Physics

Physics **6**, 104 (2013)

Viewpoint

Foiling Quantum Hackers

Hoi-Kwong Lo
Centre for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering, and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada

Published September 23, 2013

Researchers have implemented a new quantum encryption method that, in principle, may provide the ultimate security against hackers in real-world cryptography applications.

Subject Areas: **Quantum Information**

A Viewpoint on:
Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks
A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel
Phys. Rev. Lett. ***111****, 2013* – Published September 23, 2013

Experimental Measurement-Device-Independent Quantum Key Distribution
Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan
Phys. Rev. Lett. ***111****, 2013* – Published September 23, 2013

Quantum cryptography holds promise for communication schemes that are, in theory, perfectly secure. But in the last few years, hackers have exploited security loopholes to crack some of the most sophisticated quantum encryption systems. Fortunately, two new papers in *Physical Review Letters*, one by Allison Rubenok, at the Institute for Quantum Science & Technology in Calgary, Canada, and colleagues [1] and the other by Yang Liu, at the Hefei National Laboratory for Physical Sciences and the University of Science and Technology of China, and colleagues [2] now report a new quantum encryption method that can remove the weakest link of quantum encryption schemes: loopholes associated with defects of the photodetectors used at the receiver end. Code makers have now regained the upper hand against code breakers.

Code makers and code breakers have been fighting for thousands of years. With the rise of the Internet, the importance of communication security is growing. Each time we do online banking or use messaging apps on our smart phones, we should be concerned about communication security. Conventional (classical) cryptographic systems are often based on unproven computational assumptions.

In contrast, quantum encryption methods such as quantum key distribution (QKD)—the use of quantum states to transmit a shared encryption key between communicating parties—offer, in principle, unconditional security based on the laws of physics. This is an ideal solution in the long term, but we are not there yet: while QKD schemes have been demonstrated and have already led to commercially available products, a few research groups, in the last few years, have reported a number of high-profile successful hacks [3] against QKD systems, thus casting doubts on the security of practical QKD. Charles Bennett [4], an IBM Fellow and a co-inventor of quantum cryptography, wrote: "Photon detectors have turned out to be an Achilles' heel for quantum key distribution (QKD), inadvertently opening the door ... to subtle side-channel attacks."

In one hacking example, Eve (the eavesdropper) can blind the detectors of Bob (the receiver) with a low-power, continuous-wave laser. While the detector is blinded, it works as a classical detector and loses the "quantum" protection: Eve can then intercept, unnoticed, Alice's (the sender's) signals. Countermeasures for quantum hacking have been proposed—such as security patches [5], teleportation tricks [6], and full device-independent QKD (DI-QKD) [7]—but all have been proven to be either *ad hoc* or impractical, e.g., not compatible with long-distance communications or with key generation at sufficient speeds.

The two new papers implement a new quantum encryption method called "measurement-device-independent" QKD (MDI-QKD) that was first put forward in 2012 by my research group [8] and appears today to be the only practical solution to quantum hacking at the detector side. A simplified schematic diagram of a possible MDI-QKD setup is shown in Fig. 1. The security of MDI-QKD relies on a time-reversed version [9] of an Einstein-Podolsky-Rosen (EPR) type of QKD protocol. In essence, Bob and Alice generate sequences of randomized pulses and send them to a third party (which may

DOI: 10.1103/Physics.6.104
URL: http://link.aps.org/doi/10.1103/Physics.6.104

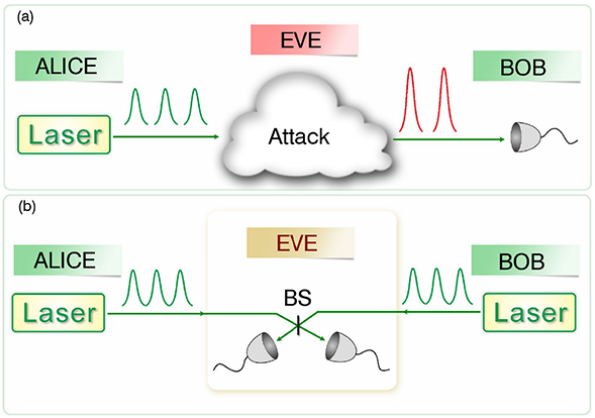

FIG. 1: (a) Conventional prepare-and-measure QKD setup, in which Alice sends qubits to Bob through an insecure quantum channel, controlled by Eve. (b) MDI-QKD setup: both Alice and Bob send quantum signals to a detection station for a Bell-state measurement. The two signals interfere in a beam splitter and are then sent to two detectors, which reveal publicly which qubit pairs are in the same Bell states (without revealing their values). Such qubits form the secret encryption key shared by Bob and Alice. Even if Eve controls the measurement station, she cannot gain information on the final key without being noticed. (Y. Liu *et al.*, Phys. Rev. Lett. (2013))

