Quantum cryptography: quantum mechanics as foundation for theoretically unconditional security in communication

M. Jacak[2], T. Martynkien[2], J. Jacak[1], D. Melniczuk[1], W. Donderowicz[3], 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

Contact author: Witold A. Jacak (e-mail: witold.aleksander.jacak@pwr.wroc.pl)

Quantum cryptography is a novel paradigm within cryptology employing fundamental laws of quantum mechanics on the physical layer of communications. These laws are counterintuitive, but indeed more general than classical physics laws which turn out to be merely approximation, serving properly on macroscopic scales according to our classical expectations of systems behavior. Whenever systems approach dimensions of nanometers, quantum effects emerge, invalidating classical expectations towards systems evolution dynamics. This poses serious challenges to classical models of information processing (based on classical systems evolution and related mathematical frameworks) within further miniaturization, but on the other hand offers much more powerful information processing models based on quantum dynamics (which directly endanger popular public-key cryptography, due to qualitatively higher efficiency in regard to solving some difficult mathematical problems). Simultaneously, beyond quantum computers, novel concepts were also formulated within the scope of communication and particularly cryptography, which can offer theoretically absolute (i.e. unconditional) level of encryption security (either by solving the private key distribution problem for theoretically absolutely secure symmetrical private-key cryptographic systems, such as the One-Time Pad, which is referred to as Quantum Key Distribution or enabling non-local quantum secure deterministic communication utilizing a completely non-classical properties of entangled quantum states). In contrast to quantum computers, quantum cryptographic protocols have been successfully implemented, and are considered an important branch of applied Information Technology security.

Specifically the QKD protocols are already a maturing communication security technology employing quantum mechanics principles to solving cryptographic problem of symmetric private key distribution. The QKD protocols (that can be generally divided into two classes in regard to utilizing or not the quantum entanglement [1-4]) in conjunction with the One-Time Pad (OTP) classical symmetric cryptographic encryption scheme offer theoretically unconditional security [5] of confidential communication. However, the experimental and even commercially available industrial implementations are very susceptible to technical conditionings of the transmitting media (i.e., optical fiber infrastructure and associated alignment of the quantum optics) [6,7]. This is specifically addressed to the dark fiber infrastructure limitation of the metropolitan backbone networks in the form of interconnections of telecommunication optical lines, which are implemented by thermal weldings, posing an obstacle for QKD deployment in terms of quantum channel decoherence (on a metropolitan scale, within a connection between two locations separated by ca. 4-5 km distance, there are usually several infrastructural weldings connecting separate optical fibers). Research on QKD deployment in practical telecommunication network environments resulted in evaluation of boundary conditions for QKD feasibility versus quantum channel and transmission parameters and a successful resolution of channel quality problem by proper alignment of experimental setups for both the no-entanglement and entanglement based quantum cryptography, correspondingly encoding qubits on the interfering phase shifts of photons in Mach-Zehnder interferometers and on the entangled pairs of photon polarizations (with these 2 implementations being most optimal to corresponding types of QKD protocols).

In this paper a short introduction to quantum cryptography is presented, along with a detailed description of known protocols, their implementations and related novel research and development results (specifically considering recent research efforts resulting with state of the art non-entanglement and entanglement based quantum cryptography systems deployment in real optical fiber metropolitan backbone networks environments).

Keywords: Quantum cryptography, Quantum key distribution, QKD, Quantum secure direct communication, QSDC

1. Introduction

At the basis of quantum cryptography concept lies a specific property (connected to a special character of quantum measurement of *von Neumann* postulate in quantum mechanics) of quantum information. According to this property quantum information cannot be read (or measured) in a classical way without irreversible loss of its part, and this constitutes foundation for a theoretically absolute level of security offered by quantum cryptography. In other words security of quantum cryptography is based on fundamental laws of quantum mechanics theory, and related quantum information theory (generally understood as describing properties of information encoded on quantum states of nanoscopic physical systems), specifically along with the quantum measurement demolishing character and related *no-cloning* theorem of Żurek and Wootters [21].

The sole idea of quantum cryptography (acknowledged to Bennett and Brassard) have been directly inspired by work of Wiesner, and particularly his concept of *quantum money*, which illustrates well the general mechanisms behind theoretical absolute security of quantum cryptography. As insight into Wiesner's proposition might be considered a good introduction, helping to understand general concepts of quantum cryptography, and so we will briefly present it below.

1.2. Quantum money

Suppose we had possibility to physically mark each banknote with an unique quantum information sequence (e.g., some sequence of quantum bits analogous, so called qubits, which are defined as abstract representation of some physical, quantum mechanical two-level systems, exactly as classical bits are abstractly defined on some classical physics two-level systems). Let us also assume that these qubits reside in mutually non-orthogonal quantum states, i.e., they are characterized by non-orthogonal superpositions of the basis states (one should note according to quantum mechanics foundations, states of physical systems are described as elements of normalized linear spaces, called Hilbert spaces, and thus behave like vectors, undergoing superpositions which are linear combinations of basis vectors). The fraud would be impossible because quantum mechanics (*no-cloning* theorem) would prohibit exact copying of a marked banknote. If on a banknote there was a random sequence of qubits, in states spanned by some non-orthogonal basis $\{|\psi>, |\varphi>\}$ e.g.,

$$|\psi> = |0>, \quad |\varphi> = |+> = \frac{1}{\sqrt{2}}(|0> + |1>),$$

than this banknote would be unequivocally identified by quantum state of this sequence e.g.,

$$|\psi> \otimes |\varphi> \otimes |\varphi> \otimes |\varphi> \otimes |\psi> \otimes |\varphi> \otimes |\psi> \otimes ... \otimes |\varphi>.$$

However if the banknote had been copied in a fraud attempt, than in accordance to the *no-cloning* theorem, the above sequence of qubits would have been changed and the mark on an original banknote would have been partly distorted rendering it valueless. The proposition further refined by Wiesner, Bennett, Brassard and Breidbard, has passed unnoticed (obviously partly because of seemingly small practical importance). Another publication by Wiesner [24] also shared this fate, but in 1984 Bennett and Brassard had presented a simple protocol [1] (ready for straightforward implementation) that used non-orthogonal quantum states to code classical information in a purpose of cryptographic keys distribution implementation. This is how quantum cryptography was born, which as a matter of fact is more precisely a quantum key distribution scheme.

Few years later there emerged other, different approach to quantum cryptography. In 1991 Ekert proposed protocol [25] employing quantum entanglement for realization of a quantum key distribution concept. The non-classical correlations of the measurements of entangled quantum states, derived from postulates of quantum mechanics, and verified experimentally [26], are the reason of fundamental discrepancies (violation of Bell inequality [27]) with a classical way of perceiving reality (assumptions of realism, and locality as in an EPR programme [28-30]). Security of quantum cryptography based on quantum entanglement is also connected to properties of quantum measurement and it is not yet clear if there is some fundamental difference between the two types of protocols. As each measurement of mutually entangled pair of qubits, done in purpose of copying classical information encoded in it, causes projection on a state of measurement

basis and in effect destroys entanglement. Both legitimate sides of communication sending between themselves entangled pairs of qubits may then in principle detect any potential eavesdropping – by checking that their respective pairs of qubits are no longer fully entangled (measurement statistics not violating Bell inequality).

2. Quantum Key Distribution

The Quantum Key Distribution (which is generally referred to as a quantum cryptography) protocols are designed to protect transmitted bits of a key (classical information bits, encoded on a basis of non-orthogonal qubits) from potential eavesdropping – which is understood as a sequence of measurements of those qubits done in order to reveal coded bits of a key. In a domain of classical information, channels of information transmission, realized on carriers of classical information (e.g., macroscopic not quantum values of electrical voltage or electromagnetic waves, behaving according to classical physics laws) can be eavesdropped without any disturbance. In a classical case eavesdropping is a completely reversible measurement, however difficult it would be to perform – it is always possible in principle – so there are no private channels in theory of classical information coding. If one defines concept of quantum channel, in analogy to classical channel in a domain of quantum information, i.e., information being transmitted in this channel by means of quantum carriers existing in mutually non-orthogonal states (e.g., mutually non-orthogonal polarizations – vertical-horizontal and two diagonal – of individual photons), than eavesdropping looses its classical property – it is not reversible anymore (as quantum measurement is not and introduces some disturbance to measured states, by projecting those to states mutually orthogonal). Therefore eavesdropping in quantum transmission may be easily detected: it is enough for both sides of secret communication to contact classically (by means of some classical public channel, eg. telephone, internet, etc.) and avoid revealing exact quantum states of previously transmitted qubits, detecting potential attempt of eavesdropping by comparing orthogonality of respective qubits in a sequence. The detection of eavesdropping results in canceling of actual session of QKD, which is what the security of quantum cryptography is based on.

2.1. Quantum key distribution without entanglement

The first proposition of quantum cryptography is due to Bennett and Brassard, who in 1984 presented a paper [1], supported by an experiment describing protocol of quantum key distribution later named BB84. This protocol is based on non-orthogonal states of photons polarization and its general schema is presented in fig.1. The situation is following: Alice and Bob want to exchange in a secure way a symmetrical private key, which they could later use in a symmetric cryptosystem of secret communication. Eve (who is a figure representing an eavesdropper) wants to eavesdrop on a transmission of this key, trying to compromise its privacy in order to be able to intercept forthcoming secret communication.

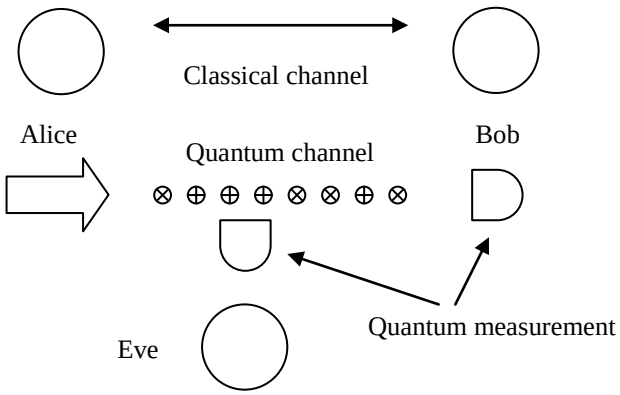


Fig.1. Quantum key distribution without entanglement (protocols BB84 and B92). Alice sends a symmetrical key (encoding bit of classical information on non-orthogonal qubits of quantum information – e.g., vertical-horizontal and diagonal photons polarizations) to Bob. Eventual eavesdropping could be detected by means of public communication by a classical public channel.

In order to ensure security of a key exchange, Alice and Bob decide to use quantum channel [31-33], encoding key's classical bits on qubits of quantum information sent by this channel. In order to do this Alice uses source of qubits in states spanned by basis $\{|0>,|1>\}$ and qubits in states spanned by a maximally non-orthogonal basis (in relation to the first one) $\{|+>,|->\}$. The states of this basis are:

$$|+>=\frac{1}{\sqrt{2}}(|0>+|1>) \quad |->=\frac{1}{\sqrt{2}}(|0>-|1>)$$

and in a Euclidean space these are vectors crossing with 45° angle with vectors representing states $|0>$ and $|1>$ on a planar. In BB84 protocol (and in it's derivatives) those qubits are mutually orthogonal polarizations of photons (horizontal and vertical – labeled as states $|0>$ and $|1>$) and maximally non-orthogonal in relation to those latter (but also mutually orthogonal) two diagonal polarizations of photons (labeled as states $|+>$ i $|->$). Each polarization is measured in relation to some fixed reference system (eg. the measuring device). Achieving such polarizations is reduced to sending laser beam through a Pockels cell (which is performing a quantum measurement of photon polarization: either in an orthogonal basis of horizontal-vertical directions of polarization $\{|0>,|1>\}$, labeled on fig.1. as $\oplus$, or in an orthogonal basis of diagonal directions of polarization $\{|+>,|->\}$, labeled as $\otimes$). Measurement in diagonal basis of polarization is achieved by a rotation of measuring device (Pockels cell) by 45° in an axis of laser beam. In that way Alice can randomly choose polarization of sequent laser pulses (sequent photons, while holding assumption that each laser pulse contains one photon) sent to Bob. Alice and Bob agree on some convention of encoding classical information bits on quantum information qubits, eg. bits 0 and 1 are encoded by $|0>$, $|1>$ qubits respectively and $|+>$, $|->$ qubits respectively, i.e.,

$$|0>\leftrightarrow 0,\ |1>\leftrightarrow 1,\ |+>\leftrightarrow 0,\ |->\leftrightarrow 1.$$

Alice stores produced sequence of bits for created states of qubits, which she is sequentially sending to Bob. Those qubits (photons, or rather their polarizations) are making a quantum channel (by moving in air, optical fibers or in void). Each sent qubit is always in state from either orthogonal basis $\{|0>,|1>\}$ ($\oplus$), or orthogonal basis $\{|+>,|->\}$ ($\otimes$), which is maximally non-orthogonal basis in relation to the first one. Bob performs measurements of received qubits in basis $\{|0>,|1>\}$ ($\oplus$) or $\{|+>,|->\}$ ($\otimes$), while he choose those bases in a random manner (i.e. he has no information on which measurement basis Alice chose for the specific received qubit). If Bob scores a correct choice of measurement basis (he luckily chooses the same basis as Alice for some specific qubit) than in accordance with *von Neumann* projection postulate he receives information on completely not disturbed quantum state of a qubit – the same information Alice has (in this case on the position of this qubit in a bit sequence of key stored by Alice and Bob, values of this bit will be equal). However if Bob doesn't score a correct choice of basis (he chooses second basis, maximally non-orthogonal to the first one), than according to *von Neumann* postulate, in a result of quantum measurement, he receives with an equal probability (50%) one of states of the chosen basis (in this case on the position of this qubit in a bit sequence of key values of this bit will be different with 50% probability). The next phase of the protocol is communication by a classical public channel: Alice and Bob exchange information on their sequence of measurement basis choices for each qubit defining position of a bit in transmitted key (which in this phase is called a raw key). All bits of the raw key on positions corresponding to qubits for which they chose different measurement basis are discarded – in a process called sifting. Then Alice and Bob receive averagely shorter by half a sifted key. The sole process of creation of a sifted key however introduces into it a strong random factor, due to lack of correlation between Alice's and Bob's measurement basis choice – this is the reason why quantum key distribution systems are not suited for secure transmission of secret messages instead of keys.

