Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution

Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo

Centre for Quantum Information and Quantum Control
Department of Electrical and Computer Engineering & Department of Physics
University of Toronto, Toronto, Ontario, Canada M5S 3G4
ztang@physics.utoronto.ca

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) closes all potential security loopholes due to detector imperfections without compromising the performance of a standard QKD system. Here we report the first demonstration of *polarization* encoding MDI-QKD over 10 km optical fibers. Decoy state techniques are employed to estimate gain and error rate of single photon signals. Intensities and probability distribution of signal and decoy states are optimized. Active phase randomization is implemented to protect against attacks on the imperfect sources. A 1600-bit secure key is generated in the experiment. Our work shows that polarization encoding MDI-QKD is a practical solution to confidential communication.

Quantum key distribution (QKD) allows two parties, Alice and Bob, to share a secret key even with the presence of an eavesdropper, Eve [1, 2]. The security of QKD is guaranteed by quantum physics with the assumption that perfect single photon sources and detection devices are used [3–5]. However, this assumption cannot always be satisfied by current technology, and the gap between theory and practice compromises the security of QKD. Fortunately, it has been shown that phase randomized weak coherent sources can be used to replace single photon sources in QKD [6]. Furthermore, as shown in [7–9], decoy state techniques can dramatically increase the key rate in practical applications [10]. Nonetheless, imperfections in the detection devices still present security loopholes that can be exploited by Eve to steal the secret key. Several detector side channel attacks have been successfully launched on sophisticated commercial QKD systems [11–15].

Recently, measurement-device-independent quantum key distribution (MDI-QKD) has been proposed to close all the security loopholes at the detection devices [16]. In the MDI-QKD protocol, Alice and Bob independently prepare phase randomized weak coherent pulses in one of the four BB84 states (with decoy states) and send them to an untrusted third party, Charlie, who can be an eavesdropper, Eve. Charlie/Eve then performs Bell state measurements (BSM), and announces to Alice and Bob over a public channel the successful BSM events. Alice and Bob can get a sifted key by dropping events where they send pulses in different bases. Finally, a secure key can be generated after error correction and privacy amplification.

Various experimental attempts on MDI-QKD have been reported in both time-bin [17,18] and polarization encoding [19]. We remark that in [17,19], only Bell state measurements with different combinations of BB84 states and intensity levels are conducted, and in fact no real QKD (which requires Alice and Bob randomly switch their qubits' states and intensity levels) is performed. A time-bin encoding MDI-QKD experiment is reported in [18]. However, intensities of signal and decoy states are not optimized in their experiment. In addition, phase randomization of weak coherent pulses, a crucial assumption [20] in the security proof of standard decoy state QKD [8, 9], is neglected. In fact, a successful attack on a QKD system without phase randomization has been demonstrated recently [21].

Here we report the first experimental demonstration of *polarization* encoding MDI-QKD over 10 km optical fibers. Active phase randomization of weak coherent pulses is implemented to close security loopholes in the sources. Intensities and probability distribution of signal and decoy states are optimized [22]. Our work verifies for the first time the feasibility of polarization encoding MDI-QKD, where there exists no direct optical link between Alice and Bob. Our experiment also paves the way for future implementations of polarization coding MDI-QKD in optical fiber network as well as in free space, where Alice and Bob send photons from the ground to an untrusted third party Charlie on a satellite.

Figure 1 shows the schematic of the experiment. Each of Alice and Bob possesses a CW laser whose wavelength

