Reg. No: 2015/18/E/ST2/00327; Principal Investigator: dr Karol Mieczysław Horodecki

In recent years our civilization generates more stored information in several days than the amount of it generated and stored since the beginning of the mankind till nowadays. According to the “global village” effect there is a constant growth of need for sending this information at large distances. Its non-negligible percentage are the so called sensitive data including personal ones protected by low, and e.g. copyrights protected as well. All these data are vulnerable to various attacks and their practical protection is a difficult problem nowadays.

Partial solution to this problem is offered by quantum cryptography – a fast developing domain of quantum informatics whose task is to assure secure transfer of information guaranteed by the laws of physical theory - quantum mechanics. This problem concerns also the post-quantum cryptography where security is assured by the physical principle of no-faster-than-light communication. These multidisciplinary domains involve physics, mathematics and informatics. Due to both of them making use of physical axioms one can prove on ground of mathematics that informatics-like goal – the security of transfer of information is achieved if only the information is encoded in a proper way – according to the so called cryptographic protocol.

The main task of particular quantum and post-quantum protocols is to achieve one of the two resources: private random bit string – (secure randomness) or private shared random bit string – shared only by the honest parties, which is the so called cryptographic key.

The devices realizing cryptographic protocols are already available commercially by now, and although protecting against simple eavesdropping, they are vulnerable to the newest kind of attacks –that of hacker’s brake-in. Theory concerning such attacks is not much developed by now. Certain publications concern mainly the attacks called “Trojan horse” ones, which mainly attack the devices of the honest parties in real time, While more sophisticated, including attack during the production or before use are even less studied. We come to define main tasks of our project. One of them is to find qualitative and quantitative dependence of obtained cryptographic resource (key and/or randomness) from strength and type of the hacker’s attack. We are going to develop a theoretical model enabling estimation of security of the transfer or storage even in case of a partial break-in.

Another weak point of quantum cryptography in its original approach, is the fact that the user has to trust the device’s specification. Such a trust can be in some cases not justified, due to imperfections of implementation or even maliciously produce a device ready to be eavesdropped from the beginning.

For this reason another task of the project will amount to search for possibility of communication in case of cooperation of the producer and eavesdropper. The research will also concern developing theory of randomness, known as resource theory.

For the above reason, our area of investigation will in main part concern the device independent cryptography: the user will trust only the statistics of the device, not its specification.

However, due to the fact, that the scenario in which the user trusts the provider is much more technologically advanced, we will consider also this scenario. In turn we believe to get to know the amount of privacy in the so called, not yet much studied private states, as well as obtain theoretical framework for obtaining secret randomness.

We expect also, that the result allow the users for more conscious use of the quantum-cryptographic devices even in case of only partial control and in presence of noise. We also hope, which is the third main task is that the proof techniques worked out in cryptographic context as well as some new one that we will find, can be useful in studying the main phenomena of quantum mechanics – quantum entanglement, quantum non-locality and contextuality.

Due to, as we have argued in the beginning, the big challenge of our civilization of XXIst century – surely the century of information, research regarding protection of information against various attacks, is among those the most welcome.