Theoretical scheme described above is just an idealized model. In a practical implementation due to imperfections of sources (weak laser pulses sometimes contain none photons at all) and detectors, Bob does not always register a photon in a pulse. If Bob doesn't register any photon in a pulse from Alice, they communicate over classical public channel and discard this qubit in a transmitted bit sequence of a key (this requires time synchronization in sending sequent qubits) – finally distributing a sifted key with length being a fraction of number of all laser pulses sent. Let us emphasis again that security of QKD from the attempt of eavesdropping is based upon disturbance of quantum information which is introduced by a quantum measurement on transmitted qubit. In principle if Eve doesn't have a way to predict random sequence of choices of measurement basis by Alice, the eavesdropping can be detected with arbitrarily high probability. Suppose a situation in which Eve intercepts a quantum channel and does quantum measurements upon it,

resending measured qubits further to Bob. Similarly to Bob, Eve doesn't know the basis of a state of qubit to be measured. Therefore all possibilities of basis choice sequence are completely equivalent to measuring qubits in bases chosen randomly (in sense of no correlation with their actual bases). Again similarly to Bob, Eve by doing measurements in case of not correctly chosen basis, will receive purely random result of quantum state of a specific qubit, projecting it to one of orthogonal states of the measurement basis. If Bob than chooses correct measurement basis on this qubit (the same as Alice originally chose) – the qubit doesn't have to be in the same state as Alice measured it, because it was previously altered to other measurement basis by Eve – thus having non-orthogonal state to Bob's measurement basis. This illustrates that Eve trying to eavesdrop does introduce some errors to the sifted key (which is made from the raw key buy discarding bits with positions corresponding to qubits for which Alice's and Bob's measurement bases were different). Because statistically Eve doesn't score a correct choice of a basis in 50% of cases (just as Bob), then idealistically assuming that she measures each sent qubit, Alice and Bob have 25% of errors in a sifted key. In a basic schema of QKD Bob and Alice sacrifice randomly chosen bits of a sifted key and publicly compare their values (by means of classical communication). If they discover errors than they know about potential eavesdropping and can discard a key in this compromised session.

2.2. Quantum key distribution with entanglement

Before one can discuss entanglement based quantum key distribution it is important to explain Bell inequalities violation and the EPR program.

2.2.1. Realism, locality and EPR program

According to the classical intuition, confirmed well in the macroscopic world, all objects have properties existing independently of the measurement carried out on them. This assumption, classically well confirmed empirically, is referred to as realism, and in other words assures existence of objective reality. According to this view, the role of the measurement is therefore only to discover (through observation) of the physical property value – and these values must be fixed regardless of the number of measurements performed (i.e. measurements are repeatable). In quantum mechanics, however, in a fundamental way the measurement is a non-repeatable procedure – and in the light of the assumptions of realism it is a destructive, invasive procedure, which gives a result only in a probabilistic manner presumption about values of the specific properties (observables) of an object, causing the so-called collapse of the state at the same time.

Shortly after the above quantum mechanics predications became clear, there emerged an interpretation of quantum mechanics, according to which objects (systems) have no specific quantum property – the value of these properties appear only as a result of the measurement (i.e. entanglement with the classical quantum system, which exponentially increase in the number of degrees of freedom). Such controversial views were met with strong opposition in scientific community of the early XX century. Especially important here was the authority of Albert Einstein, who did not accept the existence of such non-intuitive laws of nature, who together with Boris Podolsky and Nathan Rosen proposed a programme [28] (called EPR from the initials of the authors) that defines the physical correctness of the theory by introducing the notions of the so-called elements of reality (associated with realism), locality and completeness. According to the program, each of the elements of a complete physical theory would have a corresponding fragment. The argument aimed to demonstrate the incompleteness of quantum mechanics by suggesting that a specific element of reality (which according to the authors could be defined as any physical property whose value can be determined before the measurement) does not have a corresponding fragment of the theory. The thought experiment (shown here in a modified form by David Bohm [30]) on the so-called EPR singlet entangled spin state of the two electrons, or alternatively entangled polarization state of 2 photons of the so called Bell basis:

$$|\eta> = \frac{|10> - |01>}{\sqrt{2}},$$

The 100% anti-correlations of the measurements of the above states of specific qubits (outcome of the measurement of the 1st part of the system against the 2nd, always demonstrate opposite outcomes) appear to violate classical expectations about causality (principle that some 2 systems separated casually, i.e. on a distance such that the time between the events, e.g. measurements on those systems, is shorter than the time required for light moving with highest possible velocity to cover this distance, cannot be in any way related

or casually connected (in principle, cannot be correlated). Measuring the state of the qubit based on the first calculation, depending on the result determines the result of the measurement is always opposite the second qubit, which occurs here with a strict anti-correlation, which is not affected by factors such as spatial separation of the physical systems serving for definition of both qubits (the mentioned electrons or photons). This brings us to another foundational assumption which works well in the classical world: locality (consisting in the fact that the systems casually separated in space and time cannot influence each another, leading to any measureable correlations), which in the case discussed above of the EPR thought experiment (under assumption of realism) is clearly broken. In accordance with the postulated criterion of belonging to the set of elements of reality, the 100% anti-correlation resulting from the maximally entangled state measurement, leads to existence of some new physical properties: manifesting themself in being able to determine or confidently predict the measurement of the second qubit, which is simply an element of reality, not having, in quantum mechanics, theoretical explanation under assumption of local realism. Under assumption of the local realism, theory of the physical laws of quantum mechanics in view of the EPR paradox and non-local anti-correlations seem to be incomplete on the fundamental level. This incompleteness has been referred to as the so-called hidden variables, existence of which could explain how 1st part of the system (1st qubit) could immediately after its probabilistic measurement influence the 2nd part of the system (2nd qubit) spatially separated, so that a measurement performed on the 2nd qubit will deterministically anti-correlate with the outcome of the measurement of the 1st qubit (this might be equivalent to the qubits somehow communicating in no-time due to their entanglement). Recently (in the late 80s of the XX century), the hidden variables theories in view of experimental implementations of the considerations described below, have been proven to have a non-local character, which results with the property of quantum mechanics violating either locality or realism assumptions.

2.2.2. Violation of Bell inequalities (quantitative proof of the local realism absence in quantum information)

What verifies the correctness of the assumptions is ultimately an experiment. More than 30 years after appearance of views contained in the EPR program, in the 60's John Bell proposed a simple method of analysis (based on the inequality of the statistical nature) of the similar thought experiment of which an actual physically empirical verification would be possible. In this experiment, there are performed series of measurements of two previously prepared reproducibly particles, assuming locality of physical laws in a way assuring causal separation (i.e. so as to exclude the possibility of a causal link, according to the theory of relativity, for example, by making measurements in a small time difference with sufficient spatial separation - at a constant and maximal velocity of light in vacuum, which is also the maximum speed of propagation of local physical interactions). With the assumption of realism, each particle having (to simplify the example) just two physical properties: A and B for the first particles, and C and D for the second particle, which measured only unveil specific values existing before (these values are uncovered by the measurement). As a result of the measurement of each of these properties is therefore obtained a corresponding value a and b respectively for the first particle and c and d for the second. Again, to simplify the analysis, let the values of these physical properties be determined only on the two elements set $\{-1, 1\}$, which would corresponded to the physical situation of photon polarization or electron spin measurements along chosen reference frame axes. Let us notice that the value of a specially constructed nonlinear combination would be the following:

$$ac + bc + bd - ad = c(a+b) + d(b-a) = \pm 2 .$$

Due to the possibility of noise causing inaccuracies in measurement outcomes, or the possibility of inaccuracies in the preparation of particles, let us assume that the physical properties A, B, C, D of both particles were before the measurement correspondingly equal to $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$ with probability $p(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$. Now let us consider statistical expected value of the quantity $AC + BC + BD - AD$, i.e. is a common physical property of both particles (not a linear combination):

$$E(AC + BC + BD - AD) = \sum_{\tilde{a},\tilde{b},\tilde{c},\tilde{d}} p(\tilde{a},\tilde{b},\tilde{c},\tilde{d})(\tilde{a}\tilde{c} + \tilde{b}\tilde{c} + \tilde{b}\tilde{d} + \tilde{a}\tilde{d}) \leq \sum_{\tilde{a},\tilde{b},\tilde{c},\tilde{d}} 2\, p(\tilde{a},\tilde{b},\tilde{c},\tilde{d}) = 2 .$$

Due to linearity of the expected value definition, we thus obtain:

$$E(AC) + E(BC) + E(BD) - E(AD) \leq 2 .$$

This result is known as one of Bell's inequality (a collection of statistical inequalities obtained under similar to the above analysis). More specifically, this inequality was derived in a similar manner to the original output of Bell's inequality by Clauser, Horn, Shimony and Holt and called the CHSH inequality [34] (the

initials of the authors). This inequality is possible for simple experimental verification - experimental runs as a series of measurements (for each of the separated causally particles, measurements would consider one of the two of each particle physical properties, selected every time in a random manner, thus statistically producing measurements results of each of the 4 pairs of two particles properties at rate of approximately 25%). After the experiment, it is possible to verify the result of Bell's inequality by calculating the expected value (i.e. an average value) of the measurement sample for each pair of values of the physical properties of both particles. In a classical case, when there is no entanglement between the particles, this result is consistent with the relevant statistical expectations shown above. But what happens when the measured physical properties of the particles are indeed entangled? Consider an example of two entangled photons in the below state (one of the so-called Bell states, and the original EPR singlet state analyzed above in discussion of local-realism violating anti-correlations):

$$|\eta>=\frac{|10>-|01>}{\sqrt{2}},$$

this time not implemented on spins of electrons, but rather vectors corresponding to polarizations of the photon along selected reference frame axes (related to conditions of actual physical experiment feasibility). To carry out the experiment, the photon source is required to provide in a reproducible manner, photon pairs in maximally entangled Bell states (this is implemented by non-linear crystals within the so called parametric down conversion process [42]), which (the photons) are then spatially separated. Assume that the measured physical properties of the two photons is their polarization vectors in the axis directions set by the versors $\hat{z},\hat{x}$ for this first photon and $-\frac{\hat{z}+\hat{x}}{\sqrt{2}},\frac{\hat{z}-\hat{x}}{\sqrt{2}}$ for the second, which determines the observables (physical properties or quantities) for the first photon to be $A=\sigma_z$, $B=\sigma_x$ and for the second: $C=-\frac{\sigma_z+\sigma_x}{\sqrt{2}}$, $D=\frac{\sigma_z-\sigma_x}{\sqrt{2}}$, where $\sigma_x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, $\sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ are the Pauli matrices. According to the von Neumann postulate we have decomposition of obserabes into projection operators on the computational basis of qubits:

$$\sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0><0|-|1><1|,$$

$$\sigma_x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\xrightarrow{diagonalizacja}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0><0|-|1><1|,$$

$$-\frac{\sigma_z+\sigma_x}{\sqrt{2}}=-\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\xrightarrow{diagonalizacja}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0><0|-|1><1|,$$

$$\frac{\sigma_z-\sigma_x}{\sqrt{2}}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ -1 & -1\end{bmatrix}\xrightarrow{diagonalizacja}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0><0|-|1><1|,$$

with the eigenvalues ± 1 representing value outcomes of those 4 physical quantities (observables) measurements.

