Field Test of Measurement-Device-Independent Quantum Key Distribution

The main type of obstacles of practical applications of quantum key distribution (QKD) network are various attacks on detection-side. Measurement-device-independent QKD (MDIQKD) protocol is immune to all these attacks, and thus, a strong candidate for network security. Recently, several proof-of-principle demonstrations of MDIQKD have been performed. Although novel, those experiments are implemented in the laboratory with secure key rates less than 0.1 b/s. Besides, they need manual calibration frequently to maintain the system performance. These aspects render these demonstrations far from practicability. Thus, justification is extremely crucial for practical deployment into the field environment.

Generally, there are three basic criteria for a practical QKD system: Stabilization under real-world environment, a moderate secure key rate, and an automatic operation. First, all previous demonstrations are taken in the laboratory without perturbation of the field environment. A field test of the MDIQKD scheme has been attempted over an 18.6 km deployed fiber (9 dB transmission loss), but random modulated decoy state is not added in that experiment and thus secure key could not be generated. Second, the secure key rates in all previous experiments are limited, of which the highest is 0.12 b/s at 50 km transmission distance (10 dB transmission loss). Last but not least, all previous experiments need manual calibration frequently to maintain the system performance per 10 min. This is fatal for a practical application. A sufficiently good performance will involve many aspects, such as time, spectrum and polarization modes. This poses another challenge on implementing an automatic calibration system. It is wondered whether the MDIQKD system is suitable for a practical deployment or not.

In this field-environment test, we take the field test in three adjacent sites located in Hefei City, China. We develop a decoy-state MDIQKD system, operated at a clock rate of 75 MHz and with a superconducting nanowire single photon detector system of more than 40% detection efficiency. To rule out the unambiguous state-discrimination attack, we have utilized the internally modulated signal laser source which is intrinsically phase randomized. Besides, we employ the vacuum+weak decoy state scheme to defeat the PNS attack. In order to achieve both a highly efficient coincidence count rate and a desirable error rate, we require a perfect and stable bell state measurement, namely, the two independent laser pulses should keep indistinguishable after traveling through two separated fiber links, especially in the scenario of an unstable field environment. Thus, three aspects, time, spectrum and polarization, should be taken into account. To maintain the system performance and continuous operation, we develop several automatic feedback systems, serving for calibrating the time, spectrum and polarization modes of two independent laser

pulses.

The field test demonstrates the feasibility and robustness of the MDIQKD protocol in an unstable environment. In this test, by developing an automatic feedback MDIQKD system operated at a high clock rate, we perform a field test via deployed fiber network of 30 km total length achieving a 16.9 b/s secure key rate, which is at least two orders of magnitude higher than the previous results of MDIQKD demonstrations. The result lays the foundation for a global quantum network, which can shield from all the detection-side attacks.

Besides, the goal of regular QKD protocols and the MDIQKD protocol is not restricted to point-to-point communication, but is to realize a global quantum network. The MDIQKD protocol has an intrinsic property which is desirable for constructing quantum network with the star-type structure, since the detection system placed in Charlie's site in the middle node can be shared by all the transmitters. Furthermore, when more transmitters are added in the network, only laser sources and modulators are needed which are much cheaper and smaller than the detection system. While the existing quantum networks are suffering from various attacks, especially the detection-side ones, the MDIQKD protocol will perfectly shield the QKD network from these existing and potential detection-side attacks. We can expect that the MDIQKD network may be built within reach of current technology in the near future.

We remark that there is still much room for us to make MDIQKD system more practicable. First, we can increase the system clock rate by further minimizing the overall timing jitter. Second, with the development of the SNSPD technology, the detection efficiency can be further improved. Besides, the dark count rate may be effectively reduced to sub-Hertz. Last but not least, with the decoy-state parameters and the basis choice optimized, we can expect a faster key rate generation to enable some practical applications. We note that this field test utilizes the system based on which we have implemented a long-distance MDIQKD over 200 km [2].

This work appears as an invited paper on IEEE journal of selected topics in quantum electronics [1].

[1] Yan-Lin Tang, **Hua-Lei Yin**, *et. al.*, IEEE Journal of Selected Topics in Quantum Electronics, **21**, 6600407, (2015).
[2] Yan-Lin Tang, **Hua-Lei Yin**, *et. al.*, Physical Review Letters, **113**, 190501 (2014).