Cryptographic primitives for quantum networks

Iordanis Kerenidis[1,2]

[1] LIAFA, CNRS, Université Paris Diderot, Paris, France
[2]Centre for Quantum Technologies, National University of Singapore, Singapore

Abstract

We study a number of fundamental cryptographic primitives that can be used as building blocks for constructing secure quantum networks. Such primitives include coin flipping, bit commitment, oblivious transfer etc. They are widely used in classical networks, nevertheless their security is based on computational assumptions, since information theoretic security is impossible. In this tutorial, we study these primitives in the quantum world under various security definitions.

We start by looking at bit commitment and coin flipping with information theoretic security: we fully analyze a simple protocol for bit commitment; we provide tight lower bounds based on a relation between fidelity and trace distance of quantum states and on Kitaev's formulation of protocols as semi-definite programs; and we describe optimal protocols based on Mochon's protocol for weak coin flipping with arbitrarily small cheating probability.

We then describe other security models, including the noisy storage, device independent and relativistic models, and provide the main ideas on how to construct protocols in these models.

We conclude by discussing the practicality and efficiency of these protocols and how/whether they can be used in future quantum networks.