Now calculating expected values of the observables according to the quantum mechanics definition: $E(A)=<A>=<\psi|A|\psi>$ for common physical properties of both particles – pairs of observables of photon polarization vectors (in their entangled state $|\psi>=|\eta>=\frac{1}{\sqrt{2}}(|10>-|01>)$) we will obtain specific numerical values:

$$E(AC),\ E(BC),\ E(BD),\ E(AD),$$

which should fulfill Bell inequality:

$$E(AC)+E(BC)+E(BD)-E(AD)\le 2.$$

Thus we have an expected value for *AC* observable:

$$E(AC)=E\left(-\frac{\sigma_z\otimes\sigma_z+\sigma_z\otimes\sigma_x}{\sqrt{2}}\right)=\left\langle-\frac{\sigma_z\otimes\sigma_z+\sigma_z\otimes\sigma_x}{\sqrt{2}}\right\rangle=$$

$$=-\frac{1}{\sqrt{2}}(<\sigma_z\otimes\sigma_z>+<\sigma_z\otimes\sigma_x>)=-\frac{1}{\sqrt{2}}(<\eta|\sigma_z\otimes\sigma_z|\eta>+<\eta|\sigma_z\otimes\sigma_x|\eta>)=$$

$$=-\frac{1}{\sqrt{2}}(<\eta|00><00|\eta>-<\eta|01><01|\eta>-<\eta|10><10|\eta>+<\eta|11><11|\eta>+$$

$$+<\eta|01><00|\eta>+<\eta|00><01|\eta>-<\eta|11><10|\eta>-<\eta|10><11|\eta>)=$$

$$=-\frac{1}{\sqrt{2}}(-\frac{1}{2}-\frac{1}{2})=\frac{1}{\sqrt{2}},$$

for *BC* observable:

$$E(BC)=E\left(-\frac{\sigma_x\otimes\sigma_z+\sigma_x\otimes\sigma_x}{\sqrt{2}}\right)=\left\langle-\frac{\sigma_x\otimes\sigma_z+\sigma_x\otimes\sigma_x}{\sqrt{2}}\right\rangle=$$
$$=-\frac{1}{\sqrt{2}}(<\sigma_x\otimes\sigma_z>+<\sigma_x\otimes\sigma_x>)=-\frac{1}{\sqrt{2}}(<\eta|\sigma_x\otimes\sigma_z|\eta>+<\eta|\sigma_x\otimes\sigma_x|\eta>)=$$
$$=-\frac{1}{\sqrt{2}}(<\eta|10><00|\eta>-<\eta|11><01|\eta>+<\eta|00><10|\eta>-<\eta|01><11|\eta>+$$
$$+<\eta|11><00|\eta>+<\eta|10><01|\eta>+<\eta|01><10|\eta>+<\eta|00><11|\eta>)=$$
$$=-\frac{1}{\sqrt{2}}(-\frac{1}{2}-\frac{1}{2})=\frac{1}{\sqrt{2}},$$

for *BD* observable:

$$E(BD)=E\left(\frac{\sigma_x\otimes\sigma_z-\sigma_x\otimes\sigma_x}{\sqrt{2}}\right)=\left\langle\frac{\sigma_x\otimes\sigma_z-\sigma_x\otimes\sigma_x}{\sqrt{2}}\right\rangle=$$
$$=\frac{1}{\sqrt{2}}(<\sigma_x\otimes\sigma_z>-<\sigma_x\otimes\sigma_x>)=\frac{1}{\sqrt{2}}(<\eta|\sigma_x\otimes\sigma_z|\eta>-<\eta|\sigma_x\otimes\sigma_x|\eta>)=$$
$$=\frac{1}{\sqrt{2}}(<\eta|10><00|\eta>-<\eta|11><01|\eta>+<\eta|00><10|\eta>-<\eta|01><11|\eta>+$$
$$-<\eta|11><00|\eta>-<\eta|10><01|\eta>-<\eta|01><10|\eta>-<\eta|00><11|\eta>)=$$
$$=\frac{1}{\sqrt{2}}(\frac{1}{2}+\frac{1}{2})=\frac{1}{\sqrt{2}},$$

and finally for *AD* observable:

$$E(AD)=E\left(\frac{\sigma_z\otimes\sigma_z-\sigma_z\otimes\sigma_x}{\sqrt{2}}\right)=\left\langle\frac{\sigma_z\otimes\sigma_z-\sigma_z\otimes\sigma_x}{\sqrt{2}}\right\rangle=$$
$$=\frac{1}{\sqrt{2}}(<\sigma_z\otimes\sigma_z>-<\sigma_z\otimes\sigma_x>)=\frac{1}{\sqrt{2}}(<\eta|\sigma_z\otimes\sigma_z|\eta>-<\eta|\sigma_z\otimes\sigma_x|\eta>)=$$
$$=\frac{1}{\sqrt{2}}(<\eta|00><00|\eta>-<\eta|01><01|\eta>-<\eta|10><10|\eta>+<\eta|11><11|\eta>+$$
$$-<\eta|01><00|\eta>-<\eta|00><01|\eta>+<\eta|11><10|\eta>+<\eta|10><11|\eta>)=$$
$$=\frac{1}{\sqrt{2}}(-\frac{1}{2}-\frac{1}{2})=-\frac{1}{\sqrt{2}}.$$

It follow that the value of the considered quantity:

$$E(AC)+E(BC)+E(BD)-E(AD)=\frac{4}{\sqrt{2}}=2\sqrt{2}>2$$

violates Bell (or more precisely CHSH) inequality. The postulates of quantum mechanics measurement result so with contradiction – i.e. violation of Bell's inequality, the introduction of which bases on local realism. Since the actual crucial experiments were carried out proving the above contradiction and the results confirmed the predictions of quantum mechanical rather than classical viewpoint – therefore on a fundamental level, one of the assumptions (locality or realism), or both at the same time are incorrect. This fact directly related to the strange properties of entangled states in quantum mechanics, lies at the root of what advantages quantum computing and quantum models of communication channels over their conventional counterparts can offer, also quite directly to quantum cryptography field.

2.2.3. Ekert protocol (E91)

The second proposition of QKD procedure is due to Ekert [3], who in 1991 introduced a novel protocol later named E91. Its conception for encoding classical information is usage of a pair of qubits in entangled states. If two qubits are in maximally entangled state, one of four possible Bell states, e.g., a singlet state:

$$|\eta>=\frac{|10>-|01>}{\sqrt{2}},$$

than there is no classical information about states of specific qubits (their states are maximally mixed). The proposition of entangled QKD was partly based on previous ideas of experimental validation [22] of Bell inequalities (specifically of CHSH inequality [34]). Pairs of entangled qubits in Ekert's protocol are separated in space (sent between sides of secret communicationb: Alice and Bob), and their measurements might be used to send information, with simultaneous usage of classical public channel (in an analogy to schema of quantum teleportation [35,57]).

In E91 protocol and in most of its derivatives, those pairs of entangled qubits are pairs of photons with entangled polarization states. A brief schema of QKD with entanglement is shown in fig.2. The basic element of set up of such protocol is a quantum source,

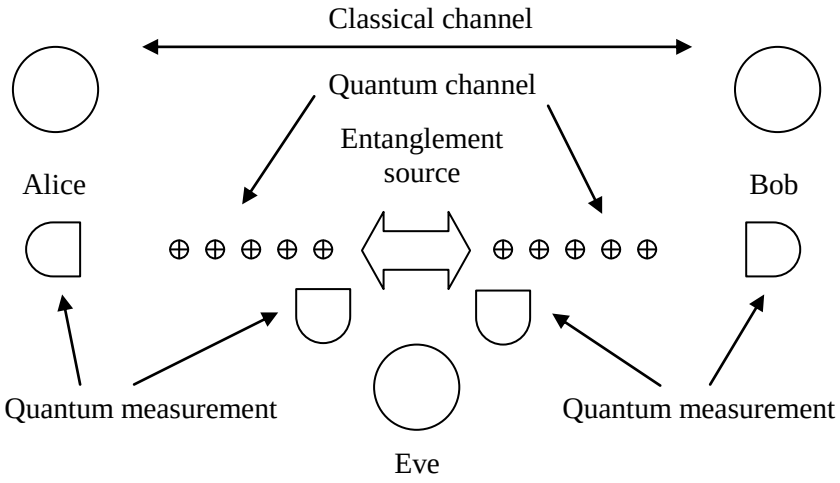


Fig.2. Quantum key distribution with entanglement (E91 protocol). Pairs of maximally entangled qubits (these can be photons with maximally entangled polarization states, e.g., singlet states) are generated by quantum entanglement source and separated in space between Alice and Bob by means of quantum channels. The source may be positioned at Alice's side, at Bob's side or anywhere else. Eventual Eve's eavesdropping (who may be doing quantum measurements on an arbitrary quantum channel, and in a worst case be controlling entangled photons source) is detected by analysis of correlation statistics of measurements results (by means of public classical communication) in view of Bell inequality – if it is not violated, than there was a potential eavesdropping (which might be as well due to decoherence in quantum channel).

producing spatially separated pairs of photons (so it is possible to send them in two separate quantum channels) in maximally entangled states of their polarization.

Alice and Bob are receiving sequent pairs of entangled photons, sent in a singlet state spanned by orthogonal basis $\{|0>,|1>\}$ of vertical-horizontal polarization (in fig.2. labeled as $\oplus$):

$$|\eta> = \frac{|10> - |01>}{\sqrt{2}},$$

in relation to some fixed reference system – e.g., the source device. The source might be positioned in an arbitrary place – at the location of Alice, Bob or anywhere else (eg. at site of an institution commercially providing entangled states) – only important issue is existence of quantum channels between source and Alice, source and Bob and that they knew a reference system of entangled photons polarization. After receiving each sequent photon from an entangled pair, Alice and Bob perform quantum measurement in one of three basis (on the scheme from fig.2. for simplification we presented measurement in one of just two bases), which is chosen in a random fashion. In the original E91 protocol, those three different measurement bases are being obtained by rotation of a measuring device (which is measuring horizontal-vertical polarization, ie. in an orthogonal basis $\{|0>,|1>\} - \oplus$) in relation to a fixed reference system (eg. geometry of construction of a source device) in an axis of a photons beam. Angles of those rotations (creating three mutually non-orthogonal measurement bases, which we will label the same as angles), are for Alice: $\alpha_1 = 0, \alpha_2 = \frac{\pi}{4}, \alpha_3 = \frac{\pi}{8}$, and for Bob: $\beta_1 = 0, \beta_2 = -\frac{\pi}{8}, \beta_3 = \frac{\pi}{8}$. In accordance with *von Neumann* postulate, quantum measurement realized in those basis will result in a projection of quantum states of individual photons on two states of a measurement basis, returning corresponding eigenvalues: ± 1. For the measurement in first bases Alice and Bob will know, that measured eigenvalue in fact corresponds to the polarization state of received photon from the entangled pair, however in two other cases their measurement will result only in probabilistic projection. One can introduce expected values of observables $\alpha_i \otimes \beta_j$ (which are coefficients of correlation measure of observables α_i, β_j corresponding to measurement bases). We have $E(\alpha_i \otimes \beta_j) = <\psi | \alpha_i \otimes \beta_j | \psi>$, where $|\psi> = |\eta> = \frac{|10> - |01>}{\sqrt{2}}$, therefore:

$$E(\alpha_i \otimes \beta_j) = \frac{1}{2}(<10|\alpha_i \otimes \beta_j|10> - <01|\alpha_i \otimes \beta_j|01>) = -\cos 2(\alpha_i - \beta_j)\cdot$$

Let us emphasize that in a case of the same choice of bases by Alice and Bob (ie. observables pairs α_1, β_1 and α_3, β_3) they will obtain a 100% anticorrelation of their results, ie: $E(\alpha_1 \otimes \beta_1) = E(\alpha_3 \otimes \beta_3) = -1$.

