Title: Laser damage creates backdoors in quantum cryptography

Authors: Shihan Sajeed, Poompong Chaiwongkhot, Mathieu Gagné, Jean-Philippe Bourgoin, Carter Minshull, Matthieu Legré, Thomas Jennewein, Raman Kashyap, and Vadim Makarov

Abstract: Our society relies on cryptography daily. Currently, mathematical complexity-based methods are used for encryption. Their security is threatened by the development of quantum computer, and by advances in cryptanalysis. The mathematical methods thus need to be replaced. One likely replacement is quantum-physics-based secure communication protocols. For example, quantum key distribution (QKD) allows two remote parties to grow a shared secret key in a manner that is resistant to future quantum computers. QKD has seen an impressive technological progress over the past 20 years, and is commercially available today.

The security of QKD is based on the laws of physics: it is impossible to measure an unknown quantum state without altering it. The QKD protocol guarantees that any attempt of eavesdropping will be detected. However, as for any cryptographic system, QKD security relies on both the QKD protocols and the implementation devices on which this protocol runs. However, implementation devices are not perfect. Their behaviour often deviates from the idealized behavior. This often opens exploitable loopholes that compromise the security. Still, if the imperfections are known, the assumed model can be changed and security proofs can be modified to guarantee security. In summary, practical quantum communication protocols are assumed to be secure, as long as implemented devices are properly characterized and all known side channels are closed.

Does it mean, we have reached an unbreakable secure communication protocol, and ended the struggle of cryptographers versus hackers? Not so fast! Even though there is no limit on how perfectly implemented devices can be characterized, an eavesdropper can still create new deviations on-demand in an installed QKD system by laser damage. We present a proof-of-principle demonstration of this. We utilize laser damage to modify device characteristics to break the security of an installed QKD system [1].

Our experiment involved a free-space QKD system for long distance satellite communication [2]. It has been shown in [2] that the system must include a spatial filter or 'pinhole' for security against certain attacks. We have tested the endurance of the system with the pinhole installed against laser damage. From a distance of 26 m, we shot an 810 nm laser beam, delivering 3.6 W c.w. power at the pinhole. The intensity there was sufficient to melt the material and enlarge the hole diameter from 25 μm to ≈ 150 μm. With the enlarged pinhole opening, it was again possible for eavesdropper to compromise the security [1,2]. Thus laser damage completely neutralizes the spatial filter countermeasure.

Attacking quantum key distribution systems is a new application for laser damage. Actively engineering imperfections via laser damage represents perhaps the ultimate possibility to breach security of quantum communication. We are excited to present and discuss this new application with the laser damage community, and foster new cross-disciplinary collaboration.

Note: Preliminary results of this investigation were accepted for talk at this conference in 2014, however we could not present it in 2014 owing to delays with obtaining US visa. We now have new and much stronger results. The presenter now has the visa and will deliver the talk if it is accepted again. The preprint version of this work can be found on: http://arxiv.org/abs/1510.03148

[1] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, arXiv:1510.03148 [quant-ph].

[2] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).