A Quantum Key Distribution System Immune to Detector Attacks

Allison Rubenok[1], Joshua A. Slater[1], Philip Chan[2], Itzel Lucio-Martinez[1], and Wolfgang Tittel[1]

[1] Institute for Quantum Information Science and Department of Physics & Astronomy, University of Calgary, Canada.
[2] Institute for Quantum Information Science and Department of Electrical & Computer Engineering, University of Calgary, Canada.
jaslater@ucalgary.ca

Abstract. Quantum cryptography promises the distribution of cryptographic keys secured by fundamental laws of quantum physics. However, results in quantum hacking have demonstrated that the information theoretic security of quantum cryptography protocols does not guarantee security for actual implementations. Most notable are attacks against the vulnerabilities of single photon detectors [1–4]. In this talk we will report the first proof-of-principle demonstration of a new protocol that removes the threat of any such attack [5]. We demonstrated the protocol over 80 km of spooled fibre as well as across different locations within the city of Calgary [6], confirming this protocol as a realistic approach to secure communication and demonstrating the possibility for controlled two-photon interference in a real-world environment, which is a remaining obstacle to realizing quantum repeaters and quantum networks.

Information theoretic security for quantum key distribution (QKD) has been proven under various assumptions about the devices of the legitimate QKD users, Alice and Bob. However, it is now clear that some of the assumptions made in QKD proofs are difficult to meet in real implementations. Most recently, various possibilities for Eve to remote-control or monitor single photon detectors have been demonstrated [1–4]. Fortunately, this side-channel can be removed by two recently proposed QKD protocols [5, 7], each of which ensures that controlling or monitoring detectors, regardless by what means, does not help Eve to gain information about the distributed key.

We thus report the first experimental demonstration [6] of one of those protocols: Measurement-Device Independent Quantum Key Distribution (MDI-QKD) (a complete theoretical description is presented elsewhere [5]). The protocol involves Alice and Bob randomly, independently and secretly preparing photons in one of the four BB84 qubit states, where the qubit state encodes a key bit: "0" $\in [|0\rangle, |+\rangle]$ and "1" $\in [|1\rangle, |-\rangle]$. Alice and Bob send their photons to Charlie, who performs a Bell-state measurement (BSM). In the cases where his measurement results in a projection onto a maximally entangled $|\Psi^-\rangle$ Bell state, and where Alice's and Bob's preparation bases are the same, Alice's and Bob's key bits must be anti-correlated. As usual, the information Eve may have gained

during qubit transmission is bounded from error rates, and then error correction (EC) and privacy amplification can generate a final secret key. The remarkable feature of MDI-QKD is that it de-correlates detection events from key bits, thus preventing detector attacks from gaining information about the secret key.

To demonstrate the feasibility of MDI-QKD, we performed experiments in two different configurations. First, with Alice, Bob and Charlie located in the same lab, with Alice and Bob connected to Charlie via separate spooled fibres of various lengths and loss. Second, with Alice, Bob and Charlie located in different locations within the city of Calgary, and with Alice and Bob connected to Charlie by deployed fibres of 12.4 and 6.2 km length, respectively.

A previously undemonstrated feat, and a crucial element for MDI-QKD, is a BSM with photons generated by independent sources that travel through separate deployed fibres. To properly implement a BSM, these photons need to be indistinguishable (i.e. in polarization, frequency and arrival time). However, BSMs in real-world environments are impossible without active stabilization, due to time-varying properties of optical fibres that can cause significant changes to photon properties in less than a minute. We thus developed the ability to track and stabilize photon arrival times and polarization transformations, as well as the frequency difference between Alice's and Bob's lasers during all measurements. We emphasize that this achievement is not only key to implementing the MDI-QKD protocol, but also removes a remaining obstacle to realizing future applications of quantum communications such as quantum repeaters [8].

For our proof-of-principle demonstration of the MDI-QKD protocol, Alice and Bob generated time-bin qubits encoded into attenuated laser pulses and sent these photons to Charlie, who recorded the number of two-photon detections corresponding to a projection onto the $|\psi^-\rangle$ Bell state. This data yields the gains and error rates. The experiment was repeated for four different lengths of spooled fibre (and then the real-world links) and for three mean photon numbers, μ.

We then modeled the experiment taking into account all identified system imperfections [6]. The model results and experimental data, are plotted in Fig. 1a,b, and match within the experimental uncertainties, suggesting that we understand all imperfections of our implementation, and that the use of deployed fibres does not impact on the performance of the protocol, or the BSM.

Next, we evaluated how much secret key could be extracted from our measured error rates and gains using our model (in place of a decoy-state analysis, which is currently impractical for MDI-QKD [5], but is likely to improve) and assuming optimal conditions (i.e. no PNS attack, EC efficiency of 1 and long key strings). We find that key distribution is possible up to 27.1±3.6 dB, which corresponds to 135±18 kms of standard optical fibre (with an EC efficiency of 1.17 [9], these values change to 24.0±3.7 dB loss and 120±18 km distance).

Our steup contains only standard, off-the-shelf components. The extension to higher key rates using state-of-the-art detector [10] is straightforward, and the development into a complete QKD system follows standard procedures [9]. Furthermore, the technological advance that enabled BSMs in a real-world environment with truly independent photons also removes a remaining obstacle for

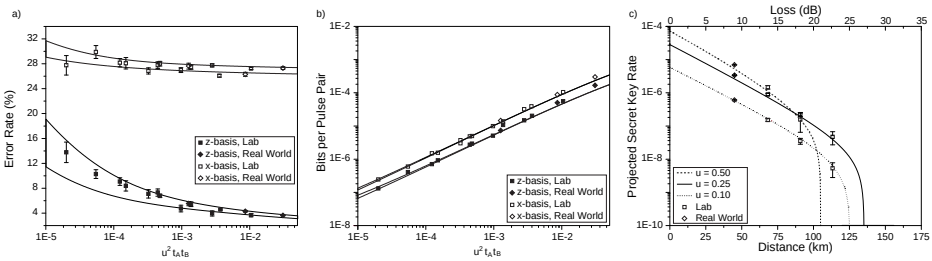

Fig. 1. a,b) Experimental results (points) and modeled values (regions between lines) for error rates and gains as a function of $\mu^2 t_A t_B$ ($t_{A(B)}$ is the transmission coefficient characterizing the links between Alice (Bob) and Charlie). One-standard deviation uncertainties were calculated assuming Poissonian detection statistics. The modeled regions are based on parameters that have been established through independent measurements. Monte-Carlo simulations using uncertainties in these measurements lead to predicted regions as opposed to lines [6]. **c)** Secret key rates as a function of loss and distance (assuming 0.2 dB/km) for different mean photon numbers.

building a quantum repeater, which promises quantum communication such as QKD over arbitrary distances.

References

1. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel, *Opt. Express*, **15** (15), 9388-9393 (2007).
2. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum Hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
3. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4,** 686689 (2010).
4. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V. Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **18** (26), 27938-27954 (2010).
5. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
6. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I., & Tittel, W. Proof-of-principle field test of quantum key distribution immune to detector attacks. arXiv:1204.0738v1 (2012).
7. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
8. Sangouard, N., Simon, C., De Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83,** 33-80 (2011).
9. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. Opt. Express **19** (11), 10387-10409 (2011).
10. Yuan, Z. L., Sharpe, A. W., Dynes, J. F., Dixon, A. R. & Shields, A. J. Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes. *Appl. Phys. Lett.* **96,** 071101 (2010).