General paradigm for distilling classical key from quantum states - entanglement approach to quantum security

Karol Horodecki[1,2,3]
[1] *Institute of Informatics, University of Gdańsk, 80–952 Gdańsk, Poland*
[2] *Institute of Theoretical Physics and Astrophysics University of Gdańsk, 80–952 Gdańsk, Poland and*
[3] *National Quantum Information Center of Gdańsk, 81–824 Sopot, Poland*

Quantum cryptography provides the protocols for generation of shared secret key between two honest parties that are far from each other, which can be used for the *one-time-pad* encryption.

Some of the protocols and most of the simplest security proofs are based on the fact, that there are special quantum correlations called *pure entanglement*. Entanglement of in general *mixed* quantum states is the merit of the *theory of entanglement*, developed since its beginning in parallel and with an apparent connection to quantum cryptography. Currently, interrelation between the two becomes more and more formalized.

In this thesis we present one of the firm links between quantum cryptography and theory of quantum entanglement as well as some consequences, steaming from the spin-off between the two. It is achieved by first studying the structure of bipartite quantum states that contain secure key.

We assume the *quantum worst-case* scenario, in which the honest parties together with an eavesdropper share a pure state $|\psi\rangle\langle\psi|_{ABE}$. We characterize the *bipartite* states (of AB subsystem of $|\psi\rangle\langle\psi|_{ABE}$) that have directly accessible secure key, called further **private states**.

We then focus on the case of *collective attacks* according to which the parties share multiple copies of some pure state $|\phi\rangle\langle\phi|_{ABE}$, i.e. the state $|\phi\rangle\langle\phi|_{ABE}^{\otimes n}$ for some natural n. The honest parties are far apart but can operate locally each at her/his site, and communicate with each other, processing the AB subsystems. The subsystems E are with the eavesdropper who can listen to their communication.

The link we provide is quantitative. The amount of security that can be extracted from a tripartite state $|\phi\rangle\langle\phi|_{ABE}$ in the collective attacks scenario is shown to be equal to an *entanglement measure*, called **distillable key**, which is a function of *solely* the bipartite state of AB subsystem of $|\phi\rangle\langle\phi|_{ABE}$.

In spirit of entanglement theory, distillable key is defined as the maximal number of secure bits obtained in a form of some private state by means of local operations (at each site) and communication called 'classical' - over e.g. a cellphone - between the honest parties that are far apart. Thus, distillable key is to be associated with a reach class of private states, which are in general *mixed* and includes the well known *pure* entangled state called *singlet*. In contrast to singlet state, some of the private states are shown to be hardily distinguishable from *separable* (insecure) states when shared by the honest parties, and can exhibit an effect called **locking of entanglement**.

Entanglement approach allowed among others for establishing an **upper bound on distillable key**, in terms of entanglement measure called *relative entropy of entanglement*. The major consequence of this approach is the fact, that not only the states that can be transformed into pure entangled states by the honest parties contain security. We show, that there are some **bound entangled states**, (whose entanglement can not be made pure by the honest parties in this scenario), **that contain secure key**. This result implies, that the honest parties may sometimes communicate in private using quantum security, despite of the fact, that they can not communicate faithfully quantum data.

In this thesis we present some details of the results invoked above, give a short guide over some new results obtained in terms of private states over past years, and provide a bunch of open problems.