COHERENTLY CORRELATED BEAMS AND THEIR USE IN QUANTUM COMMUNICATIONS

V.C. USENKO[1], C.V. USENKO[2], B.I. LEV[1,2]

[1]Institute of Physics, Nat. Acad. of Sci. of Ukraine
(46, Nauky Ave., Kyiv 03028, Ukraine),

[2]Taras Shevchenko Kyiv National University, Faculty of Physics
(6, Academician Glushkov Ave., Kyiv 03127, Ukraine)

UDC 530.145
©2005

The statistical properties of two-mode coherently correlated states of a laser beam and the possibility to use them in the construction of secure quantum channels are described. The stability and security of a corresponding quantum-cryptographic protocol are analyzed.

1. Introduction

The physics of quantum communications which include quantum cryptography [1–3] is one of the modern and dynamical branches of quantum physics. The task of quantum cryptography, in particular, consists in the development of methods or protocols for the construction of secure channels for the transmission of data, in which the laws of quantum physics make it impossible to intercept any information.

The need in such channels is caused by the insufficient reliability of classical asymmetric cryptography with the use of an open key. This method is based on the mathematical complexity of an encoding procedure and thus can instantaneously become useless due to the unexpected break in mathematical methods or the inevitable development of computational facilities, in particular, due to the appearance of quantum computers. Completely secure is classical symmetric cryptography with the use of a closed (secret) key (in this case, it is optimum to have a key with the same length as that of an encoded message). But the main difficulty of a cryptography of this type is the necessity to transmit the secret key to both participants of the secure informational exchange (by the tradition accepted in cryptography, the participants of such an exchange are called Alice and Bob, and a potential enemy who can try to intercept them is called Eve).

Thus, there appears the necessity in communication channels which would be sufficiently secured from the interception in order that Alice and Bob can possess, as a result, a common guaranteedly secret key which can be used then for the encoding of any informational exchange through the existent commonly available channels (in particular, the Internet). That is, quantum cryptography is engaged in just the development of methods for such a secret key distribution. It is worth noting that the quantum key distribution (QKD) is, in fact, the first practical application of the laws of quantum physics on the level of separate quanta, being, in this case, on the crossing of quantum mechanics and information theory. For two last decades, quantum cryptography has passed a way from theoretical ideas to the first industrial prototypes, but it requires to be developed up to now.

The first quantum-cryptographic protocol [6] was proposed by C. Bennett and G. Brassard in 1984 (it was then named as BB84). It foresees the usage of four quantum states of individual particles with a half-integer spin which can be aligned along or opposite to one of the two orthogonal directions: $|\rightarrow\rangle$, $|\leftarrow\rangle$,$|\uparrow\rangle$,$|\downarrow\rangle$. The binary value 0 is assigned to states $|\uparrow\rangle$ and $|\rightarrow\rangle$, and the value 1, respectively, to states $|\downarrow\rangle$ and $|\leftarrow\rangle$. The states of a two-level quantum system begin, thus, to be considered as bits, and the system itself as a quantum bit (a qubit), whose main difference from a classical (Shannon) bit consists in that the value of a qubit arises only under its measurement. Prior to the measurement, it is a superposition of states which correspond to two binary values.

Though the protocol was proposed for electrons, it was realized, like the other protocols, on the base of photons, whose states are different by polarization. Below, we will describe this protocol for polarized photons. Since a polarization is characterized by the axis rather than a direction on this axis, we consider 4 states in the photon realization: one with the horizontal polarization h (it is treated as bit 1), one with the vertical polarization v (bit 0), and two with the diagonal polarization $+\frac{\pi}{4}$ (bit 1) and $-\frac{\pi}{4}$ (bit 0).

A state of photons is registered in one of the Cartesian bases: vertical-horizontal (h/v) and diagonal

$(+/-\frac{\pi}{4})$ ones which are turned each relative to other by angle $\frac{\pi}{4}$.

