Security of Quantum Key Distribution

Normand Beaudry, Agnes Ferenczi, Varun Narasimhachar, Tobias Moroder, Xiongfeng Ma, Marco Piani, Norbert Lütkenhaus

Institute for Quantum Computing, and Department of Physics & Astronomy, University of Waterloo, 200 University Avenue W, Waterloo, ON, N3L 3G1, Canada

nlutkenhaus@iqc.ca

Abstract: Quantum Key Distribution offers the promise of secure communication at unprecedented security level. Secure systems can be implemented by standard optical communication components - if done right. We report on the divide of right and wrong.

OCIS codes: (060.4785) Optical security and encryption; (270.5568) Quantum cryptography

1. Introduction

Quantum Key Distribution (QKD) offers the promise of unprecedented security levels for secure communication, as the protocols themselves can be proven to be secure against adversaries with unlimited computation power. QKD is naturally a point-to-point technology with a limited distance due to technological limitations. For a review see [1]. Thanks to reconfigurable optical paths and related ideas it can be extended easily turned into a multi-user application, and by introduction of trusted nodes (trusted repeater network), it can be developed into a scalable secure network [2,3]. In future, with the development of quantum repeater technology, the trust assumption into the connecting nodes will be eliminated and we obtain a fully operational quantum network. Even today, with the trusted repeater networks, QKD becomes attractive for user operated networks, while the fully quantum networks would be interesting in a service provider scenario. The advance of QKD technology led already to an ETSI Industry Specification Group [4], aiming at certification procedures for QKD and also for standardization of interfaces and operation conditions.

The clear advantage of QKD is the provable security of its key distribution protocols. These security proofs can be derived also for optical implementations using standard components such as threshold photo-detectors and laser pulses. However, these security proofs rely on a generic modeling of these devices. By definition, a device always deviates from a model, and we have to learn how to deal with this. In this talk I will outline first how security proofs work within quantum optical models for devices, and then will address the security of actual implementations.

2. Optical Implementations

For fiber optical communication, the most widespread implementations of QKD use a phase encoding [5,6], where specific settings of relative phase between two subsequent laser pulses encode the signal information, which is then read out in an interferometric configuration, so that constructive or destructive interference in time slots indicate the signal value. Detection is usually done with some photo-detectors in the avalanche regime (threshold detectors) which are sensitive to single photons.

The set-up is usually designed in such a way that for a single photon source the system would implement exactly the ideal QKD protocol. However, typically we use attenuated laser pulses as signal sources and also the detectors are actually sensitive to modes, not only single photons, so that we have to worry also about adversaries that insert signals comprised of many photons into the detector.

So what about the security of these systems? Over time, security proofs based on abstract qubits (quantum mechanical two-level systems) emerged [7,8] and now became easy to use [9]. But, as we said, our systems operate with optical modes, which correspond to infinite dimensional Hilbert spaces. Fortunately, we have two basic tools that connect our practical optical implementations to these qubit based proofs:

a) Source: tagging

Tagging [10,11] is a valuable method when dealing with sources that emit statistical mixtures of the desired single photon signal, vacuum signals, and also multi-photon signals. Multi-photon signals might give away part or the complete information about the relative phase of pulses, and moreover, they would require larger dimensional Hilbert spaces to describe them. Tagging now simply means that we simply pretend that the source gives the complete information about the encoded information for all multi-photon signals to Eve. Therefore, we are left with the ideal single photon states as qubits, and then having vacuum and multi-photon signals which we now can

describe classically, as in both cases an adversary is supposed to know exactly which state he/she gets, either a information-free vacuum state, or the full classical information about the encoded information for multi-photon states. It turns out, that as long we can verify that at least some single-photon signals contributed to the detected signals in a worst case scenario, we can still do QKD.

b) Receiver: Squashing

On the receiver side, we tend to talk about threshold detectors as single-photon detectors, but that refers to the fact that a single photon suffices to trigger the event. What is does not mean is that indeed only single photons trigger it. Even if we use ideal single photon sources on the sending side, an adversary might employ an eavesdropping attack which results in multi-photon signals entering the receiver's device. In actual implementations we already notice that in the fact that with some probability actually more than one detector in the receiver is triggered. A real protocol must define what to do with these events. It turns out that we cannot simply discard these events, but have to keep a record of it. Otherwise, a simple intercept/resend attack can break the QKD implementation in extreme cases.

To avoid this situation, we can make use of squashing models of detection devices [12,13]. These squashing models are thought set-ups that allow us to think about the detection process as a two-step (see Fig. 1):

i) in a first step, the incoming light modes are mapped into a qubit signal space corresponding to a single photon (squashing map),

ii) in a second step, the idealized original measurement is performed on that single photon (target measurement).

