Unconditionally secure communication protocol based on superdense coding - development of non-local entanglement based quantum communication concepts

M. Jacak¹, W. Donderwich², J. Jacak¹, J. Gruber³, I. Jóźwik³, W. Jacak¹
¹ Institute of Physics, Wroclaw University of Technology, Wyspianskiego 27, 50-370 Wroclaw, Poland
² Institute of Informatics, Wroclaw University of Technology, Wyspy Piastowskiej 27, 50-370 Wroclaw, Poland
³ CompSecur sp. z o.o. R&D Department, ul. Pilsudskiego 74/309, 50-020 Wroclaw, Poland

Quantum Secure Direct Communication (QSDC)
- No secret key exchange for unconditional security in communication of classical information
- Entanglement distribution
- Quantum channel communication is fully deterministic
- No classical information communicated locally (non-local classical communication)
- No way to intercept the message

QSDC Protocol based on Superdense coding scheme
- A protocol based on the superdense coding scheme can be treated as a fundamental unconditionally secure communication model in quantum information and communication theory to which it is possible to reduce entanglement based quantum cryptographic protocols developments.

Towards development of the physical implementation of the entanglement QSDC protocol based on superdense coding scheme and AIT entanglement setup
- AIT system 1 AIT system 2
  - system overview
  - BBO crystal for entagelment generation
  - system overview
  - BBO crystal for entagelment generation
  - EPR source

Protocol description:
- Distribution of an entangled pair of photons between two parties (1) planning to securely communicate classical information. If entanglement distribution is not trusted, then the protocol should include the verification runs (randomly mixed between the protocol sending runs), as well as steps 1a., 2a., 3a., 4a., 5a.,
- Instead of performing the Ekert type or alike QKD protocol to establish shared random private key for a classical and quantum channel communication to Bob (non-local classical communication), it has been revised in the context of unconditionally secure communication by K. Bostrom and T. Felbing (1995).
- A superdense coding scheme, like a common quantum secret key distribution, provides the tool for transmitting classical information over a quantum channel but with no noise (perfect security) provided that each pair of EPR components is communicated by classical means.
- An entanglement-based quantum cryptographic protocol is used for quantum channel communication to Bob (non-local classical communication). This protocol includes the verification runs (randomly mixed between the protocol sending runs), as well as steps 1a., 2a., 3a., 4a., 5a.,

Protocol properties:
- Does not involve quantum distribution of secret private keys in order to provide unconditional security in communicating classical information
- Based on fundamental properties of maximally entangled qubit states and superdense coding scheme

Protocol problems:
- The practical aspects of the superdense coding based QSDC protocol are being analyzed, with special concern paid to providing proper identification of the corresponding, subsequent EPR pairs based on precise synchronization measures. On a theoretical level a quantified security comparison of this direct entanglement based quantum communication protocol with the EPR QKD protocol by A. Ekert is developed and the extensions are being made involving both operations and classical communication (LOCC). The quantum information Neumann entropy analysis of security in presence of noise is provided which is performed within the Schmidt representation framework accounting the fundamental property of all QKD protocols.

Summary and conclusions:
- Unconditional security of classical communication by quantum channel is feasible in the protocol based solely on the non-local phenomenon of the quantum entanglement (it is not based on a potentially questionable on a fundamental level ability to detect fluctuation that in principle should be introduced by an eavesdropper on a measured quantum channel being highly implementation-technology sensitive, but rather employing deeper non-linear properties of quantum mechanics as initially discussed in e.g. J. Barrett, L. Hardy, A. Kent, No-Signaling and Quantum Key Distribution, Phys. Rev. Lett. 95, 010503 (2005) or A. Acin, N. Gisin, L. Masanes, From Bell’s Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. 97, 204025 (2006).
- An unconditional and secure integrity of the communication within the protocol can be achieved in case of noise presence in a quantum channel, which is in principle a general situation requiring application of the entanglement purification methods.
- The unconditional security of the communication in the proposed entanglement QSDC protocol is device and implementation-technology independent.
- The aforementioned issues overlap with a framework of assumptions for most generally provable non-unconditionally secure QKD protocols (most general security proofs should be based on non-local entanglement properties, Bell inequality violation and impossibility of superimposition in contrast to possibly incomplete quantum mechanics postulates – essentially concerning quantum measurement; should account for general cases of noisy channels determined by inevitable decoherence and should be device or technology independent, a matter of high importance as is evident in context of a series of recently published papers discussing success/failure attacks on specific implementations).
- A protocol based on the superdense coding scheme can be treated as a fundamental unconditionally secure communication model in quantum information and communication theory to which it is possible to reduce entanglement based quantum cryptographic protocols developments.

Quantum Key Distribution (QKD) / Expansion (QKE)
- Secret key exchange
- With or without entanglement distribution
- QC communication completely indeterministic
- Classical information communicated locally after encrypting with the key (the key can possibly be compromised and in such case the message is intercepted a key is locally communicated in a classical channel)

Quantum Key Distribution (QKD) vs Entanglement based QKD
- Entanglement based non-local QKD protocol is more general than entanglement based QKD, as in particular, it can be used as a mean to unconditionally securely exchange a private (and it required also a truly random) secret key, as well as any other classical information (in a deterministic manner in contrast to non-deterministic communication that is an essential property of all QKD protocols).

Quantum Key Distribution (QKD) vs Quantum Communication (QC)
- QKD is in principle reduction-equivalent of non-entanglement quantum cryptography, as the basis for device independent security proof of the latter lies within the framework of entanglement purification concept
- non-entanglement quantum cryptography is a subcategory or a special case of a more general entanglement based communication
- it becomes equivalent in case when component of the EPR pair is immediately measured just upon generation

Research on novel protocols of secure, entanglement based quantum communication in quantum cryptographic systems supported by the National Research and Development Center of Poland NCBR within the INNOTECH program (Action NTech)