For each particle which is sent by Alice to Bob, she randomly chooses the value of a bit and the basis and prepares a particle in the relevant state. Each time, when Bob expects the arrival of a particle, he activates his detectors and chooses randomly one of thw two bases h/v or $+/-\frac{\pi}{4}$, in which the measurement will be performed. He registers which basis has been used and which bit value he has derived. After the exchange of a sufficient number of particles, he openly informs Alice (via a commonly used net), in which events he has registered particles and which basis has been used. But he communicates nothing about the values of bits he has derived. Alice compares event by event, whether Bob's basis was consistent with that, in which she prepared a relevant particle. The events, in which the bases do not coincide, or Bob has not registered a particle, are rejected. As for the remaining events, Alice and Bob can be sure that the corresponding values of bits are identical. These bits form the so-called sieved key.

The security of such a protocol is based on that an interceptor will disturb, in most cases, a quantum system unknown for him/her, by performing the measurement. Thus, either the sieved keys of Alice and Bob are identical, no interception has occurred, and the key is guaranteedly secret and can be used in the cryptographic encoding of information, or, depending on the degree of noncorrelatedness of the sieved keys (which is characterized by the QBER parameter — the quantum bit error rate), Alice and Bob can apply the cryptographic procedures of correction of errors to them and can enhance the security, or can reject these keys and repeat the transfer procedure. The communication on this protocol was reported at the IEEE International Conference on Computers, Systems, and Signal Processing in India and remained almost unnoticed for the community of physicists.

In 7 years, in 1991, A. Ekert proposed a protocol which is called, by analogy, E91 [7]. This protocol is based on the use of pairs of fermions that are in a singlet state (in honor of the Einstein-Podolsky-Rosen experiment, such particles are called EPR-correlated). The particles of a pair are separated, and one moves to Alice, and the other to Bob. They measure the spin of a next particle in one of the three directions, whose azimuth angles are equal to 0, $\frac{\pi}{4}$, and $\frac{\pi}{2}$ for Alice and $\frac{\pi}{4}$, $\frac{\pi}{2}$, $\frac{3\pi}{4}$ – for Bob. Each particle is considered as a quantum bit which has the value 1, if the particle spin is directed upward, and –1, if the spin is directed downward. After the transfer of a sufficient number of bits, Alice and Bob reject the recordings, in which one of them or both did not register a particle. Then they compare the orientation of the own analyzers in each separate measurement and divide the derived values of bits into two parts. The first part includes the events, in which the orientations of analyzers were different, and the second – those with the same orientation. By the first group of events, they calculate values of the Bell parameter which includes the correlation coefficients of measurements performed in different, specifically selected pairs of bases:

$$S = |E(a_1,b_1) - E(a_1,b_3) + E(a_3,b_1) + E(a_3,b_3)|. \quad (1)$$

In this case, each coefficient is the difference of the probabilities to register the identical and different values of bits:

$$E(a_i,b_j) = P_{++}(a_i,b_j) + P_{--}(a_i,b_j) -$$
$$-P_{+-}(a_i,b_j) - P_{-+}(a_i,b_j). \quad (2)$$

Here, $P_{\pm\pm}(a_i,b_j)$ stands for the probability of that the result ±1 was derived by Alice in the basis a_i and the result ±1 was derived by Bob in the basis b_j.

For the considered singlet state of two fermions and with regard for the collection of the used bases, the value of this parameter should be equal to $2\sqrt{2}$, which violates the so-called Bell inequality [7] that requires for $S \leq 2$ to be valid. Thus, by calculating this parameter, Alice and Bob can verify its value and draw conclusion whether the interference in a state of the system has happen (i.e. the interception). If such a check has not reveal the signs of the vioplation of a state, then the second collection of bits that were derived in the same bases can be considered completely anticorrelated. Thus, this collection can be transformed into a cryptographic key, whose security is based, thus, on the Bell inequality.

In order to experimentally realize his protocol, Ekert proposed to use the scheme of the experiment proposed in [8] for the verification of the Bell inequalities, in which the pairs of polarized photons are used.

Further, the mentioned protocols were supplemented, were slightly changed, but remain to be the base for all experimental realizations of quantum cryptography which were carried out on the basis of two-level states of photons of a laser beam represented by their polarization (sometimes, the encoding by frequency or phase is also used). In this case, the development of protocols was related to the aspiration to make them to be more applicable and secure against the increasingly perfect techniques of interception, without the introduction of basic changes in circuits.

