Wrocław University of Technology
WUT Institute of Physics
WUT Institute of Informatics

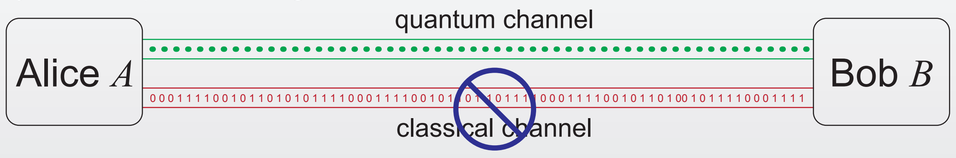
CompSecur IT Solutions

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

M. Jacak[1], W. Donderowicz[3], J. Jacak[1], J. Gruber[2], I. Jóźwiak[2], W. Jacak[1]
[1] Institute of Physics, Wrocław University of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland
[2] Institute of Informatics, Wrocław Univeristy of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland
[3] CompSecur sp. z o.o. R&D Department, ul. Piłsudskiego 74/309, 50-020 Wrocław, Poland

Quantum Secure Direct Communication (QSDC)

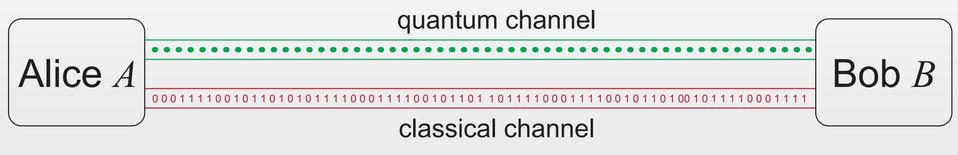
- No secret key exchange for unconditional security in communication of classical information
- Entanglement distribution
- Quantum channel communication is fully deterministic
- No classical information communicated locally (non-local classical communication)
- No way to intercept the message



fully deterministic non-local communication of classical information through a quantum channel

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 as it is locally communicated in a classical channel)



indeterministic communication of classical information through a quantum channel

QSDC Protocol based on Superdense coding scheme

Superdense coding scheme

(Ch. Bennett, S. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. 69, 2881, 1992)

- Originally published as a protocol that allows to encode 2 bits of classical information per single qubit
  - Without entanglement it is possible to encode just 1 bit of classical information per qubit
- The protocol has siginificant implications in a domain of information and communication security, enabling QSDC
- In 2002, 10 years after the original proposition of the superdense coding scheme, it has been revised in the context of unconditionally secure communication by K. Bostrom and T. Felbinger. K. Bostrom, T. Felibinger, Deterministic Secure Direct Communication Using Entanglement, Phys. Rev. Lett. 89, 187902 (2002)

Bell states

$$\left|\Psi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \otimes \left|1\right\rangle_B + \left|1\right\rangle_A \otimes \left|0\right\rangle_B\right)$$

$$\left|\Psi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \otimes \left|1\right\rangle_B - \left|1\right\rangle_A \otimes \left|0\right\rangle_B\right)$$