Lets consider expected value of observable: $\alpha_1 \otimes \beta_3 + \alpha_1 \otimes \beta_2 + \alpha_2 \otimes \beta_3 - \alpha_2 \otimes \beta_2$. From linearity and simple calculations we have:

$$E(\alpha_1 \otimes \beta_3 + \alpha_1 \otimes \beta_2 + \alpha_2 \otimes \beta_3 - \alpha_2 \otimes \beta_2) =$$
$$= E(\alpha_1 \otimes \beta_3) + E(\alpha_1 \otimes \beta_2) + E(\alpha_2 \otimes \beta_3) - E(\alpha_2 \otimes \beta_2) =$$
$$= <\psi | \alpha_1 \otimes \beta_3 | \psi> + <\psi | \alpha_1 \otimes \beta_2 | \psi> + <\psi | \alpha_2 \otimes \beta_3 | \psi> - <\psi | \alpha_2 \otimes \beta_2 | \psi> = -2\sqrt{2}.$$

Of course this is the case only if states measured by Alice and Bob were in fact maximally entangled singlet states, i.e., $|\psi> = |\eta>$. If however, Eve eavesdropped on the quantum channel (or the channel was not perfect itself – inside occurred decoherence of polarization states of entangled photon pairs – what is assumed by Alice and Bob to be a potential eavesdropping attempt) than measured by them states of entangled photon pairs were not singlet states: $|\psi> \neq |\eta>$. Their entanglement was weaker and therefore expected value of $\alpha_1 \otimes \beta_3 + \alpha_1 \otimes \beta_2 + \alpha_2 \otimes \beta_3 - \alpha_2 \otimes \beta_2$ observable was:

$$E(\alpha_1 \otimes \beta_3) + E(\alpha_1 \otimes \beta_2) + E(\alpha_2 \otimes \beta_3) - E(\alpha_2 \otimes \beta_2) < -2\sqrt{2}.$$

This fact allows Alice and Bob to detect potential eavesdropping. They do it in a following way: after finishing receiving and measuring entangled pairs they disclose by means of public classical communication their sequences of bases choices (ie. angles by which they rotated their set-ups), discarding all cases where one of them did not register any photon at all (imperfections of sources and detectors), and publicly exchange all measurement results done in not the same bases. Then they are able to estimate expected value of observable considered above:

$$E(\alpha_1 \otimes \beta_3) + E(\alpha_1 \otimes \beta_2) + E(\alpha_2 \otimes \beta_3) - E(\alpha_2 \otimes \beta_2).$$

If it is equal to $-2\sqrt{2}$, than they are sure that quantum channel has not been eavesdropped upon and that left (secret) measurement results done with the same bases are strictly anticorrelated – so they may be used to encode classical information (eg. in a convention: bit 0 is corresponding to qubit $|0>$ and bit 1 to qubit $|1>$ for Alice and conversely for Bob due to anticorrelation). In this fashion (the process is similar to sifting in BB84 protocol) Bob and Alice obtain a sifted key – in which information appeared in a random manner – based on correlation lack of measurement bases choice. If however estimated expected value does not comply with above equation (ie. Bell inequality, more precisely CSHS inequality is preserved) than Alice and Bob know about potential eavesdropper and they can discard the compromised key obtained in current session.

3. Hardware realizations of quantum key distribution

In realistic implementations of QKD protocols, much more sophisticated procedures are used, allowing to preserve perfect key security (ie. lowering probability of secret information leakage below arbitrarily small parameter) up to some critical degree of error rate in a sifted key. Among those procedures are estimation of errors number (which are potentially due to eavesdropping, or simply due to decoherence in an imperfect quantum channel), correction of those errors (either ordinary linear correction schemes or some more advanced techniques can be used, eg. interactive procedure proposed by Brassard and Salvail [37]), finally privacy amplification procedure taking into account maximal information about a key potentially available to Eve and allowing to reduce this information below arbitrarily small level by reducing length of a sifted key. In result of those procedures, which are referred to as a key reconciliation, Alice and Bob obtain a perfectly secure and errorless (parameterized by accordingly small variables of information leakage risk and errors rate) private key, which can be further used in a classical symmetric cryptosystems for secret communication.

Let us now focus on more detailed practical realizations of quantum key distribution protocols without entanglement. Those protocols are based on sending single qubits – practically these are usually photons, because of high development level of quantum optics technology. In protocols BB84 and its derivatives, states of transmitted qubits are polarizations from two mutually non-orthogonal bases (eg. $\{|0>,|1>\}$ i $\{|+>,|->\}$). The schema of BB84 is illustrated in fig.1 (where bases of polarization of sequent photons were respectively labeled by $\oplus$: $\{|0>,|1>\}$ and $\otimes$: $\{|+>,|->\}$). Hardware realization of original BB84 is illustrated in fig.3. Photons source at the side of Alice is a highly attenuated (marginal output power) laser, and a Pockels cell (two polarization filters connected by a piezoelectrical crystal, which allows to control birefringence with an applied voltage, and in consequence to choose a specific polarization in orthogonal basis, eg. horizontal polarization from a horizontal-vertical basis $\oplus$). The Pockels cell (or the whole source device) can be rotated by 45˚ angle (in one direction back and forth) in relation to some fixed reference system, eg. a starting position, allowing a choice of maximally non-orthogonal polarization basis of sent photons (in a 45˚ rotated configuration the source is emitting photons in a specific – one of two diagonal – polarization of basis $\otimes$). On Bob's side (and also on Eve's side if there is an eventual eavesdropping) the measuring system consists of a Pockels cell controlling polarization (horizontal-vertical in starting configuration in relation to agreed upon with Alice fixed reference system, eg. Alice's device, and two diagonal) by its rotation by 45˚ angle in an axis of laser beam in relation to mentioned reference system, of a polarizing beamsplitter (separating it on two beams of orthogonal polarizations), on which two output directions are photon detectors. Quantum channel between Bob and Alice might be any medium of electromagnetic wave – eg. an optical fiber, air or void).

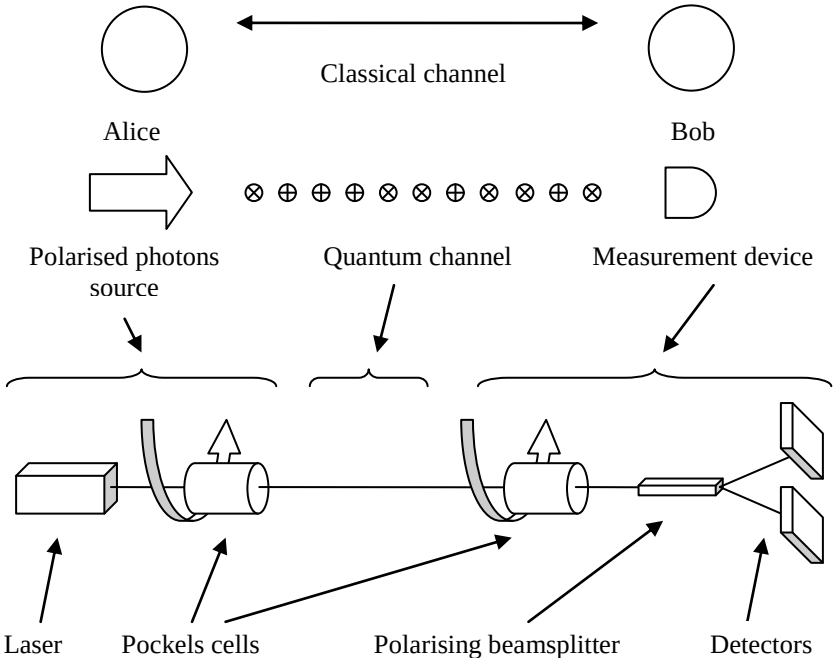


Fig.3. A schema of practical realization of QKD BB84 protocol (and its derivatives). The source of polarized photons at Alice's side consists of laser and Pockels cell rotated by 45˚ angle in an axis of laser beam. Quantum channel may be an arbitrary optical medium (eg. air, void or optical fiber). The measurement device (at Bob's but also on Eve's side) is also a rotated (in relation to a fixed reference system) Pockels cell, polarizing beamsplitter and two single-photon detectors.

The most convenient in commercial applications are obviously optical fibers, which already have highly developed network infrastructure. QKD protocols based on light polarization however do pose some implementation difficulties in case when the quantum channel is a standard telecommunication fiber. For such fibers fluctuations of birefringence connected to small anisotropy of material pose alongside with depolarization a main type of decoherence. This is why another possibilities of qubit carriers based on photons are investigated – here an interesting approach is application of photons phase shifts (shifts of phases of electromagnetic waves). In case of replacing polarization qubits with phase qubits, due to smaller time scales of dephasing than depolarization in optical fibres, perspectives of longer quantum channels implementation (of order of hundreds km) seem to be realistic. One protocol of QKD based upon coding

classical information on qubits defined as a difference of photons phases is B92 (proposed by Bennett [2] in 1992). The idea is however due to Ekert – the earlier proposition of QKD realization employing quantum entanglement [3], known as protocol E91.

In a modified protocol B92, source at Alice's side consists of a laser and Mach-Zehnder interferometer. This interferometer in turn consists of a polarizing beamsplitter (here polarization of photons does not play any role) connected to phase modulator (which allows control of bases and actual states of those bases for transmitted photons: eg. orthogonal basis $\{|0>,|1>\} - \oplus$, states of which correspond to photon phase shifts of 0 and π respectively, and maximally non-orthogonal to latter basis $\{|+>,|->\} - \otimes$, states of which correspond to photon phase shifts of $\frac{\pi}{2}$ and $\frac{3\pi}{2}$) on one beam, a large roll of fiber on other beam (resulting in time delay of photons in second beam needed to allow sending photons of both beams with only one quantum channel) and an obverse polarizing beamsplitter merging two beams into one. At Bob's side (and eventually at eavesdropping Eve's side) the measuring device consists of analogical but obverse interferometer (with phase modulator allowing measurement basis choice control in a same fashion as described above, and with the same roll of optical fiber on an opposite beam resulting in realignment of time delay of laser pulses). The interferometer is connected to polarizing beamsplitter, and on the end of two beams photon detectors are placed. In case of same basis choice (the same configuration of modulator by Bob and Alice) appropriate set up of devices will cause constructive interference in defined detector and destructive interference on the second one. On the other hand different basis choice will cause random *von Neumann* projection and a random interference constructive in one detector and destructive in the other. The propagation of laser light wave in this schema is following: pulse from laser is split on two pulses in Mach-Zehnder interferometer at Alice's side, which then propagate by a short and long path to quantum channel, where they are sequentially transmitted. Entering Bob's (or Eve's) interferometer they create three pulses – one which is transmitted twice by a short path, one which is transmitted once by a short path and once by a long path and one which is transmitted twice by a long path – the middle one (opposite to the first and latter, which are discarded) causes intereference due to its indistinguishability. Phase modulators give possibility to encode and decode classical information in a manner described earlier (also in analogy to photons polarization based protocols). Because of a lack of necessity to preserve coherence of polarization in B92 protocols family, optical fibers are in this case a better quantum channel than for BB84 protocols family.

In turn issues of hardware realizations of quantum key distribution systems with entanglement in a similar systems are currently left only on experimental planar. Due to necessity of quantum information processing on a level of not trivial realizations of quantum computers to perform algorithms of quantum privacy amplification (indispensable for preservation of key privacy in conditions of realistic decoherence or a potential eavesdropping), those technologies currently have small perspective for a practical use.

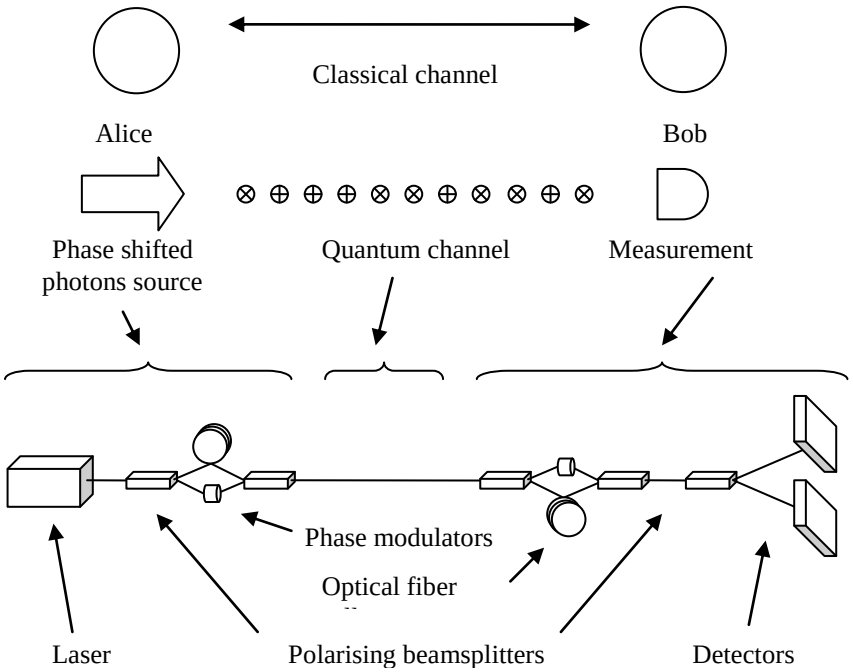


Fig.4. A schema of a practical realization of modified protocol B92 (and its derivatives) of QKD. The source of phase shifted photons at Alice's side consists of laser and Mach-Zehnder interferometer (which in turn consists of polarizing beamsplitter, phase modulator on one beam and optical fiber roll on another beam and of obverse polarizing beamsplitter merging two beams into one. At Bob's side (and eventually at Eve's side) the measuring device consists of analogical but obverse Mach-Zehnder interferometer (with phase modulator allowing measurement basis choice and the same length of optical fiber roll on an opposite beam). The interferometer is connected to polarizing beamsplitter and two single-photon detectors. Due to lack of necessity of coherent polarization preservation optical fibers make in this case a better quantum channel than for polarization based protocols.

