Robustness of round-robin differential-phase-shift quantum-key-distribution protocol against source flaws

Akihiro Mizutani,[1] Nobuyuki Imoto,[1] and Kiyoshi Tamaki[2]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*

Abstract—Recently, a new type of quantum key distribution (QKD), called the round-robin differential-phase-shift (RRDPS) protocol [1], was proposed, where the security can be guaranteed without monitoring any statistics. In this paper [2], we investigate source imperfections and side-channel attacks on the source of this protocol. We show that only *three assumptions* are needed to prove the security, and no detailed characterizations of the source or the side-channel attacks are needed. This high robustness is another striking advantage of the RRDPS protocol over other protocols.

Introduction— For guaranteeing the security of the RRDPS protocol, there are some issues to be addressed from a practical point of view. These issues arise because there is a gap between the properties of the actual devices used in QKD systems and the mathematical model that the security proofs assume, which is also the case for all QKD protocols. In the case of the RRDPS protocol, all the security analyses including the original proof [1] and the recent work [3] have made ideal assumptions on Alice's light source, which are hard to realize in practice. Therefore, to consider the security proof accommodating source flaws is indispensable toward a practical and secure implementation of this protocol.

Main results— In this paper, we extend the security proof of [1] to accommodate the source flaws. Surprisingly, we found that the security can be guaranteed based only on the three assumptions on Alice's source. These assumptions are described as follows. As for Alice's side, she employs blocks of L light pulses, and applies phase modulation $\theta_{a_k}^{(k)}$ $(1 \leq k \leq L)$ to each of the pulses depending on a randomly chosen bit $a_k \in \{0,1\}$.

A1. For every light pulse, the probability of the vacuum emission for the bit value 0(1), namely, $p_0^{(k)}(0)(p_1^{(k)}(0))$ is upper and lower bounded by $p_{\mathrm{U},0(1)}(0)$ and $p_{\mathrm{L},0(1)}(0)$, respectively.

A2. The L pulses contain in total at most ν_{th} photons except for the probability e_{src}.

A3. There is no quantum and classical correlation among the sending states, and the system that purifies each of the sending states is possessed by Alice.

We note that when more detailed characteristics of the source is available, we can relax the assumption **A3** to accommodate any classical correlations among the sending pulses (see Ref. [2] for details). Importantly, no assumptions on the phase modulation $\theta_{a_k}^{(k)}$ or detailed specifications of imperfections and side-channel attacks on the source are needed. Even with these imperfections and side-channels, we show that the RRDPS protocol can distribute the key over longer distances (see Fig. 1). These results show that the RRDPS protocol is highly robust against the source flaws, which is another striking advantage of this protocol over other protocols. Moreover, we found that if the probabilities of emitting the vacuum state are the same for both bits, the information leakage to Eve is exactly the same as the one in the original paper [1] (see Ref. [2] for details). Even if these probabilities differ, the performance of the key generation rate is not significantly compromised as shown in Fig. 1.

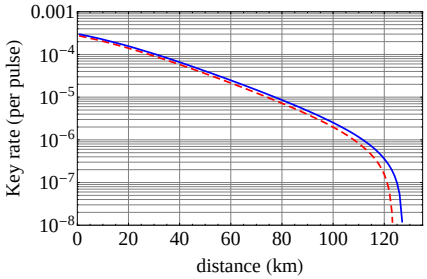

FIG. 1: Secret key rate per pulse versus distances. The solid line is for the case of $p_0^{(k)}(0) = p_1^{(k)}(0)$ for all k $(1 \leq k \leq L)$, and the dashed line is for the case of $p_0^{(k)}(0) \neq p_1^{(k)}(0)$ occurs for some or every k.

Conclusions— We have shown the security of the RRDPS protocol with imperfect light sources and side-channel attacks on Alice's source. In our security analysis, the characterization of Alice's source is simple in the sense that if Alice monitors only ν_{th}, the vacuum emission probability and the independence among the sending states, the amount of privacy amplification needed can be obtained. This means that the security of the RRDPS protocol can be guaranteed without detailed specifications of the source imperfections and side-channel attacks on the source.

Acknowledgments— We thank H.-K. Lo, M. Koashi, H. Takesue, T. Sasaki, T. Yamamoto, K. Azuma, L. Qian, R. Ikuta, S. Kawakami and G. Kato for helpful discussions. NI acknowledge support from the JSPS Grant-in-Aid for Scientific Research(A) 25247068. This work was in part funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Gov-

ernment of Japan).

[1] T. Sasaki *et al*, Nature **509**, 475 (2014).

[2] A. Mizutani *et al*, Phys. Rev. A **92**, 060303(R) (2015).

[3] H. Takesue *et al*, Nature Photon. **9**, 827-831 (2015).