# Quantum information and cryptography

prof. dr hab. P. Horodecki (WFTiMS PG)

Quantum information is a branch of modern science which is a highly nontrivial composition of quantum mechanics and information theory that originates from Shannon and Turing works. Historically the first discoveries that founded that field were the idea of quantum money that are impossibility to counterfeit (S. Wiesner, 1970) and quantum cryptography with polarized photons (C. H. Bennett and G. Brassard, 1984).

The present lecture will be devoted to essential ideas of quantum information with a special attention paid to quantum cryptography - the discovery that is already commercially available. First we shall review basic axioms of quantum mechanics including especially quantum measurement theory. Then we shall introduce the notion of quantum bit. Some counterintuitive properties of quantum bits will be presented including the property of strong correlations called quantum entanglement. Elementary quantum communication tasks will be discussed. In particular notion of quantum channel will be introduced and illustrated physically.

Then fundamental quantum analogs of informational theoretic quantities will be defined (von Neumann entropy, coherent information and quantum mutual information) together with their properties. Then the main ideas of classical cryptography will be discussed together with the corresponding classical informational theoretical quantities.

With all those tools the original quantum cryptographic protocol Bennett and Brassard (BB4) protocol will be presented. Then its entanglement based scheme due to Ekert (E91) will be discussed. General equivalence between those protocols will be proven via so called ,,prepare and measure" scheme. Limitations of the schemes will be pointed out in the case of channels with so called zero quantum capacity.



Projekt „Rozwój interdyscyplinarnych studiów doktoranckich na Politechnice Gdańskiej w zakresie nowoczesnych technologii" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

Here we shall also derive surprising extension of cryptography scheme beyond BB84.

Then further issues crucial to quantum cryptography will be analyzed. The first is unconditional security ie. the security in case of channels with the presence of memory.

Here the importance of quantum de Finnetti theorem will be stressed. The second issue corresponds to device in depended security. This is the new concept in quantum security which can be verified on the basis of statistical outcomes of the cryptographic device with no reference to its internal structure.

The exemplary quantum implementations of cryptographic protocols via quantum opticalschemes including especially (i) BB84 type version on polarized photons and (ii) continuous variables versioned based on coherent states generated by lasers will be presented and discussed.



Projekt „Rozwój interdyscyplinarnych studiów doktoranckich na Politechnice Gdańskiej w zakresie nowoczesnych technologii" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.