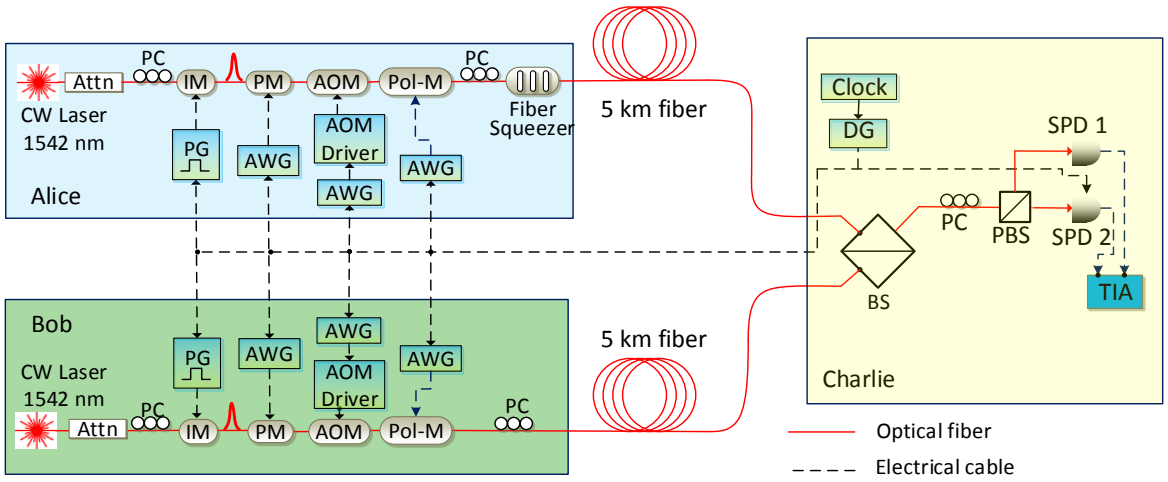

Fig. 1. (Color online) Experimental setup of polarization encoding MDI-QKD: Attn, optical attenuator; IM, intensity generator; PM, phase modulator; AOM, acousto- optic modulator; Pol-M, polarization modulator; PG, electrical pulse generator; AWG, arbitrary waveform generator; DG, electrical delay generator; BS, beam splitter; PBS, polarizing beam splitter; PC, polarization controller; SPD, single photon detector; TIA, time-interval analyser.

is locked to one molecular absorption line of a gas cell at around 1542.38 nm. The frequency mismatch between these two independent lasers is less than 10 MHz, which guarantees spectral indistinguishability between them. The laser light is attenuated and modulated by an intensity modulator (IM) to generate weak coherent pulses with width of around 1 ns (FWHM) at a repetition rate of $f = 500$ KHz. Phase of each individual pulse is actively randomized by a phase modulator (PM) in the range of $[0, 2\pi]$. To implement the decoy state method, intensities of pulses are randomly modulated using an acousto-optic modulator (AOM) between the signal state (with average photon number μ) and two decoy states (with average photon numbers ν and ω). We perform a numerical simulation to optimize the performance [22]: the intensities are optimally set to be $\mu = 0.3$, $\nu = 0.1$ and $\omega = 0.01$; the probabilities to send out pulses with intensities μ, ν, and ω are set to be 20%, 45%, and 35%, respectively . Polarization of each pulse is randomly switched by a polarization modulator (Pol-M) [23] to one of the four BB84 states. The PMs, AOMs, and Pol-Ms are driven by arbitrary waveform generators (AWGs) with pre-stored random patterns. Finally, Alice and Bob apply unitary transformations on their photons using a fiber squeezer (in Alice's setup) and polarization controllers (PCs) so that their polarizations are properly aligned in both the rectilinear and diagonal bases.

Alice and Bob send their pulses through a 5 km fiber spool to Charlie, who performs a partial Bell state measurement with a beam splitter (BS) and a polarizing beam splitter (PBS). A coincidence event (measured by the time interval analyser, TIA) between the two single photon detectors (SPDs) indicates a projection into the Bell state $|\psi^+>$.