even be an untrusted eavesdropper, Eve) who performs a so-called Bell-state measurement of the two incoming signals: the outcome of the measurement is successful for those combinations of Alice's and Bob's photons that are in the same Bell state. These measurements do not need to be secret: once the results are publicly announced, they allow Bob and Alice to pick the sequence of bits associated with successful Bell's measurements as their private encryption key. What makes MDI-QKD practical is the fact that it can work with attenuated laser pulses (as opposed to ideal single-photon sources) and with so-called decoy state techniques (which use decoy signals to confuse Eve and allow Alice and Bob to obtain additional information to detect Eve's action) [10].

MDI-QKD has the remarkable advantage of being inherently immune to all attacks against detectors, thus foiling all such existing and potential attacks. In fact, with MDI-QKD, one could even outsource the manufacturing of photon detection systems—the most challenging component of QKD—to an untrusted party without compromising security. This means, for instance, that a top-secret communication between two countries could be securely held even with a completely untrusted network node manufactured by a third, hostile party—a dream scenario in communication security.

The papers by Rubenok *et al.* and Liu *et al.* are important because they bring us closer to the practical application of MDI-QKD, showing that it can work on actual fiber links of a certain length, and, unlike the original demonstration paper [8], even if Bob's and Alice's signals have different intensities.

Rubenok *et al.*'s [1] experiment is the first field test of MDI-QKD with installed fibers: the author provided both a lab demonstration of the MDI approach over more than 80 km of spooled fiber as well as over 18 km of installed fibers connecting different locations within the city of Calgary (Canada). The authors prove that a number of essential elements of MDI-QKD can be made to work. First, they show that the scheme can work with attenuated pulses of varying photon numbers, without relying on single photons. Second, as in Ref. [8] but now over much longer transmission distances, they manage to fulfil an important requirement: Bell-state measurements can work only if Bob and Alice send out photons that are not distinguishable (in terms of spectrum, polarization, and timing). This is achieved through the implementation of active stabilization systems. However, the article falls short of being a full demonstration of QKD: the authors transmit the same key a number of times but do not perform a random generation of key bits and signal intensities.

Liu *et al.*'s lab experiment [2] goes one step further and performs a real QKD experiment. Similarly to the experiment of Rubenok *et al.*, the authors use attenuated pulses and are able to control the pulses' spectrum, timing, and polarization to make them undistinguishable. Furthermore, they use trusted sources that generate truly random keys: randomized coherent states with intensity modulation. The authors evaluate the scheme's performance realistically, taking into account the finite length of the key. However, one should notice that their experiment requires expensive components for both state preparation and photon detection. For instance, expensive and complicated custom-made detectors are used, which may be available to only a few research groups in the world.

What lies in the future? Both experiments used a specific encoding scheme called time-bin encoding (in which information is encoded in photons arriving at different times). One needs to demonstrate the versatility of MDI-QKD with other popular encoding schemes such as polarization encoding [11]. Practical applications also demand higher speed: it is reasonable to think that the 1-megahertz scheme of Liu *et al.* may be extended to the delivery of secure keys at gigahertz rates. Finally a more systematic parameter optimization will need to be carried out and an MDI-QKD demonstration with standard commercial off-the-shelf single-photon detectors will be needed to pave the way for widespread deployment. In the longer term, demonstrating the feasibility of MDI-QKD in a network setting (as opposed to a one-to-one conversation) will be an important milestone. Conceptually, MDI-QKD allows many individual users to use, at their end, only simple signal preparation devices and outsource expensive and complex measurement devices to even untrusted network providers, which is very appealing for network security [12].

