Encrypting-device QKD working as a measurement device independent system

Muataz Alhussein[1] and Kyo Inoue[1]
Graduate School of Engineering, Osaka University
Email: muataz@opt.comm.eng.osaka-u.ac.jp

Introduction: Measurement device independent quantum key distribution (MDI-QKD) was proposed to be free from side-channel attacks utilizing imperfections in measurement devices [1]. In conventional MDI-QKD, Charlie, who is assumed to be an untrusted party, performs Bell state measurement (BSM) on Alice's and Bob's signals. The main challenge in practical implementation of such MDI-QKD schemes is to establish synchronization between the received signals in term of the timing, the polarization state, the temporal and spectrum shapes for the BSM. In order to avoid such practical difficulties, this work introduce a modified BB84 protocol named encrypting-device quantum key distribution (ED-QKD). It employs an additional operation at Bob, by which Bob`s detection event does not contain key information itself, making detector`s behavior independent of the security of a created key. Our setup is simpler than conventional MDI-QKD schemes, yet it can overcome side-channel attacks utilizing detectors imperfections.

Protocol and operation: The setup of the proposed scheme is shown in Fig.1. Alice prepares a qubit as:

$$|S\rangle = (|0\rangle + e^{i\varphi_a}|1\rangle)/\sqrt{2},$$

where |0> and |1> represent the bases of a two-dimensional Hilbert space, e.g., one-photon states at two time-bins, and φ_a is randomly chosen from one of four values {0, π, π/2, 3π/2}. The above qubit is sent to Bob, where he performs two processes. First, Bob acts on the received signal with a unitary phase operator as:

$$\sigma(\varphi_b) = \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\varphi_b}|1\rangle \end{cases},$$

where φ_b is chosen randomly from one of four phases{0, π, π/2, 3π/2}. This operation contrasts to the conventional BB84 where one of two phases {0, π/2} is chosen. As a result of this Bob`s operation, the relative phase in the qubit becomes the sum of Alice`s and Bob`s phases, which means Alice`s phase is encrypted with Bob`s operation. Next, Bob measures (φ_a + φ_b) using a delay Mach–Zehnder interferometer (MZI) (in case of a time-bin qubit), which is constructed so that detectors D1 and D2 conclusively click for phase differences of 0 and π, respectively, and announces the measurements results (detectors and detection time) to Alice.

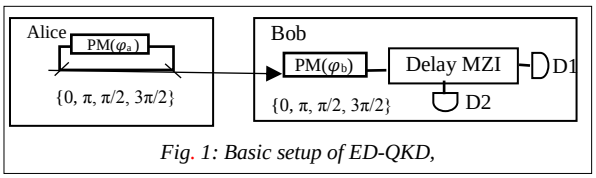

Fig. 1: Basic setup of ED-QKD,

In the above setup and operation, the detection event is determined by Alice's and Bob's phases as shown in Table 1, where conclusive detections are listed. Utilizing this relationship, Alice and Bob create key bits as follows. Frist, they categorize their phase data to two basis X= {0, π} and Y= {π/2, 3π/2}. After the quantum transmission is completed, they exchange their basis through a classical channel. Next, they discard the events where their bases are mismatched. Then, they assign {0, π/2} to bit "1" and {π, 3π/2} to bit "0" for the left events. Finally, in case where Alice and Bob used basis X and detector D2 clicked, Bob flips his bit. In case where they used basis Y and detector D1 clicked, Bob flips his bit. With the above protocol, Alice and Bob share identical bits, which can be a secret key. For the current scheme, even if an eavesdropper manipulates the detectors and controls measurement results, she cannot obtain information about the key. Thus, the current scheme works as a MDI system.

Table 1: phase modulation and detection event

Alice φ_a	0	π	0	π	π/2	3π/2	π/2	3π/2
Bob φ_b	π	0	0	π	3π/2	π/2	π/2	3π/2
Detector	D2	D2	D1	D1	D1	D1	D2	D2
Bits	flip	flip			flip	flip		

System performance: The above mentioned protocol assumes a single-photon qubit. In practical systems, however, an attenuated coherent light is used as a quasi single-photon, for which a photon-number splitting attack is threatening. Fortunately, a decay method can be implemented in our ED-QKD because Bob has data of the photon counting rate, and the security of the present scheme can be equivalent to that of decoy state QKD [2]. Therefore, the system performance is similar to that of decay BB84-QKD.

Summary: We proposed a novel QKD scheme called ED-QKD that prevents side-channel attacks utilizing detectors imperfection, which requires no BSM as in conventional MDI systems, and thus offers a higher practicality.

[1]H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, p. 130503, 2012.
[2] Ma, X., Qi, B., Zhao, Y. & Lo, H. K, "Practical decoy state for quantum key distribution, " Phys. Rev. A, vol. 72, p. 012326 (2005).