An important practical problem for hardware realization of QKD based on existing telecommunication network of optical fibers (abstracting from dephasing type of decoherence) is a signal strength loss (of laser pulses) in long fibers. Because of current lack of possibilities of coherent amplification of optical signal, there exist (in connection to necessity of weak laser pulses) a practical barrier in lengths of optical fibers for QKD application. Transmission losses for silicon optical fibers are of order 10^{-1} dB/km – what causes that quantum cryptography applications realized on optical fibers with lengths of order 1000 km (signal loss ~ 10^2 dB which is equivalent to transmission of order 10^{-3} of signal strength) are currently beyond current technology, even just because of this reason. Therefore a lot of attention is given to quantum channels in air and void, which seem to allow practical applications of global QKD today by use of communication satellites network (of course it would require such a network of newly designed satellites to be placed on orbit, however technology of appropriate detectors and sources allowing acceptable level of coherent optical communication between Earth and satellites network is available).

Another significant and maybe even more serious restriction for QKD systems, on current development level of these protocols is their *peer-to-peer* communication model. Appearing propositions (e.g., conception of QKD implementing *one-to-few* communication model [39]), are not introducing any qualitative changes in this aspect. Possibility of full scaled integration of quantum key distribution applications into different models of telecommunication networks with various topologies presently remains unresolved issue. However currently commercially available QKD systems ready to be integrated in large LAN networks (or even MAN networks) with star or ring topology are already finding customers in the field of commercial applications – especially for e-banking services.

4. Experimental deployments of quantum cryptography in telecommunication backbone optical networks

Despite not easy to meet criteria believed to be indispensable for implementation of error correction schemes critical for practical realization of quantum information processing devices, a lot of single elements of a quantum computer have been already realized. Nevertheless even theoretical possibility to scale those to a large device (a quantum computer, which would immediately call for quantum cryptography to enable sustained secure communication in contrast to a current motivation based on assumption that this is indeed feasible) remains an open issue.

This problem however is not encountered in case of practical implementation of quantum cryptography, at least in case of QKD protocols without entanglement (where there is no need to apply quantum privacy amplification procedures – based on entanglement purification techniques [56] – requiring non trivial quantum computation capabilities). Even though practical QKD with entanglement is therefore seemingly far from commercial application it is still very valuable experimentally and recent development in this approach has shown some significant improvements [40-43] which have a potential for commercial market. Both protocol families are already realized in few academic centers all over the world (e.g. Cambridge, Geneva, Vienna) and in few commercial companies (e.g. MagiQ, IdQuantiqe, AIT).

Currently a lot of research effort is put towards *hardware* realization of optical set-ups for experimental quantum cryptography deployments in telecommunication networks (implementing BB84, B92 and E91 protocols families). The main factor of success in modern quantum cryptographic deployment into telecom infrastructure is high quality of photon sources and detectors, polarization manipulators, beamsplitters and phase modulators, and steering electronics. Such elements and techniques for preparing optical set-ups are well known in experimental quantum optics – however required precision level for QKD implementation introduces restraints in devices parameters not easy to comply with. In addition to *hardware* implementation core elements, obviously *software* elements of the systems are also required – these are software modules for devices control, integration, statistical data analysis, error corrections, privacy amplification procedures and user interfaces. These modules are usually independently developed and integrated into the whole system in proper configuration upon experimental deployments. For example projects realized in the NLTK (National Quantum Technologies Laboratory) of the Institute of Physics of Wroclaw University of Technology in Poland is carried out in cooperation with AIT and IdQuantique.

Quantum cryptography deployment enables implementing practical applications of novel technological-scientific achievements in a field of quantum information processing and quantum communication. Due to extremely high level of precision required for those techniques and their strong connection with currently ongoing scientific research in this field, it seems that such attempts may function only in an environment of a technical academic centers contribution. Eventual commercial applications of QKD setups, scaled down and integrated into compact devices are being carried out usually as a *spin-off* enterprises.

A special attention is focused on feasibility of quantum key distribution implementation with entanglement – the problem of generating entangled photon pairs is resolved with procedure of type-II parametric down-conversion. Those pairs can be analyzed in view of non-local quantum statistics (Bell and CSHS inequalities) of their polarization states [27]. Core elements for *hardware* realization of optical entanglement QKD setups can be divided in four main groups: coherent light source, entanglement generation (parametric down-conversion), detection and events registering, data analysis and processing. As a coherent light source, fully integrated semiconductor 25 mW laser system (wave length $\lambda = 405nm$ – blue/violet) can be used. Entanglement generation is realized by well investigated [42] method of parametric down-conversion using BBO crystal: its effect is a stream of photon pairs with double wave length ($\lambda = 810nm$), which create entangled pairs along two space directions. Compensation of optical paths lengths for ordinary and extraordinary beams requires using half-wave plate and other BBO crystals (thinner by half) on both those directions. Detection and events registering is a critical element of *hardware* part of the project. Each of two end stations of QKD protocols are equipped in four single photon detectors (in a form of passively quenched silicon avalanche diodes working in Geiger mode). Due to imperfect sensitivity this number of detectors is necessary for polarization or phase shift measurement in randomly chosen basis. The basis choice is done by a beamsplitter and the measurement itself is performed by transmitting beam thru polarizing beamsplitter to

detectors. Detection events for each input channel (detector) must be registered in counting device memory (possibly directly in a computer memory) with time resolution of order of 1 ns during a period of about 1 minute. For this purpose appropriately configured programmable logic system is used for registering detection events and sending data to a computer. Data analysis and processing is performed on two workstation class computers (one for each protocol end station).

Deployment of the experimental R&D QKD systems in the real optical fiber infrastructure of backbone metropolitan network poses a series of challenges. The physical infrastructure of optical fibers is determined by the city telecommunication canalization layout. Dark fibers connecting two, even not very distant metropolitan locations, physically sharing an industry-standard telecom line with many parallel optical fibers (constituting the initial P2P topology and medium for QKD metropolitan network) are still divided in a series of thermally welded interconnections and junctions at telecom canalization crossings, which are the main reason for decoherence and quantum signal losses, resulting in increased quantum bit error rates (QBER) and in a consequence, in infeasibility of key distribution in practical network scenarios.

Therefore prior to deployment of the QKD network in a standard telecom metropolitan backbone infrastructure, extensive laboratory work has to be performed on the setups developed from the laboratory configuration described in [7]. This chapter presents recent state of the art experimental research towards deployment of QKD in metropolitan backbone networks carried out in NLTK Laboratory of Wroclaw Univeristy of Technology in cooperation with CompSecur company in Poland. The optical fiber line of the SMF28 standard has been used towards implementing different interconnection and welding configurations that would most optimally affect operation of two R&D QKD approaches based on the IdQuantique Clavis2 setup (non-entanglement QKD [1,2]) and the AIT Quelle setup (entanglement QKD [3, 4]) in the telecommunication network. Qubits encoding on photons propagating within fiber optics was different in case of both systems (the former encoding qubits on interfering phase shifts of laser impulses in Mach-Zehnder interferometers like setup, while the latter encoding qubits on polarizations of entangled photon pairs generated in the non-linear spontaneous parametric down conversion (SPDC) process [42] in a BBO (barium borate) type crystal [4], however still performing BB84 [1] alike protocol as measuring one of the photons immediately after entanglement generation).

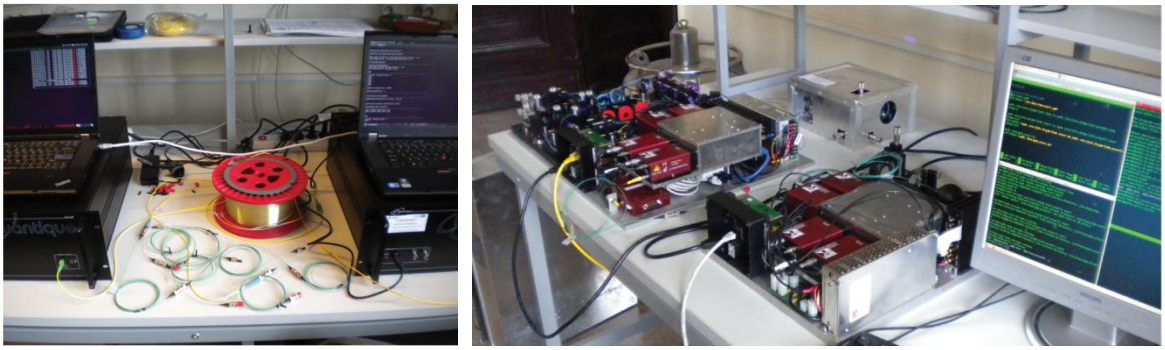


Fig. 5. Experimental deployment versions of QKD Quantum Key Distribution setups not using entanglement in the NLTK laboratory of Wroclaw University of Technology, Poland (based on IdQuantique Clavis2 system from Geneva, Switzerland, on the left) abd using entanglement (based on AIT system from Vienna, Austria, on the right)

In the preliminary laboratory configuration the main optical fiber line (single mode SMF28 standard) of 6.6 km has been subsequently modified in laboratory test runs, being prolonged by subsequently welded or interconnected (with F3000/APC and FC/PC adapters) optical fiber patch-cord lines. The interconnectors results with high QBER increases, thus favoring thermal fiber welding which in proper proximity distribution were characterized by at least one order lower loss induction than interconnectors (ca. 0.01 dB per welding, however depending on proximities and welding quality). Also industry standard telecom fiber optics line tests has been carried out towards welding and interconnections configuration in regard to optimizing QBER and conditioning of metropolitan network physical deployment requirements connecting two locations in a city at a distance of ca. 4-8 km (with a telecom line of ca. 5-10 km and 4 up to several weldings).

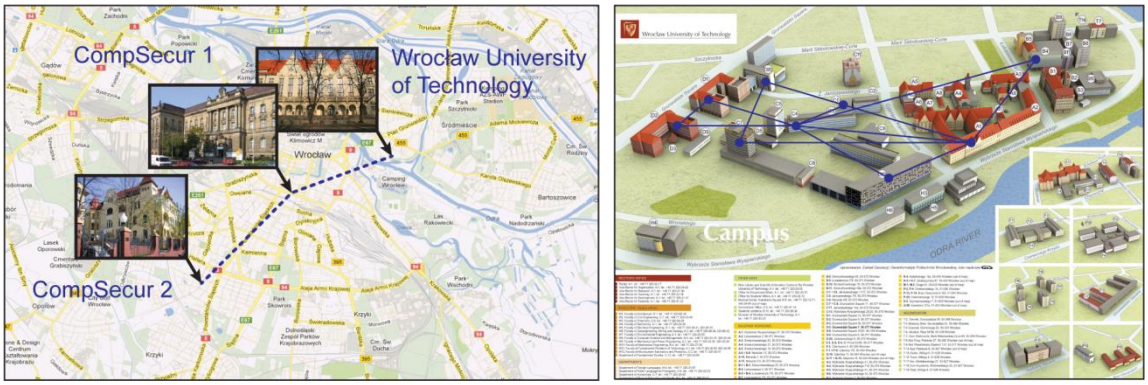


Fig. 6. An analysis of the backbone architecture of Wroclaw metropolitan network and its key nodes was carried out to identify connections of a highest potential in regard to securing with quantum cryptography (analysis includes classification of the threats on the particular nodes and the connection lines, technical characteristics of optical fibers connecting the backbone network nodes and levels of nodes importance from network, business and administration perspective). The experimental testing route was ca. 4.8 km long while connecting Wroclaw University of Technology (WUT) and Compsecur/National Technology Organization (NOT).

Important stability issues are associated with external conditions including temperature and quality of connection, but experimental QKD systems modifications and alignments (especially needed for the entanglement based setup) allow to obtain stable QKD parameters. In terms of deployments feasibility primary focus should be directed towards the non-entanglement based setups which can operate properly with acceptable raw key exchange rate (RKER) generating targeted amount of distilled secret bits (DSB) under laboratory simulation of real optic fiber backbone metropolitan network configuration with required optimization of interconnections and welding infrastructure (estimated compensation for up to 13 dB of overall noise).

The presented measurements were performed for different number of fiber interconnections between Alice and Bob stations, but important experimental setup constituted:

- a 6.632 km fiber spool SMF28 with F3000/APC connectors outgoing from Alice station, interchanged (and also combined) with a telecom standard single-mode optical dark fiber line of ca. 4.8 km and 4 up to 14 weldings (thermal optical fiber weldings)
- further attached, via symmetric F3000/APC adapter, to a 1-meter SMF28 fiber segment with F3000/APC and FC/PC connectors,
- further attached to up to seven 2-meter SMF28 fiber segments with FC/PC connectors (interconnected via FC/PC symmetric adapters),
- and finally including the last segment of 1-meter SMF28 fiber with F3000/APC and FC/PC connectors, attached to Bob station.