The experiment is run for 94 hours, with a total of $N = 1.69 \times 10^{11}$ pulses sent out by Alice and Bob. The secure key generation rate R is estimated using the following key rate equation [16]

$$R \geq q\{Q_{11}^{rect}[1 - H_2(e_{11}^{diag})] - Q_{\mu\mu}^{rect} f(E_{\mu\mu}^{rect}) H_2(E_{\mu\mu}^{rect})\}, \tag{1}$$

where q is the proportion of events where both Alice and Bob send out signal states ($\mu = 0.3$) in the rectilinear basis, $H_2(e)$ is the binary Shannon entropy, $f(E_{\mu\mu}^{rect}) = 1.16$ is the efficiency of error correction, $Q_{\mu\mu}^{rect}$ and $E_{\mu\mu}^{rect}$ are the overall gain and bit error rate of signal states, and Q_{11}^{rect} and e_{11}^{diag} are gain and phase error rate when both Alice and Bob send out pulses of single photons. Here $Q_{\mu\mu}^{rect} = 4.66 \times 10^{-5}$ and $E_{\mu\mu}^{rect} = 1.8\%$ are measured directly from the experiment, and a lower bound of Q_{11}^{rect} (denoted as $Q_{11,L}^{rect}$) and an upper bound of e_{11}^{diag} (denoted as $e_{11,U}^{diag}$) can be estimated using the decoy state method. Using an analytical method proposed in [22] and assuming three standard deviations of statistical fluctuations [24], we find that $Q_{11,L}^{rect} = 2.0 \times 10^{-5}$ and $e_{11,U}^{diag} = 15.1\%$. We can then estimate a lower bound of the key generation rate $R_L = 9.8 \times 10^{-9}$ bit per pulse and generate 1600 secure key bits.

In summary, we have implemented for the first time a polarization encoding MDI-QKD experiment over 10 km optical fibers, with intensities and probability distribution of signal and decoy states chosen to optimize the key rate. Active phase randomization is implemented to close security loopholes in the coherent sources. Our experiment shows that MDI-QKD is a practical and promising technology for secure communication.

We thank W. Cui and M. Curty for enlightening discussions, and H. Xu for his assistance in the experiment. Financial supports from NSERC Discovery Grant, NSERC RTI Grant, and the Canada Research Chairs program are gratefully acknowledged.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661 (1991).
3. D. Mayers, "Unconditional security in quantum key distribution," J. ACM **48**, 351 (2001).
4. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050 (1999).
5. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441 (2000).
6. D. Gottesman, H. -K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum. Inf. Comput. **4**, 325 (2004).
7. W. -Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
8. H. -K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
9. X. -B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
10. Y. Zhao, et al., "Experimental quantum key distribution with decoy states," Phys. Rev. Lett. **96**, 070502 (2006).
11. Y. Zhao, C. -H. F. Fung, B. Qi, C. Chen and H. -K. Lo "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).
12. L. Lydersen, et al. "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics **4**, 686 (2010).
13. N. Jain, et al. "Device calibration impacts security of quantum key distribution," Phys. Rev. Lett. **107**, 110501 (2011).
14. I. Gerhardt, et al. "Full-field implementation of a perfect eavesdropper on a quantum cryptography system, "Nat. Commun. **2**, 349 (2011);
15. H. Weier, et al. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New J. Phys. **13**, 073024 (2011);
16. H. -K. Lo, M. Curty and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
17. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "A quantum key distribution system immune to detector attacks," arXiv:1204.0738.
18. Y. Liu, et al., "Experimental measurement-device-independent quantum key distribution," arXiv:1209.6178.
19. T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporo, and J. P. von der Weid, "Proof-of-principle demonstration of measurement device independent QKD using polarization qubits," arXiv:1207.6345.
20. Y. Zhao, B. Qi, and H. -K. Lo, "Experimental quantum key distribution with active phase randomization," Appl. Phys. Lett. **90**, 044106 (2007).
21. Y. Tang, et al., "Source attack of decoy-state quantum key distribution using phase information," arXiv:1304.2541.
22. F. Xu, et al., "Measurement-device-independent quantum key distribution in a practical setting," in preparation.
23. I Lucio-Martinez, et al., "Proof-of-concept of real-world quantum key distribution in a quantum frame," New J. Phys. **11**, 095001 (2009).
24. X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," Phys. Rev. A **86**, 052305 (2012).