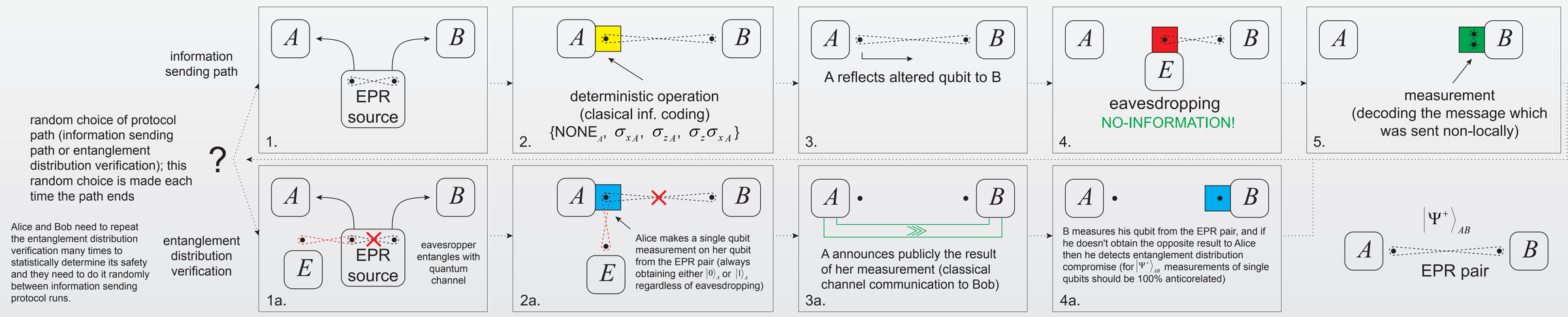
$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \otimes \left|0\right\rangle_B + \left|1\right\rangle_A \otimes \left|1\right\rangle_B\right)$$

$$\left|\Phi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \otimes \left|0\right\rangle_B - \left|1\right\rangle_A \otimes \left|1\right\rangle_B\right)$$

operation	EPR pair state	coding of classical inf.	
NONE_A	$\left\|\Psi^+\right\rangle_{AB} \to \left\|\Psi^+\right\rangle_{AB}$	00	$\Rightarrow I_A \otimes I_B \left\|\Psi^+\right\rangle_{AB} \to \left\|\Psi^+\right\rangle_{AB}$
σ_{xA}	$\left\|\Psi^+\right\rangle_{AB} \to \left\|\Phi^+\right\rangle_{AB}$	01	$\Rightarrow \sigma_{xA} \otimes I_B \left\|\Psi^+\right\rangle_{AB} \to \left\|\Phi^+\right\rangle_{AB}$
σ_{zA}	$\left\|\Psi^+\right\rangle_{AB} \to \left\|\Psi^-\right\rangle_{AB}$	10	$\Rightarrow \sigma_{zA} \otimes I_B \left\|\Psi^+\right\rangle_{AB} \to \left\|\Psi^-\right\rangle_{AB}$
$\sigma_z\sigma_{xA}$	$\left\|\Psi^+\right\rangle_{AB} \to \left\|\Phi-\right\rangle_{AB}$	11	$\Rightarrow \sigma_z\sigma_{xA} \otimes I_B \left\|\Psi^+\right\rangle_{AB} \to \left\|\Phi^-\right\rangle_{AB}$

2 bits of classical information communicated by 1 qubit in a quantum channel but non-locally

2 bits of classical information are only to be decoded from EPR pair

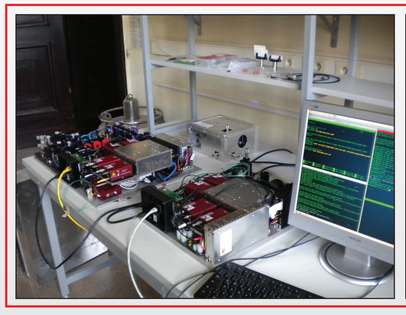


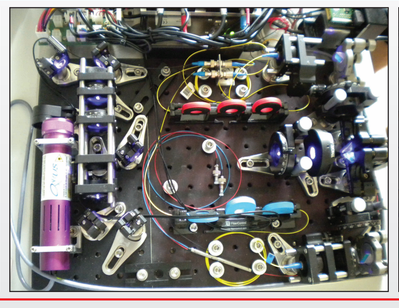
Towards development of the physical implementation of the entanglement QSDC protocol based on superdense coding scheme and AIT entanglement setup

- Theoretical concept of the superdense coding based non-local entanglement QSDC protocol and the associated developments are planned to be physically developed within two customized setups producing, detecting and synchronizing EPR photon pairs (AIT system) available to the research team in the National Quantum Technologies Laboratory NLTK and Compsecur laboratories (advanced laboratory infrastructure under supervision of the national network of the several leading Polish public universities and an academic spin-off R&D security information technologies company recently equipped in current state-of-the-art quantum communications and entanglement technologies).

