Practical Implementation of MDI-QKD with Plug-and-play Architecture

Yujun Choi,[1,2,*] Minki Woo,[1,3] Young-Wook Cho,[1] Sang-Wook Han, [1] Yong-Su Kim, [1,4] and Sung Moon[1]
[1]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea
[2]Department of Physics, Yonsei University, Seoul, 03722, Republic of Korea
[3]Graduate School of IT Convergence, Ajou University, Suwon, 16499, Republic of Korea
[4]Department of Nano-Materials Science and Engineering, Korea University of Science and Technology, Daejeon 34113, Republic of Korea
E-mail address: s.moon@kist.re.kr

We have proposed a practical implementation of measurement device independent quantum key distribution (MDI-QKD) with plug-and-play (P&P) architecture. Because the concept of P&P naturally guarantees the indistinguishability in spectral and polarization modes between two optical pulses, the proposed scheme resolves the mode matching problem while minimizing the use of active control units. The proof of principle experiment has been conducted with free space bulk optics. Also, the fiber based design of the P&P MDI-QKD is suggested.

Quantum key distribution (QKD) usually considered as the most feasible technology among various quantum information communication technologies. Although the security of QKD is guaranteed by the law of quantum physics, some loopholes can appear because of devices' imperfection. The loopholes can be exploited by an eavesdropper (Eve), thereby weaken the security of QKD system[1]. The security problem of QKD can be overcome with Device-Independent QKD (DI-QKD) which always guarantees unconditional security despite the device imperfections[2]. However, DI-QKD is highly impractical to implement since it is equivalent to the loophole-free Bell test which requires very high efficiency single-photon detection technology.

The recently proposed measurement-device-independent quantum key distribution (MDI-QKD) closes the practicality gap of DI-QKD while compromising some aspects of security[3,4]. While MDI-QKD can be vulnerable to the quantum hacking at the light sources, it closes all the possible loopholes in detection. Because measurement devices including single-photon detectors have been primary targets of the quantum hacking attempts, MDI-QKD significantly improves the security of the practical QKD system.

MDI-QKD has two remote users (Alice and Bob) that wish to exchange secure key, and one intermediary (Charlie) that assists the secure key exchange process. When Alice and Bob send weak coherent pulses encoded with their key bits, Charlie conduct Bell state measurement on them. After

Charlie's announcement of the measurement results, Alice and Bob can share secret keys with some post-processing.

Although MDI-QKD significantly improves the practicality of DI-QKD, there are still some difficulties for implementing it. The most difficult part in implementing MDI-QKD is to conduct Bell state measurement between two photons that are sent from Alice and Bob. In order to implement Bell state measurement with linear optics, two-photon interference which requires mode matching is essential. Mode matching between the pulses sent by Alice and Bob consists of three parts: spectrum, polarization, and timing. Since Alice and Bob employ independent laser sources, they need active control units to match all of them. These active control units are cumbersome and expensive when implementing the MDI-QKD system on deployed fiber. Consequently, the mode matching issue is a key element in practical use of MDI-QKD.

In order to improve the practicality of MDI-QKD, we propose a scheme which adopts plug-and-play architecture[5]. While the two independent laser sources of Alice and Bob are used in the original MDI-QKD, the proposed scheme employs a common laser source located at Charlie. Also, the plug-and-play architecture naturally compensates the polarization drift that occurs during optical fiber transmission. The only thing we have to concern is timing mode matching. Therefore, this scheme reduces the necessity of active control units and contributes to practical and secure quantum communication. In the presentation, we propose the scheme with fiber optical setup. The feasibility of the scheme is verified with a proof-of-principle experiment.

References

1. See for example, L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photon. **4**, 686 (2010).
2. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).
3. S. L. Braunstein, and S. Pirandola "Side-Channel-Free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
4. H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
5. Y. Choi *et al*., "Plug-and-Play measurement-device-independent quantum key distribution," Phys. Rev. A **93**, 032319 (2016).