MDI-DPS-QKD with no joint measurement

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. In conventional MDI-QKD, Alice and Bob respectively prepare one of four BB84 states and send it to Charlie who performs Bell state measurement (BSM) on Alice's and Bob's signals. Afterwards, Charlie announces the measurement result through a public channel. Alice and Bob then create a key bit according to Charlie's information and their own data. The main experimental challenge of MDI-QKD is to establish synchronization in term of the timing, the polarization state, the temporal and spectrum shapes for the BSM. In order to avoid such experimental difficulties, this paper proposes a new scheme of MDI-QKD based on differential phase shift (DPS) quantum secret sharing (QSS)[1], which features no use of BSM. Compared to conventional MDI-QKD scheme, the proposed scheme presents a simple setup, suitable for practical implementation.

Setup and operation principle: The setup of the proposed scheme is shown in Fig.1, where a weak coherent pulse train phase-modulated for each pulse by (0, π) is sent from Alice to Bob with a power level of less than 1 photon per pulse on average (0.1-0.2). Bob further modulates the transmitted signal by (0, π) for each pulse without measuring it, and sends it to Charlie (untrusted party), while monitoring the incoming signal power by splitting and detecting its fraction. Charlie, positioning just after Bob, measures the phase difference of adjacent pulses with a one-pulse delayed Mach-Zehnder interferometer, through which detectors 0 and 1 count a photon for a phase difference of 0 and π, respectively. When the differential phases imposed by Alice and Bob are {Alice=0, Bob= 0} or {Alice=π, Bob= π}, the total differential phase is 0 and detector 0 counts a photon. On the other hand, when Alice's and Bob's differential phases are {Alice=0, Bob= π} and {Alice=π, Bob=0}, the total differential phase is π and detector 1 counts a photon. Because the photon average number is less than 1 per pulse, the detection event is occasional and random. After the measurement, Charlie exposes the time and detector information through a classical channel to Alice and Bob, who can create an identical key bit based on Charlie's information and their own modulation data as follows. First, Alice/Bob creates bits 0 and 1 from her/his differential phases of 0 and π, respectively. In case that detector 0 clicked at Charlie, Bob holds the bit. In case that detector 1 clicked at Charlie, Bob flips his bit. In this way, Alice and Bob have an identical bit. This scheme prevents malicious Charlie from identifying the created bit, because he only knows the result of XOR, which does not provide the key bit information.

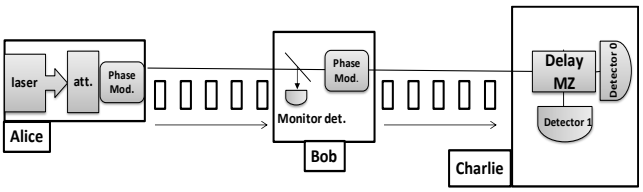

Figure 1: Setup of MDI-DPS-QKD with no joint mesuremnt.

Simulation: The transmitted signals in this scheme are basically the same as those in DPS-QKD. Thus, its security can be equivalent to that in DPS-QKD. Based on this analogy, we evaluated the system performance considering the general individual attack, which has been analyzed against DPS-QKD [2]. The main difference in system evaluation is that detection errors, which determines the system performance, occur in untrusted Charlie in the present scheme instead of Bob in DPS-QKD. In the present simulation, we assume, as an example, that Charlie uses a receiver typically employed in DPS-QKD. Under this assumption, the key creation rate as a function of the key distribution distance is similar to that in DPS-QKD, as shown in Fig. 2.

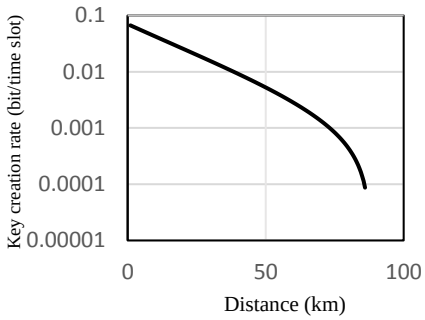

Figure 2: System performance against general individual attack.

Summary: We proposed a novel scheme of MDI-QKD, which uses no BSM for key bit creation and thus offers a simple setup.

[1] K. Inoue *et al.*, "Differential-phase-shift quantum secret sharing," *Opt. Express*, vol. 16, no. 20, pp. 15469–15475, 2008.
[2] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," *Phys. Rev. A*, vol. 73, no. 1, 012344, 2006.