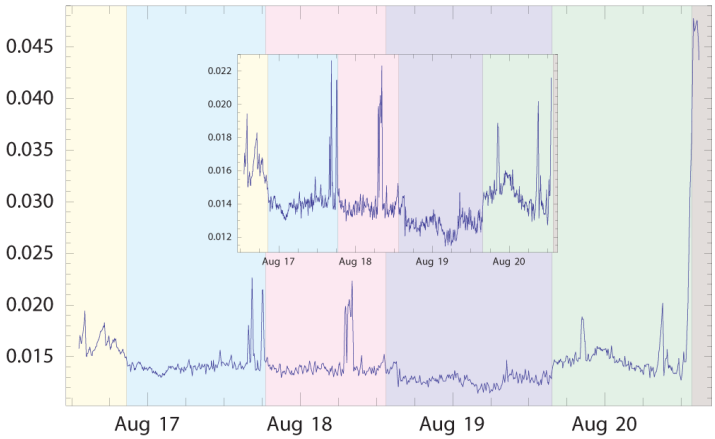


Fig. 7. Privacy amplification and Quantum Bit Error Rater (QBER). In this session setup was continuously operating for a period of 4 days with six subsequently applied numbers of fiber interconnections - respectively 7, 5, 3, 1, 2, 4 intermediate 2-meter fiber segments

The entanglement based QKD has been tested for the first time in a real telecom network environment and proved to be also feasible but within a very narrow gap of optical elements alignment and impractically poor

values of QBER and RKER with additional high instability of operation parameters. Results of the presented laboratory research were analyzed within X-R Shewhart control charts of RKER and QBER and proved as feasible deployment of the QKD metropolitan network in Wroclaw, which is currently taking place.

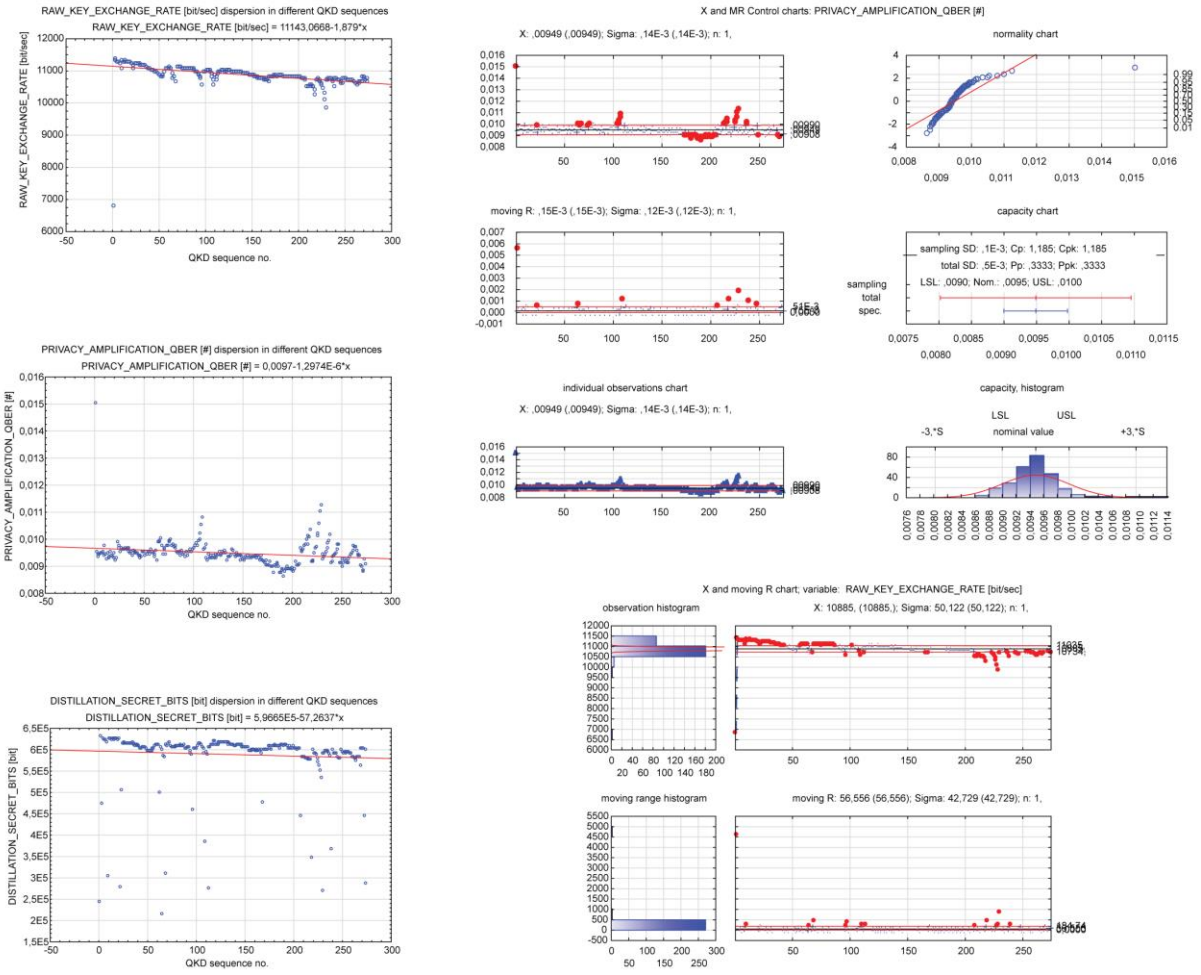


Fig.8. Statistical analysis: dispersion of RKER, QBER and BSD based on 274 quantum key distribution sequences along with X-R Shewhart control charts showing reliable operation of non-entanglement based QKD system in a metropolitan telecom network

Sample characteristics of entanglement based QKD deployment setup:

- Quantum optics and electronic components assembled in an integrated R&D system performing quantum key distribution (QKD) by means of quantum entanglement:
  - Quantum opto-electronic setups generating quantum entanglement in photons polarizations, integrated within 2 end-stations, employing both optical fibres (WDM compatibility) and telescopic (free laser beam) configurations, computer controlled with a hardware/software architecture
  - Featuring non-linear crystal implementation of the parametric down conversion procedure of quantum entanglement production in photon polarizations states (carrier of the information implemented on the polarization of photons in quantum entangled states)
  - Including laser photon source and avalanche photodiode detectors (temperature stabilized)
  - Featuring implementation of E91 [3] entanglement based QKD protocol (including implementation of key sifting, key distillation, error correction and privacy amplification functional layers)
  - Featuring integrated electronic control and interface systems (including synchronization systems)

- Including software suite (containing programming libraries)
- QKD distance: at least 5 km
- Keyrate: at least 0,2 Kbit/s on a 5 km distance
- Temperature of operation between 10 and 30 °C

Sample characteristics of non-entanglement QKD deployment setup:

- Quantum optics and electronic components assembled in an integrated R&D system performing quantum key distribution (QKD) without using of quantum entanglement:
  - Quantum opto-electronic setups integrated within 2 end-stations connected by optical fibres (WDM compatibility) and computer controlled with a hardware/software architecture
  - Including laser photon source and avalanche photodiode detectors (temperature stabilized)
  - Featuring photon phase qubit coding (interferometers with auto-compensation)
  - Featuring implementation of BB84, B92, SARG04 [1,2,44,45] QKD protocols
  - Including software suite (containing programming libraries)
  - QKD distance: at least 50 km
  - Keyrate: at least 1 Kbit/s on a 25 km distance
  - Temperature of operation between 10 and 30 °C

Below we present most recent particular experimental results towards the more advanced entanglement experimental QKD system (based on the modified AIT EPR Quelle 405 setup from Vienna).

4.1. Testing of polarization perturbation influence on a dark channel in the entangled QKD system

For implementation of E91 protocol of QKD, an entanglement of flying qubits is necessary. In the practical setup EPR Quelle (Austrian Institute of Technology, AIT) entangled pairs of photons are provided by parametric down conversion II (PDC) in BBO crystal [4,42]. In this case the mutually orthogonal, V (vertical) and H (horizontal) polarized states of photons are entangled on intersection of two cones of transmission of PDC pair produced in birefringent BBO crystal. In the system EPR S405 Quelle the space-time coincidence of photons, necessary to entanglement [63], is improved by additional correction BBO plates reducing retardation between extraordinary and ordinary photons. In result two beams of entangled photons are directed to separated optical fibers and next – one of them – through the dark quantum channel of cryptographic communication. The AIT demonstrated long distance QKD for open air dark channel [64], when the satisfactory level of conservation of polarization of flying qubits in the telescope setup is ensured. Usage of commercial fiber connections for dark channel encounters, however, a problem with polarization mish-mash produced by accidental birefringence of fiber due to strain in welding and fiber flexion regions. We report a series of tests of the system using different probe optical fibers for a dark quantum channel and compare QBER to short (2-m) polarization fiber connection. Testing include also a commercial 1.5-km long patchcord of fibers to assess possibility of practical implementation of entangled QKD system in metropolitan real network.

The objective of this report is summarizing results of stability testing of QKD system on entangled photons, (EPR S405 Quelle System, Austrian Institute of Technology), with respect to various types of optical fibers for dark quantum channel, in order to assess feasibility of practical utilization of this system in commercial communication networks. As the test indicator we have used testing cards generated by packet qcc [65] in application GNU R in the Quelle system, allowing for quick estimation of stability of system functionality. The quantitative measure is quantum bit error, QBER, which displays the summarized level of communication perturbations. QBER is an effective resultant parameter summarizing all imperfections of the system including detector errors, optical elements mish-mash and optical fiber decoherence. Comparison of QBER for various configurations of optical fibers for dark channel allows, however, to distillate the net factor caused by polarization decoherence of photons in the quantum communication line.

In the system EPR S405 Quelle (AIT) for QKD on entangled photons employing protocol E91 the polarization of photons is treated as flying qubit, which is connected with producing of entanglement by parametric down conversion of type II in BBO crystal applied in this setup. Nevertheless, it is obvious that any perturbation in the optical fiber link between Alice and Bob would modify polarization of transferred entangled photon state and effectively blur the key distribution. Especially exposed to polarization mish-

mash are commercial telecom network lines with many weldings and connectors in patchcords as well as with some accidental stress of fibers e.g., due to their flexion. All these produce uncontrolled birefringence in glass of fibers resulting in uncontrolled drift of polarization of transmitted photons. Except of polarization drift one can encounter also the damping effects of the fragile quantum signal especially inconvenient for longer connections and for fibers not exactly accommodated to transmitted wave-length requirements. Estimation of the influence rate of these perturbations onto functionality of the system is crucial from point of view of feasibility of practical usage of entangled systems even for short distance quantum cryptographic communication in standard commercial optical patchcord metropolitan networks.

4.1.1. Description of measurement and data collection

The data were gathered immediately from the protocol responsible for communication between particular modules of the system software. Each value of QBER was repeated twice and only every second its vale was collected in the final data file. The test card consists of the plot with three type points indicated and of estimated parameters on the base of the collected data. The types of points are differentiated by distinct colors. The points within 'three sigma' region and satisfying the test requiremets, are indicated in black. The points which do not satisfy configuration tests but are located inside the region of 'three sigma', are indicated in orange. The most inconveniently located points, outside the 'three sigma' region are shown in red.

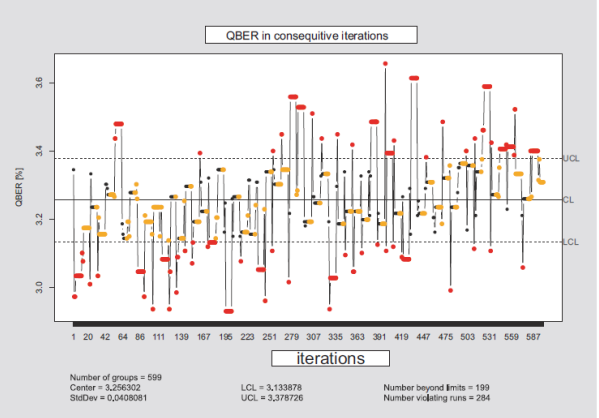
In figures are also plotted lines: (1) the line CL corresponding to average of all values of data, (2) the lines UCL and LCL located on positions CL ±3 sigma, respectively. In figure descriptions the calculated parameter values are listed.

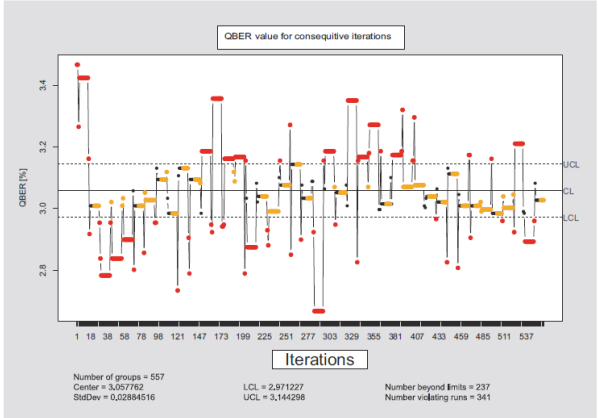
4.1.2. Comparison of dark channel efficiency for different connections and added fiber patchcords

Within the first phase of testing we have compared efficiency of quantum communication by prolongation of the connecting fiber by additional test optical fiber fragments with standard 1 meter length and using also typical standard connectors. The results are displayed in figure 9. Patchcords of 1 meter length would not enhance strongly decoherence rate of the quantum channel, but connectors FC/PC associated to each added patchcord result in dumping increase on the scale between 2 and 3 dB.