In the general case, while studying the security of protocols of quantum cryptography, one poses the task to investigate all possible means of interception [18] and their potential development. Traditionally, the attacks with the interception of photons by using the splitting of a beam and the method of cloning of a state are considered and analyzed as the most efficient. In spite of the fact that quantum physics forbids the ideal copying of an arbitrary unknown state (the theorem on impossibility of the cloning [17]), an interceptor can determine the state of a laser pulse which is a carrier of information in the quantum optical channel, by absorbing this pulse, and then will try to create a state, whose density matrix is as close to the density matrix of the original state as possible. We also mention the attacks by the so-called Trojan horses, where an interceptor sends his/her photons to the channel expecting their reflection in the setup and the return backward. This type of attacks is efficient against the realizations which are based on the phase or polarization modulation and the use of mirrors, because it allows one to determine the state of modulators.

However, the exhaustive evaluation of the security of a protocol is rather complicated, because it depends on its specific realization and the assumptions as for a technique used by an interceptor. It is commonly accepted in this case that all errors can be used potentially by an interceptor in order to derive information or are induced by its interference. This requires the additional enhancement of the security of a sieved key with the help of special cryptographic algorithms, which shortens it and, respectively, decreases the effective transmission rate.

The first practical demonstration of quantum cryptography for protocol BB84 (more properly, for its somewhat modified version B92 with the polarization encoding of single photons) was realized in 1992 [10] under laboratory conditions with the transmission of a key at a distance of 30 cm. In 2000, the realization of protocol B92 [12] was improved, and protocol E91 [11] was implemented with the use of polarization-entangled [13] pairs of photons. Further, there appeared the first commercial schemes which had, nevertheless, essential limitations.

At present, quantum cryptography demonstrates rates of about one thousand bits of a key for one second at distances of tens of kilometers with fiberoptic channels or of several kilometers in open space under the condition of direct visibility (the last variant is a candidate for the truly far quantum cryptography upon the exchange by a key, for example, with a satellite). In this case, the experiments showed that the frequency of errors for these quantum-cryptographic protocols and, as a result, the limitation as for the maximum distances of the transmission of a key are related to, first of all, the low intensity of beams. This makes the manifestations of the imperfection of one-photon detectors (which are inclined to “dark”, i.e. idle counts in the absence of photons) and optical transmission channels (which, in particular, change a state of a polarization of photons and weaken pulses) to be strong. In this case, in order to increase the maximum distance or transmission rate, the increase in the number of photons in pulses is a more efficient way than the increase in the frequency of pulses. But at the same time, the appearance of superfluous photons in a pulse can be used by an interceptor who can measure their state introducing no errors and, thus, remaining imperceptible. That is, the average number of photons in a pulse should be much less than 1 to minimize the probability of the appearance of additional photons.

This contradiction can be removed by applying powerful pulses for the construction of a channel. For this purpose, a new quantum-cryptographic protocol which is based on the use of peculiar, the so-called two-mode coherently correlated (TMCC) states [15, 16] of a laser beam was proposed. In the present work, we present a profound analysis of the security of a TMCC-protocol.

2. Properties of Beams

TMCC states are the completely correlated and, at the same time, proper states of a product of the operators of annihilation of both modes and can be represented as an expansion in the Fock states of two modes:

$$|\lambda\rangle = \frac{1}{\sqrt{I_0\left(2\left|\lambda\right|\right)}} \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} \left|nn\right\rangle . \qquad (3)$$

Here, we used the notation $|nn\rangle = |n\rangle_1 \otimes |n\rangle_2$, where $|n\rangle_1$ and $|n\rangle_2$ correspond to states of 1 and 2 modes, respectively, which are represented by their numbers of photons.

The first important feature of such states consists in the absence of terms with different numbers of photons in the sum (3). This fact yields the strong correlation between the observables related to each mode.