Should the above-mentioned outstanding issues be re-

DOI: 10.1103/Physics.6.104
URL: http://link.aps.org/doi/10.1103/Physics.6.104

solved, MDI-QKD will change the landscape of security research in QKD by making quantum hacking against detection systems obsolete, thus forcing quantum code breakers to attack QKD at the signal preparation stage in future.

Acknowledgments

H.-K. Lo acknowledges enlightening discussions with colleagues including Bing Qi, Li Qian, and Feihu Xu.

References

[1] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks," *Phys. Rev. Lett.* **111**, 130501 (2013).

[2] Y. Liu *et al.*, "Experimental Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* **111**, 130502 (2013).

[3] Y. Zhao *et al.*, "Quantum Hacking: Experimental Demonstration of Time-Shift Attack Against Practical Quantum Key Distribution Systems," *Phys. Rev. A* **78**, 042333 (2008); F. Xu, B. Qi, and H.-K. Lo, "Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System," *New J. Phys.* **12**, 113026 (2010); L. Lydersen *et al.*, "Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination," *Nature Photon.* **4**, 686 (2010); I. Gerhardt *et al.*, "Full-Field Implementation of a Perfect Eavesdropper on a Quantum Cryptography System," *Nat. Commun.* **2**, 349 (2011); N. Jain *et al.*, "Device Calibration Impacts Security of Quantum Key Distribution," *Phys. Rev. Lett.* **107**, 110501 (2011); Q. Liu *et al.*, "A Universal Setup for Active Control of a Single-Photon Detector,"arXiv:1307.5951 (2013).

[4] C. H. Bennett, "Let Eve do the heavy lifting, while John and Won-Young keep her honest," `http://dabacon.org/pontiff/?p=5340`.

[5] Z. L. Yuan, J. F. Dynes, and A. J. Shields, " Reply to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'"," *Appl. Phys. Lett.* **99**, 196102 (2011).

[6] See H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science* **283**, 2050 (1999), footnote 21.

[7] D. Mayers and A. C.-C. Yao, *"Quantum Cryptography with Imperfect Apparatus," in Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (FOCS98), (IEEE Computer Society, Washington, DC, 1998); A. Acin *et al.*, "Device-Independent Security of Quantum Cryptography Against Collective Attacks," *Phys. Rev. Lett.* **98**, 230501 (2007); N. Gisin, S. Pironio, and N. Sangouard, "Proposal for Implementing Device-Independent Key Distribution Based on a Heralded Qubit Amplifier," *Phys. Rev. Lett.* **105**, 070501 (2010); M. Curty and T. Moroder, "Heralded Qubit Amplifiers for Practical Device-Independent Quantum Key Distribution," *Phys. Rev. A* **84**, 010304 (2011).

[8] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.* **108**, 130503 (2012).

[9] E. Biham, B. Huttner, and T. Mor, "Quantum Cryptographic Network Based on Quantum Memories," *Phys. Rev. A* **54**, 2651 (1996); H. Inamori, "Security of Practical Time-Reversed EPR Quantum Key Distribution," *Algorithmica* **34**, 340 (2002); See also S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.* **108**, 130502 (2012).

[10] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.* **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.* **94**, 230504 (2005); X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Phys. Rev. Lett.* **94**, 230503 (2005).

[11] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporao, and J. P. von der Weid, "Proof-of-Principle Demonstration of Measurement Device Independent QKD Using Polarization Qubits,"arXiv:1207.6345 (2012).

[12] R. J. Hughes, "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection,"arXiv:1305.0305 (2013); B. Fröhlich *et al.*, "A Quantum Access Network," *Nature* **501**, 69 (2013).

About the Author

Hoi-Kwong Lo

Hoi-Kwong Lo is a Professor of Physics and Electrical and Computing Engineering at the University of Toronto. He received his Ph.D. in physics from Caltech in 1994. After performing research at the Institute for Advanced Study in Princeton, NJ, Hewlett-Packard Labs in Bristol, UK, and MagiQ Technologies, Inc., New York, NY, he joined the University of Toronto as an Associate Professor in 2002 and became a Full Professor in 2009. His current research interest is quantum information processing, particularly the theory and experiment of quantum cryptography. He was a Founding Managing Editor of the leading journal *Quantum Information and Computation* from 2001 to 2008. For more information see http://www.comm.utoronto.ca/ hklo/.

DOI: 10.1103/Physics.6.104
URL: `http://link.aps.org/doi/10.1103/Physics.6.104`