Patchcord length [m]	Countings of Alice [thousends/s]	Countings of Bob [thousends/s]	Effetive key [b/s]
1	165	124	1350
2	163	94	1000
3	163	74	1000
4	161	65	900
5	160	57	750
6	160	54	750

Table 1: Table with additional parameters monitored in due of QBER measurement





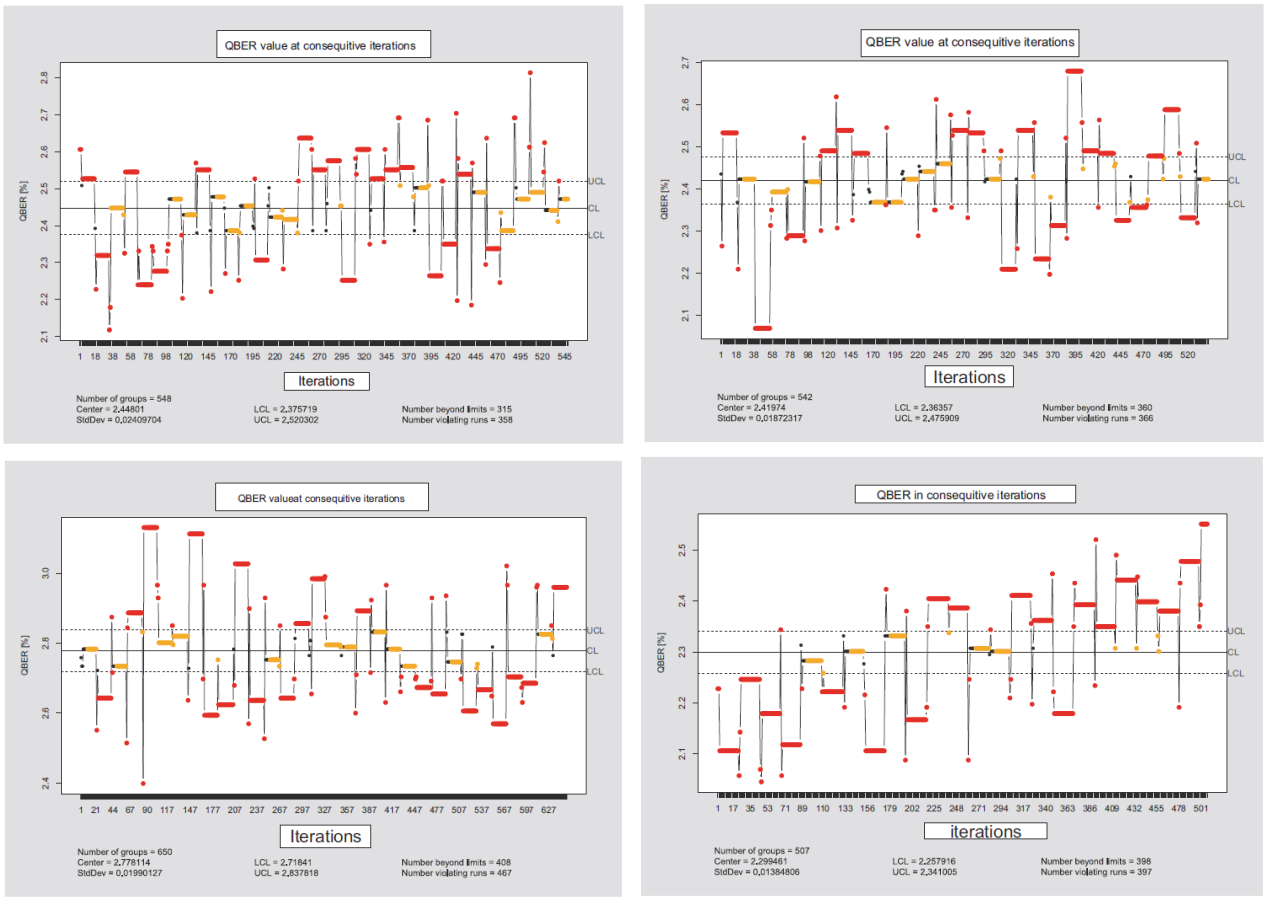


Figure 9: QBER [%] at different configurations of additional patchcord lengths (correspondingly from left top to right bottom for 1 up to 6 meters length)

4.1.3. Measurements of dark channel efficiency for pathcords with different length

In this paragraph we present the quantum dark channel efficiency for elongated fiber connection with additional patchcords of different lengths. The corresponding measurement data are illustrated in figure 10. In this experiment we used optical fibers SX 780HP with lengths 1, 2, 4, 8 and 16 of meters, respectively.

Patchcord length [m]	Countings of Alice [thousends/s]	Countings of Bob [thousends/s]	Effetive key [b/s]
0	149	118	1060
1	145	155	420
2	142	133	2350
4	141	144	2350
8	137	156	2800
16	137	157	940

Table 2: Table with additional parameters monitored in due of QBER measurement for optical fibers SX 780HP

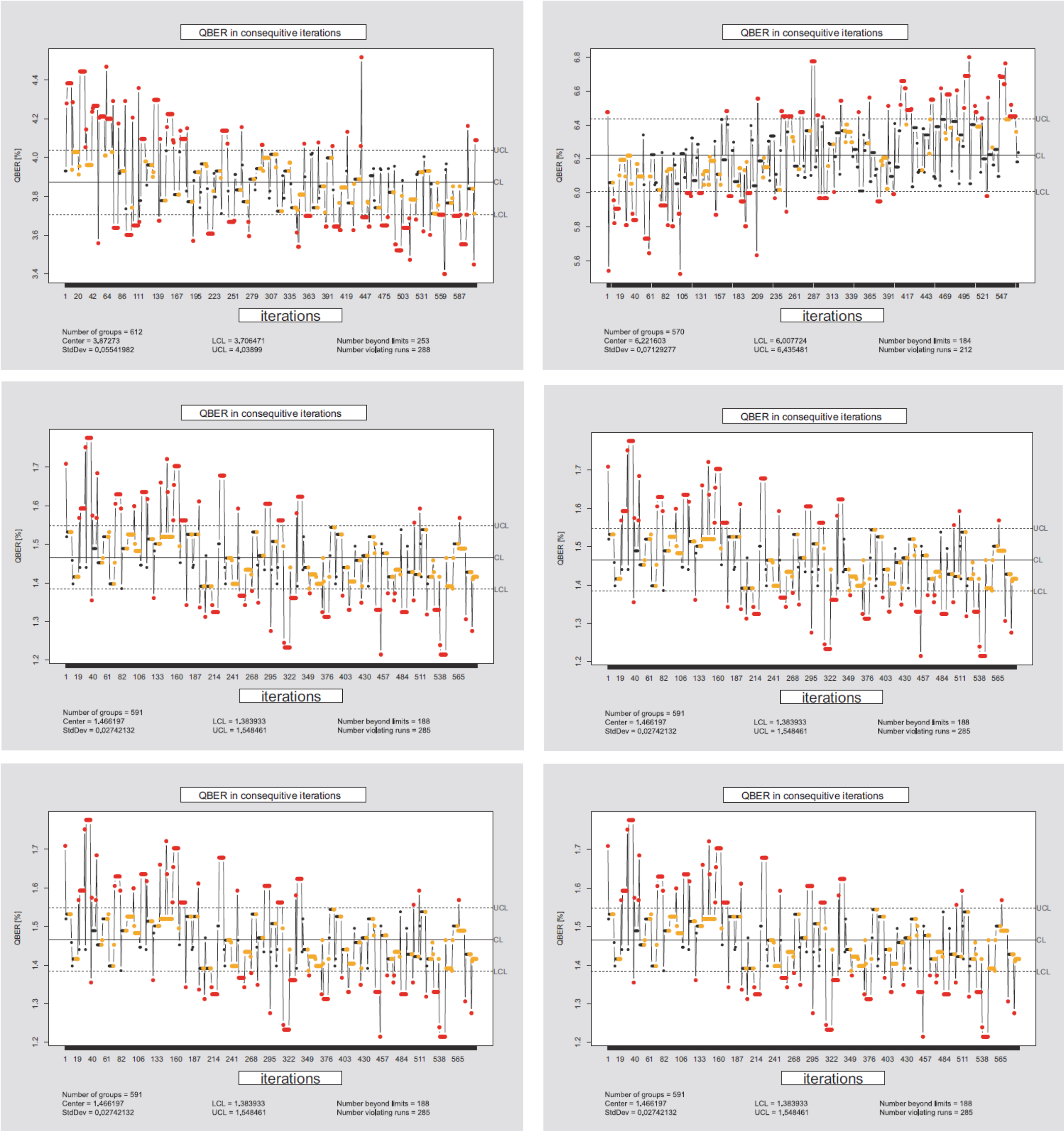


Figure 10: QBER [%] at different configurations of additional patchcord lengths of SX 780HP optical fibers (correspondingly from left top to right bottom for 0, 1, 2, 4, 8, 16 meters lengths)

4.1.4. Measurement of system efficiency with application of third telecom window commercial optical fibers

Except of testing of varius configurations of single-mode 700-900 nm fibers with additional connections, we have tested also patchcords of commercial telecom fibers accommodated to so-called third window transmission, 1530-1565 nm. First we used the fibre 1.5 km long without any additional welds or connectors. The cryptographic key has been finally obtained, but only on the rim of the system efficiency, because ca. 20 % of trials of key sending has been failed. Below we present the results of trials which have been finished with the success (figure 11, bottom). Before performing the experiment with additional patchcords, we have measured the net system as the reference data collection, which is illustrated in figure 11 (top).

Patchcord length [m]	Countings of Alice [thousends/s]	Countings of Bob [thousends/s]	Effetive key [b/s]
0	149	118	1060
1	145	155	420
2	142	133	2350
4	141	144	2350
8	137	156	2800
16	137	157	940

Table 3: Table with additional parameters monitored in due of QBER measurement for third telecom window commercial optical fibers

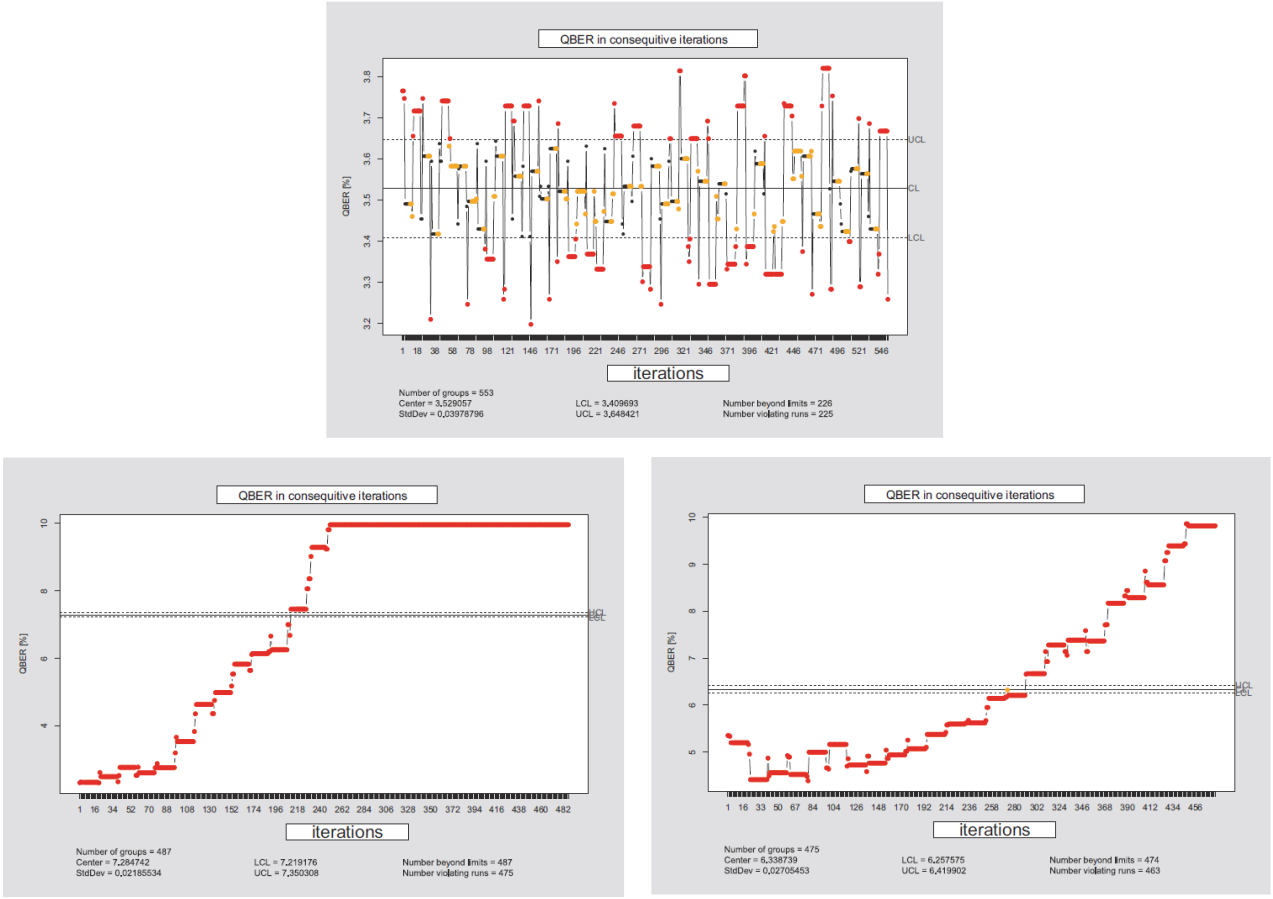


Figure 11: QBER [%] (top – without additional patchcords, bottom – 2 measurements for optical fiber 1550 nm of length of 1.5 km)

