Quantum-Computational Hybrid Cryptography based on the Boolean Hidden Matching Problem

Romain Alléaume
Télécom ParisTech - LTCI, Institut Polytechnique de Paris, 46 rue Barrault, 75013 Paris, France

March 15, 2019

Abstract

A central objective of quantum cryptography, and in particular of quantum key distribution (QKD), has been to propose and demonstrate that the use of quantum resources, and notably quantum communication resources, allows to perform cryptographic tasks that are unachievable with classical means. An important difference between classical cryptography (CC) and quantum cryptography (QC) lies in the security model. While modern CC protocols typically rely on computational hardness assumptions, QC has essentially aimed at unconditional security, however often at the expense of practicality and performance [1].

We propose here to modify this perspective and explore how to build bridges between CC and QC. In this perspective, we introduce a novel security model named quantum-computational hybrid (QCH), that consists in two assumptions: Existence of short-term encryption, perfectly secure during a relatively short time t_{comp} and Noisy quantum memories that are assumed to fully decoherence over a time shorter than t_{comp}. One can note that the validity of the QCH model seem solidly grounded when one considers existing and prospective quantum storage capabilities and puts them in perspective with even a pessimistic lower bound on t_{comp} such as $t_{comp} \geq 10^5\,\mathrm{s} \sim 1\,\mathrm{day}$.

Our main contribution is to propose a general framework for direct secure classical communication that we name quantum computational timelock (QCT). QCT leverages on the QCH model to build quantum cryptographic protocols that exhibit functionalities and performances that can scale well beyond *QKD*, while enjoying the property of being everlasting secure, i.e. information-theoretically secure after t_{comp}.

We propose an explicit construction for a protocol called Hidden-Matching Quantum Computational Timelock (HM-QCT). This protocol is based on the Boolean Hidden Matching (BHM) introduced in [2], for which there exists an exponential gap in one-way communication complexity between classical and quantum strategies. We establish the security of HM-QC through reduction to the Boolean Hidden Matching problem. This reduction leverages on the QCH assumptions in order to guarantee that any non-authorized attacker is limited to classical eavesdropping. An attractive feature of HM-QCT is that it is implementable with existing photonic technology, namely multimode coherent states encodings, linear optics, and only two threshold detectors. The performance scaling of HM-QCT, implemented over n bosonic modes relies on the fact its security can be guaranteed with while sending $O(\sqrt{n}$ photons per channel use. This allows to boost, possibly by several order of magnitude, key rates in comparison with QKD, that is limited to less that one photon per channel use. HM-QCT can moreover also lead to an important increase of reachable distances, but also in improved functionalities and practicality, stemming from reduced trust requirements on hardware implementations.

We finally point out that the quantum computational timelock framework, and the proof technique developed for HM-QCT based on a reduction to a communication complexity problem can be of independent interest in other quantum cryptographic contexts. We hope that it can also lead to interesting news connections between quantum cryptography, physical layer security and computational cryptography.

References

[1] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8:15043, 2017.

[2] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525. ACM, 2007.