Security of decoy-state QKD with alternate key distillation

T. Sumiya[1], T. Sasaki[1], M. Koashi[1], K. Yoshino[2], M. Fujiwara[3], K. Nakata[4], M. Takeoka[3], M. Sasaki[3], A. Tajima[2] and A. Tomita[4]

[1]The University of Tokyo, [2]NEC Corporation, [3]National Institute of Information and Communication Technology, [4]Hokkaido University

Most security proofs of QKD are based on the premise that signals from the sender are independent and identically distributed (IID). In one of the recent demonstrations of the decoy-state BB84 protocol, though, it was revealed that it is difficult in principle to modulate each pulse independently, and correlations between intensities of adjacent two pulses exist [1]. This effect violates the premise of the security proofs. A possible countermeasure is to combine two post-processing methods which we call "alternate key distillation (AKD)" and "pattern sifting (PS)" [2]. The AKD picks up only odd-indexed signals and considers generating a secret key from these. The PS discards some of odd-indexed signals according to a rule defined by information of even-indexed signals. These two procedures recover the IID property of odd-indexed signals and security proofs of the standard decoy-state BB84 protocol with no correlation of pulse intensities can be applied.

Similarly, it is expected that we can use even-indexed signals to generate a secret key by the same methods. However, security of the concatenation of two keys generated from odd- and even-indexed signals is not clear. The reason is that since PS for odd-indexed signals depends on even-indexed signals and the inverse is also true, two protocols to generate each key are not independent, and therefore discussion of composable security cannot be applied directly. To address this problem, we divide the standard decoy-state BB84 protocol into a sub-protocol (the shaded area) and a wrapper (the rest), as in Fig.1. The protocol with AKD and PS is then similarly decomposed as in Fig.2. We find that exactly the same sub-protocol appears for each of the odd- and the even-indexed part, and they are independent of each other. Then we can prove the security of the concatenated key from the composability of the sub-protocols.

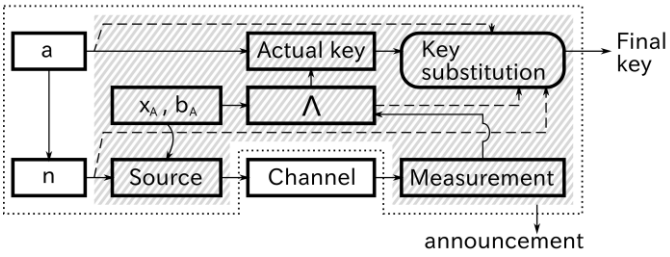

Fig.1: Structure of the standard decoy-state BB84 protocol. The shaded area represents a sub-protocol, which takes the intensity and the number of photons of each pulse as an input.

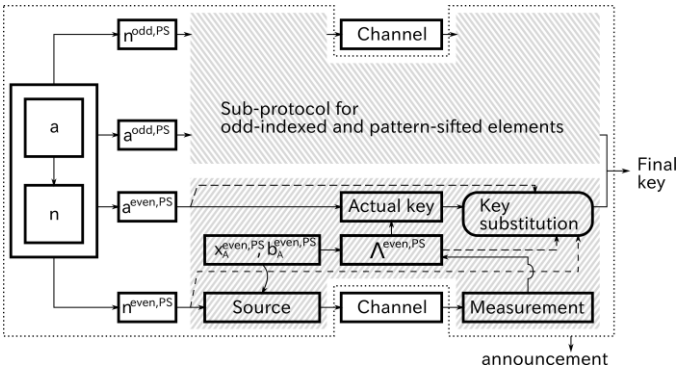

Fig.2: The concatenated protocol with AKD and PS. Only the wrapper (the non-shaded area) is dependent, while the two sub-protocols are independent.

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

-----References-----

[1] K. Yoshino et al., QCrypt 2016, poster session

[2] A. Tomita et al., QCrypt 2017 (to be presented)