4.2. Conclusions

The first conclusion consists in the statement that entanglement QKD Quelle system can be configured to work efficiently for quantum communication using ca. 800 nm wave length photons. Application of optical fiber with ca. 1550 nm transmission window considerably diminishes efficiency to the level of almost preclusion of the key distribution. Moreover, we observe that the process of key generation ceasing to be stable, i.e., the corresponding QBER does not have a normal distribution. The good example is presented in the top of figure 11. The points in this figure are accidentally distributed (between 290 to 320) with extremely high amplitude. The bottom left and right of figure 11 show that the considered perturbations strongly influence the system and change its functionality in a qualitative manner. Two adjustment procedures were necessary to restore the system functionality. The first one corresponds to mechanical adjustments of fixing of optical elements preserving alignment of pumping beam collinear with respect to the base, resulting then in proper alignment of entangled photons. Using the special system with photo-diode one can adjust the pumping beam to optimal position – this procedure had to be, however, repeated more

frequently than without dark channel modification (ca. at every 5 min in comparison to ca. 30 min for net system) for the system with dark channel with higher level of polarization mish-mash. Application of automatic piezo-electric control of the correction mirror would be thus necessary. The second adjustment procedure concerns the direct correction of polarization in order to address and compensate its drift. Each modification of the quantum channel results in some polarization drift which requires proper polarization correction. This adjustment must be performed up to achievement the optimal value of observed data. With this regard development of the system towards automatic self-adjustment of polarization is well justified. Both mentioned here improvements would enhance the feasibility level of usage of the experimental Quelle system for QKD in real commercial metropolitan telecommunication networks.

Upon laboratory research, both the entanglement and no-entanglement based QKD systems deployment in metropolitan telecommunication backbone optical fibers network has been proved to be possible and first commercial deployments currently take place (entanglement based metropolitan quantum network deployed on the telecommunication industrial standard fiber optics lines are rare – and presented experimental results (considering the first real telecommunication infrastructure based quantum network of entanglement based experimental QKD), according to the knowledge of the authors, were successfully obtained for the first time, thus enabling further research in the Quantum Secure Direct Communication (QSDC) implementations domain [50,51]). The presented experimental work constitutes important part of the QKD deployment and commercialization R&D projects that are undertaken in cooperation between NLTK, IP WUT, II WUT and Compsecur (Wroclaw, Poland) with ID Quantique (Geneve, Switzerland) and AIT (Vienna, Austria).

References

[1] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984.
[2] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. 68(21), 1992.
[3] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. 67, 1991.
[4] D. Enzer, P. Hadley, R. Gughes, C. Peterson, and P. Kwiat, *Entangled photon six-state quantum cryptography*, New Journal of Physics **45**, 2002.
[5] H. K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, Science 283, p. 2050, 1999.
[6] H. Lo and N. Lutkenhaus, *Quantum cryptography: from theory to practice*, Phys. Rev. A 66, p. 60302, 2002.
[7] M. Jacak, M. Donderowicz, J. Jacak, W. Donderowicz, J. Gruber, I. Jóźwiak, L. Jacak, W. Jacak, T*owards Wroclaw Quantum Network – industrial telecom testing and deployment of quantum cryptographic systems in a metropolitan network*, Proceedings of the 2nd Annual Conference on Quantum Cryptography QCRYPT 2012, September 2012, Singapore.
[8] E. Shannon, *Communication theory of secrecy systems*, Bell Syst. Tech. J. **28**, p. 656 (1949)
[9] R. Rivest, A. Shamir, L. Adelman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Volume **21** Issue 2, 1978.
[10] P. Shor, *Alghoritms for quantum computation: discrete logarithms and factoring*, Proceedings of 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA (1994)
[11] W. Jacak, J. Krasnyj, L. Jacak, R. Gonczarek, *Decoherence of orbital and spin degrees of freedom in quantum dots*, Wroclaw University of Technology press, monography (2009)
[12]*Quantum Information Processing and Communication – Strategic Report on Current Status*, ICT European Commission (Ed. by P. Zoller) 2005, www.cordis.lu/ist/fet/qipc.htReferences:
[13] D. Bouwmeester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information*, Springer VL, Berlin 2000
[14] M. Johnson, M. Amin, S. Gildert, T. Lanting, , et al., *Quantum annealing with manufactured spins*, Nature **473**, p. 194-198 (05.2011) – http://www.nature.com/nature/journal/v473/n7346/full/nature10012.html
[15] H. Neven (Google Inc.), G. Rose (D-Wave), et al., *NIPS 2009 Demonstration: Binary Classification using Hardware Implementation of Quantum Annealing*, Neural Information Processing Systems 2009 Conference Proceedings (2009) – http://www.google.com/googleblogs/pdfs/nips_demoreport_120709_research.pdf

[16] P. Shor, J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85**, p. 441 (2000)
[17] D. Mayers, *Unconditional security in quantum cryptography*, Journal of the ACM **48** (3), p. 351-406 (2001)
[18] H-K.Lo, H. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, Science **283** (5410), p. 2050 (1999)
[19] C. H. Bennett, G. Brassard, *Quantum Cryptography: Public key distribution and coin tossing*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)
[20] S. Wiesner, *Conjugate Coding* (1970), Sigact News **15**(1), p. 78 (1983)
[21] W. Żurek, W. Wootters, *A single quantum state cannot be cloned*, Nature **299**, p. 802-803 (1982)
[22] A. Aspect et al., Experimental Realization of Einstein-Podolsky-Rosen-BohmGedankenexperiment: A New Violation of Bell's Inequalities, Phys. Rev. Lett. 49, p. 91 (1982)
[23] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nature Photonics **4**, 686-689 (2010)
[24] S. Wiesner, *Conjugate coding*, ACM SIGACT News **15**, 78, (1983)
[25] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters **67**, 661, (1991)
[26] J. F. Clauser, M. A. Horne, *Experimental consequences of objective local theories,* Physical Review D, (1974)
[27] J. S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, 195, (1964)
[28] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review **47**, 777, (1935)
[29] D. Aerts, M. Czachor, *Security in quantum cryptography vs. nonlocal hidden variables: Analysis of a toy Model*, arXiv:quant-ph/0501003 (2005)
[30] D. Bohm, *Quantum Theory, chapter 22: The Paradox of Einstein, Rosen and Podolsky*, Prentice-Hall, Englewood Cliffs, 614, (1951)
[31] Ch. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *Experimental quantum cryptography*, Journal of Cryptology, Vol. **5**, No 1, 3-28 (1992)
[32] A. S. Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel*, Problemy Peredachi Informatsii, (1973)
[33] B. Schumacher, *Quantum* coding, Physical Review A, **51**, 2738–2747, (1995)
[34] J. Clauser, M. Horne, A. Shimony, R. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23**, p. 880-884 (1969)
[35] C.H. Bennett et al., *Teleporting an unknown quantum state via dual classical and EPR channels,* Phys. Rev. Lett **70**, 1895-1899, (1993)
[36] G. S. Vernam, *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, Journal of the American Institute of Electrical Engineers, (1926)
[37] G. Brassard, L. Salvail, *Secret key reconciliation by public discussion*, Advances in Cryptology: Eurocrypt **93** Proceedings, Lofthus, Norway, p. 410-23 (1993)
[38] A. Ekert, J. Rarity, P. Tapster, G. M. Palma, *Practical quantum cryptography based on two-photon interferometry*, Physical Review Letters **69**, 1293, (1992)
[39] P. D. Townsend, *Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing*, Elect. Lett. **33-3**, 188-190, (1997)
[40] Poppe A. et al., *Practical Quantum Key Distribution with Polarization-Entangled Photons*, arXiv:quant-ph/0404115 (2004)
[41] Jennewein et al., *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett. **84**, 4729 (2000)
[42] Kwiat P.G. et al., *New high-intensity source of polarization-entangled photon pairs*, Phys. Rev. Lett. **75**, 4337 (1995)
[43] M. Peev, M. Nolle, O. Maurhardt, T. Lorunser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, A. Zeilinger, *A Novel Protocol-Authentication Algorithm Ruling Out a Man-in-the-Middle Attack in Quantum Cryptography,* Arxiv preprint quant-ph/0407131, (2004)
[44] V. Scarani, A. Acín, G. Ribordy, N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev. Lett. **92**, 057901 (2004)
[45] C. Fung, K. Tamaki, H. Lo, *On the performance of two protocols: SARG04 and BB84*, Phys. Rev. A **73** (2006)
[46] A. Niederberger, V. Scarani, N. Gisin, *Photon-Number-Splitting versus Cloning Attacks in Practical Implementations of the Bennett-Brassard 1984 protocol for Quantum Cryptography*,

[47] D. Rosenberg, A.E. Lita, Aaron J. Miller, S.W. Nam, *Noise-free, high-efficiency, photon-number-resolving detectors*, Physical Review A, (2005)
Arxiv preprint quant-ph/0408122, (2005)
[48] X. Ma, B. Qi, Y. Zhao, H. K. Lo, *Practical Decoy State for Quantum Key Distribution*, Arxiv preprint quant-ph/0503005, (2005)
[49] X. B. Wang, *Beating the PNS attack in practical quantum cryptography*, Arxiv preprint quant-ph/0410075, (2005)
[50] C. Bennett, S.J. Wiesner. *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,* Phys. Rev. Lett., **69**, 2881 (1992)
[51] M. Jacak, W. Donderowicz, J. Jacak, J. Gruber, I. Jóźwiak, W. Jacak, *Unconditionally secure communication protocol based on superdense coding - development of non-local entanglement based quantum communication concepts*, Proceedings of the 2nd Annual Conference on Quantum Cryptography QCRYPT 2012, Singapore, September 2012
[52] F. Xu, B. Qi, H-K. Lo, *Experimental demonstration of phase-remapping attack in a practical quantum key distribution system*, New J. Phys. **12**, (2010)
[53] M. Horodecki, J. Oppenheim, A. Winter, *Partial quantum information*, Nature **436** (7051) 673-686 (2005)
[54] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, et al., *Quantum cryptography: A step towards global key distribution*, Nature **419**, p. 450 (2002)
[55] M. N. Wegman, L. Carter, *New Hash Functions and Their Use in Authentication and Set Equality*, JCSS **22**, 265-279, (1981)
[56] J. Pan, C. Simon, C.Brukner, A. Zeilinger, *Entanglement purification for quantum communication*, Nature **410**, p. 1067-1070 (2001)
[57] D. Bouwmeester, H. Weinfurter, A. Zeilinger, et al., *Experimental quantum teleportation*, Nature **390**, p. 575-579 (1997)
[58] S. Ghernaouti-Hélie, I. Tashi, T. Länger, C. Monyk, *SECOQC Business Whitepaper: Quantum Cryptography, an Innovation in the Domain of Secure Information Transmission*, SECOQC (2008)
[59] *Quantum Cryptography: Market Research Report*, Global Industry Analysts Inc. (2010)
[60] *Quantum Cryptography Market Research*, Frost & Sullivan (2010)
[61] A. Kitaev, *Quantum computations: algorithms and error correction*, Russ. Math. Surv. **52**, p. 1191 (1997)
[62] M. A. Nielsen, I. L. Huang, *Quantum Computation and Quantum Information*, Cambridge UP 2000
[63] Y. Kim, S. Kulik, and Y. Shih, *High-intensity pulsed source of space-time and polarization double-entangled photon pairs*, Phys. Rev. **A 62**, 011802 (2000)
[64] M. Aspelmeyer, H. Bohm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, *Long-Distance Free Space Distribution of Quantum Entanglement*, Science **301**, 621 (2003)
[65] L. Scrucca. *qcc: an r package for quality control charting and statistical process control*. R News, 4/1:11–17 (2004)