An hybrid security model for quantum cryptography for practical and efficient information-theoretically secure communication

Romain Alléaume[1]

[1] *Telecom ParisTech - LTCI, CNRS , 46 rue Barrault, 75013 Paris, France*

We will present a new security model in quantum cryptography, exploiting the assumption that any quantum memory is bound to decohere in a finite time during which perfect encryption could hold. We propose a new quantum cryptographic protocol in this context, and argue that can be it can offer an efficiency gap (in terms of tolerable losses and errors) compared to QKD.

Recent work on quantum data locking, whose security is based considering the accessible information [1], clearly illustrates that a relaxation of the composable security criteria that is commonly used in Quantum Key Distribution (QKD) [2, 3], can allow to design new quantum cryptographic protocols for secure communications, with improved performances. It is for example known that the locking capacity of a quantum channel is always larger than its private capacity, while it has recently been proven that quantum data locking schemes could allow to approach the classical capacity of a quantum channel. [4]

However, all quantum data locking schemes proposed so far rely on the encoding on some classical information into a large entangled state, a procedure that cannot be easily realized experimentally in the near future.

We propose a new security model for secure communication rely on a public quantum channel and an authenticated classical channel, between Alice and Bob wherein the eavesdropper E can only store quantum information during a finite time τ, to technological limits of quantum memory while Alice and Bob can use specific encryption scheme.

We can argue that both of these assumptions can be considered realistic, given the state of current technology:

Decoherence is a fundamental limitation of quantum memory. While decoherence can in principle be handled by designing and engineering carefully isolated qubits and by using fault-tolerant architectures such as topological codes, the experimental challenges to progress in this direction remain very important. One could consider for τ an optimistic upper bound on the coherence time for the coherent storage of a few qubits, and could relatively safely work with values of τ below a s.

Practical and computationally efficient classical encryption exist, like AES 256. Although such schemes are not information-theoretically secure, we do not know in practice any classical (or quantum) algorithm to break such schemes more efficiently than brute-force. We can also note that most practical QKD demonstrations combine QKD with a classical encryption scheme such as AES, which implicitly assumes that AES security is strong.

We will then present the status of a current work in progress: build an explicit protocol that allows to efficiently lock classical information, at a rate far beyond the private capacity, without resorting to the use of large entangled state at the input like in quantum data locking [4].

[1] S Guha, P Hayden, H Krovi, S Lloyd, C Lupo, JH Shapiro, M Takeoka, Quantum enigma machines and the locking capacity of a quantum channel, Physical Review X 4 (1), 011016, (2014).

[2] C.H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in Proc. of International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[3] R. Renner, *Security of Quantum Key Distribution*, PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005.

[4] C Lupo, S Lloyd, Quantum-locked key distribution at nearly the classical capacity rate, Phys. Rev. Lett. 113, 160502 (2014)