AIT system 1

system overview

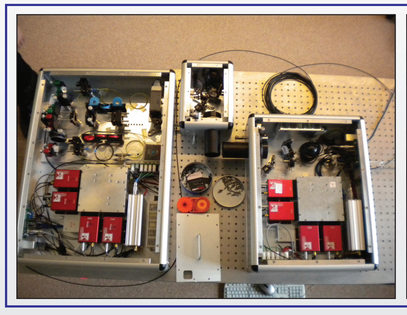


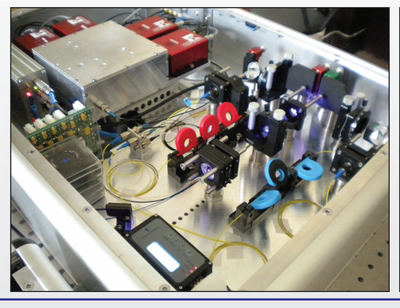


BBO crystal for entagelment generation

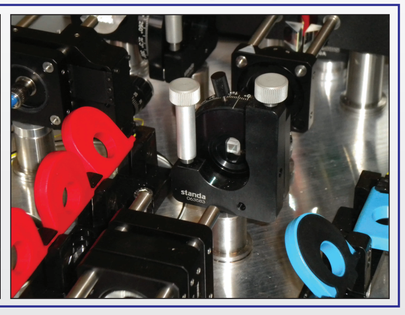
AIT system 2

system overview





BBO crystal for entagelment generation



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 (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 secure one-time pad encryption (given the exchanged random keys are at least of the bit length of the transmitted information), the parties can (provided they share appropriately pure EPR pairs, what can be determined statistically by a Bell/CHSH test and corrected in the presence of a channel noise by entanglement purification schemes) unconditionally securely transmit classical information in a way which is fundamentally proof to eavesdropping.
- A superdense coding scheme alike convention of encoding classical information on the states of Bell basis and possible local operations that transfer one Bell state into another (2.), are used and are sufficient for this secure communication protocol, involving subsequent transmitting of shared EPR pairs' components from one communication side to the other (3.), followed by proceeding measurements in the entanglement Bell basis by the receiving party combined with classical information decoding based on the aforementioned convention (5.).
- An eavesdropper potentially acquiring transmitted components of the entangled qubit pairs is unable to intercept any part of the transmitted classical information, because its decoding requires measurement of the whole EPR pair (4.).

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
- Instead directly providing security of classical communication by encoding it (indirectly by local operations) on non-local EPR pairs component qubits transmitted in quantum channels

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 E91 QKD protocol by A. Ekert is developed and the extensions are proposed involving local operations and classical communication (LOCC). The quantum information von Neuman entropy based analysis of security in presence of noise is provided which is performed within the Schmidt representation framework accounting the fundamental entanglement property, that its level cannot be increased by local operations.

Summary and conclusions:

- Unconditional security of classical communication by quantum channel is feasible in the protocol basing 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 perturbation 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. Acín, N. Gisin, L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. 97, 120405 (2006).
- Asymptotical unconditional security and integrity of the communication within the protocol can be achieved in case of noise presence in a quantum channel, which in principle is 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 unconditionally secure QKD protocols (most general security proofs should be based on non-local entanglement properties, Bell inequality violation and impossibility of superluminal signaling in contrast to possibly incomplete quantum mechanics postulates – especially 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 describing successful 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.

Entanglement QSDC vs entanglement based QKD

- entanglement based non-local QSDC protocol approach is more general than entanglement based QKD, as in particular, it can be used as a mean to unconditionally securely exchange a private (and if 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)

Entanglement QSDC vs non-entanglement QKD

- QSDC 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

The National Center for Research and Developement

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