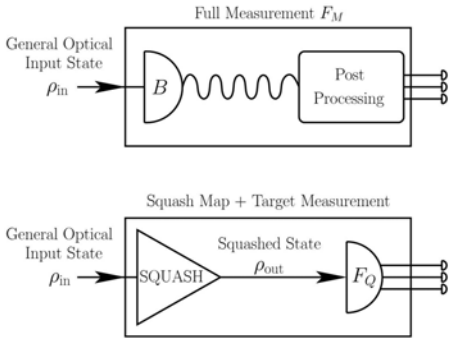

Fig 1. Diagram of full optical measurement and Though-Setup involving a Squashing Map and an idealized target measurement.

Whenever an actual detection device allows this though-setup description, we can start our security analysis with our signal after the first step, so that we can assume without loss of generality that indeed single photons impinge on the detection device.

Two things are important:

For this to work, the detection device to be considered must include the post-processing of data in such a way that the equivalence to a single-photon detection is at all possible. In the case of two detectors monitoring the outputs of an interferometer, this means that we have to declare what the post-processing does to double clicks. In our cases, it turns out that the earlier proposed method [14,15] to assign double clicks randomly as a single click of one of the detectors is a good strategy.

Secondly, the squashing model of detection are context independent, that means, the decomposition into the two steps works independently of the application, and has therefore consequences beyond QKD [16].

In our analysis we found that typical receivers for the BB84 protocol indeed possess a description in the squashing model with the right double click assignment.Combining these tools with the technique of decoy states [17-19], we obtain a secret key rate which scales linearly in the transmission efficiency of the quantum channel.

In interferometric schemes, one uses often a Mach-Zehnder set-up [5,6]. Here in one of the paths a phase shifter is inserted so that one can set the phase of the emerging two pulses. The additional loss in the phase shifter leads to a signal amplitude which differs for the first and the second pulse. Note that this changes the structure of the signal states even for the single photon contributions. We do not notice in the usual experiments, as the receiver has also a phase shifter with the same insertion loss, which compensates the amplitudes of the interfering pulses. However, the security proof has to be adapted to this situation, and we will show the result.

3. Difference between protocols and implementations

As pointed out before, it is important to remember that there is the difference between a protocol based on quantum optical models of devices and the actual implementation. I will give a quick review over the work of several groups [20-22] around the world with the most important attacks that are directed at this deviation between models and devices. Also, I will present the view what the implications for secure QKD are. Clearly, any implementation needs to contain sufficient elements to verify basic model assumptions while running the device.

4. Conclusion

Quantum Key Distribution is an active field which offers the opportunity for research on fundamental question about what the enabling power of quantum mechanics, but which also offers room to utilize and to drive optical communication engineering capabilities [23]. In doing so, one has to be careful to maintain the proper conditions for the security to be claimed.

5. References

[1] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, "A Framework for Practical Quantum Cryptography", Rev. Mod. Phys. **81**, 1301 (2009).
[2] M. Peev et al, "The SECOQC quantum key distribution network in Vienna", New J. Phys. **11,** 075001 (2009).
[3] T. E. Chapuran et al, "Optical networking for quantum key distribution and quantum communications", New J. Phys **11**, 105001 (2009).
[4] ETSI ISG group homepage, http://portal.etsi.org/portal_common/home.asp?tbid=723
[5] Z. L. Yuan et al, "Practical gigahertz quantum key distribution based on avalanche photodiodes", New J. Phys **11**, 045019 (2009).
[6] D. Rosenberg et al, "Pracitcal long-distance quantum key distribution system using decoy levels", New J. Phys. 11, 045009 (2009).
[7] D. Mayers, "Unconditional security in quantum cryptography", JACM **48**, 351-406 (2001).
[8] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,"Phys. Rev. Lett. **85**, 441-444 (2000).
[9] R. Renner, "Symmentry of large physical sysytems implies independance of subsystems," Nature Physics **3**, 645-649 (2007).
[10] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution", Eur. Phys. J. D **41**, 599-627 (2007).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comp. **4**, 325 (2004).
[12] T. Tsurumaru and K. Tamaki, "Security proof for QKD systems with threshold detectors", Phys. Rev. A **78**, 032302 (2008).
[13] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing Models for Optical Measurements in Quantum Communication," Phys. Rev. Lett. **101**, 093601 (2008).
[14] N. Lütkenhaus, "Estimates for practical quantum cryptography," Phys. Rev. A **59**, 3301-3319 (1999).
[15] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
[16] T. Moroder, O.Gühne, N.J. Beaudry, M. Piani, N. Lütkenhaus, "Entanglement verification with realistic measurement devices via squashing operations", http://arxiv.org/abs/0909.4212 (2009).
[17] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett **91,** 57901(2003).
[18] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94**, 230504 (2005).
[19] X. B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
[20] V. Makarov, "Controlling passively quenched single photon detectors by bright light", New J. Phys. 11, 065003 (2009).
[21] A. Lamas-Linares, C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," Opt. Express **15**, 9388 (2007).
[22] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, "Experimental demonstration of time-shift attack against practical quantum key distribution systems," Phys. Rev. A **78**, 042333(2008).
[23] N. Lütkenhaus, A.J. Shields, Editorial on Special Issue on "Quantum Cryptography: Theory and Practice", New J. Phys. **11**, 045005 (2009).