations according to intensity monitoring in the transmitter (Fig.3). By using IS, maximum and minimum intensity can be determined. Therefore we can estimate lower bound of secure key rate despite the fluctuation.

We calculated secure key rate by applying these methods to a finite-key security analysis [5]. As a result, we confirmed key generation over 100 km fiber transmission can be achieved, even if the optical pulses have correlations and fluctuations.

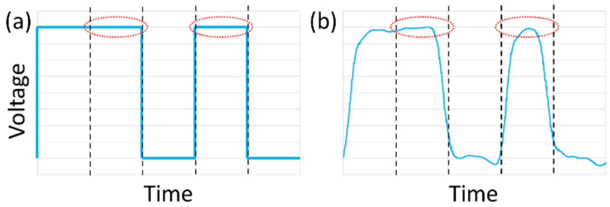
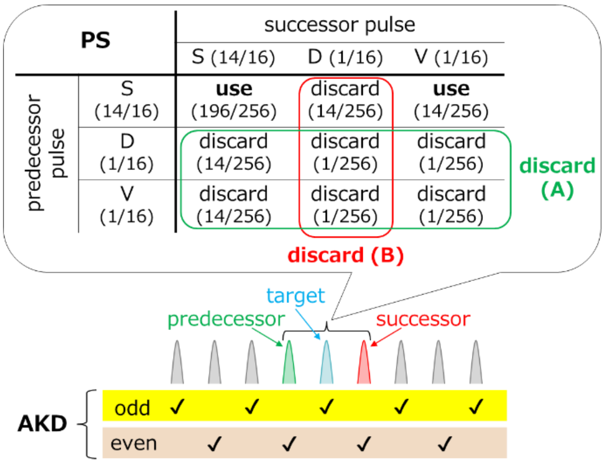


Fig.1: Electric signals to an optical modulator. Two "High" levels are equal in ideal case (a), but different in practical case (b).



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: Pattern sifting (PS) and alternate key distillation (AKD). The numbers in parentheses show typical values of the selection probability.

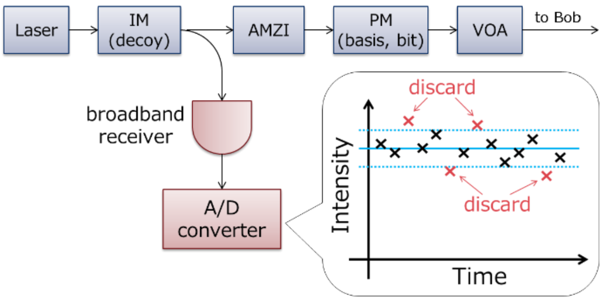


Fig.3: Intensity sifting (IS). IM: intensity modulator, AMZI: asymmetric Mach-Zehnder interferometer, VOA: variable optical attenuator.

This work was funded by ImPACT Program (Cabinet Office, Japan).

----- References -----

[1] J. F. Dynes et al., Opt. Express 20, 16339 (2012)
[2] K. Yoshino et al., Opt. Express 21, 31395 (2013)
[3] K. Yoshino et al., QCrypt 2016, poster session
[4] A. Tomita et al., QCrypt 2017 (to be presented)
[5] C.C.W. Lim et al., Phys. Rev. A 89, 022307 (2014)