Since the Fock states can be written as

$$|n\rangle = \frac{a^{+n}}{\sqrt{n!}}|0\rangle, \qquad (4)$$

we can present TMCC-states (3) in the form

$$|\lambda\rangle = \frac{1}{\sqrt{I_0\left(2\left|\lambda\right|\right)}} I_0(2\lambda a_1^+ a_2^+)\left|0\right\rangle . \qquad (5)$$

Considering TMCC-states, we cut a substate $\{|n,n\rangle\}$ which contains the states with identical nimbers of photons from the entire Fock space of two-mode states $\{|n,m\rangle\}$. The operators $A = a_1 a_2$ and $A^+ = a_1^+ a_2^+$, being the products of quantum operators that correspond to each mode, completely describe the algebra of the observables of a TMCC-state. The second defining feature of the states under consideration is that the TMCC-states are proper for a product of the annihilation operators. But, at the same time, they are not proper for each quantum operator separately.

By assuming that a TMCC-state is represented by two laser beams which are propagating in space independently each from other, we can study the observables of such an emission.

As distinct from ordinary noncorrelated coherent states, for which any quantity linear in the field has a nonzero average value, the average value of any analogous quantity for TMCC states is zero. Indeed, in the process of averaging over the first mode, the operator a_1 transforms $|n,n\rangle$, e.g., into $|n-1,n\rangle$ which is orthogonal to all available components of the state. Thus, $\langle\lambda_i|\, a_i\, |\lambda_i\rangle = 0$. An analogous relation is true for the other mode. Each mode of a TMCC-beam is not coherent separately by itself. But they possess mutual coherency which manifests itself, for example, in a spatial correlation function that contains the average values of products of quantum operators, some of these values being nonzero.

Nonzero are also the average values of the observables for each mode separately that are quadratic in the field, namely the energy and the momentum. This fact allows us to consider TMCC-modes to be quadratically correlated.

Let us study any of two TMCC-beams separately. The emission intensity registered by an observer is proportional to the average value of the operator $N = a^+a$ which is the operator of the number of photons in the relevant mode. These observables are quadratic in the field, and thus their average values are not transformed to zero (it is worth noting that this fact is not unique for TMCC-states, because the ordinary noncorrelated states and processes such as the propagation of heat demonstrate the same properties).

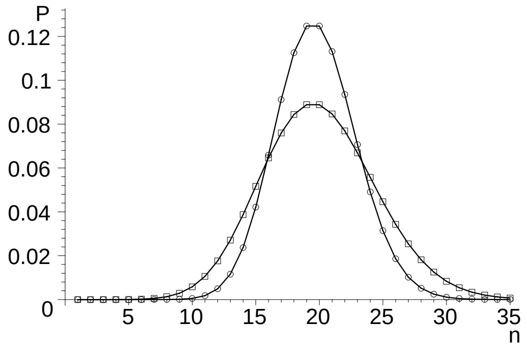

Fig. 1. Probability distribution of the registration of various numbers of photons for a TMCC-beam (circles) and the corresponding distribution for the ordinary Poisson coherent beam (crosses)

The probability to register some number n of photons depends on the intensity of a beam:

$$P_n(\lambda) = \frac{1}{I_0(2|\lambda|)} \frac{|\lambda|^{2n}}{n!^2}. \qquad (6)$$

The important property of this distribution is the rapidly decreasing (proportionally to $n!^2$) probability of the registration as a function of the number of photons. This circumstance makes the experimental identification of TMCC-states to be convenient. The plot of the probability distribution to register various numbers of photons and the corresponding Poisson distribution for an ordinary coherent beam (or the thermal emission) are given in Fig. 1.

A type of the statistics of a beam can be characterized by the Mandel parameter, which includes the average and mean square values of the number of photons:

$$Q = \frac{\langle N^2\rangle - \langle N\rangle^2}{\langle N\rangle} - 1. \qquad (7)$$

At $Q > 0$, the statistics of a beam is super-Poisson. That is, the uncertainty of the number of quanta is greater than the standard one, and a beam is less ordered than a thermal flow. At $Q < 0$, respectively, a beam has sub-Poisson statistics, the uncertainty of the number of quanta is less than the standard one, and a beam is more ordered than a thermal flow.

The dependence of the Mandel parameter (7) on the average number of photons is shown in Fig. 2. It is easy to see that a TMCC-beam manifests a pronounced sub-Poisson statistics even at low intensities.

3. Quantum Channel

Assume that we need to construct a secure quantum channel between the two participants of the transmission

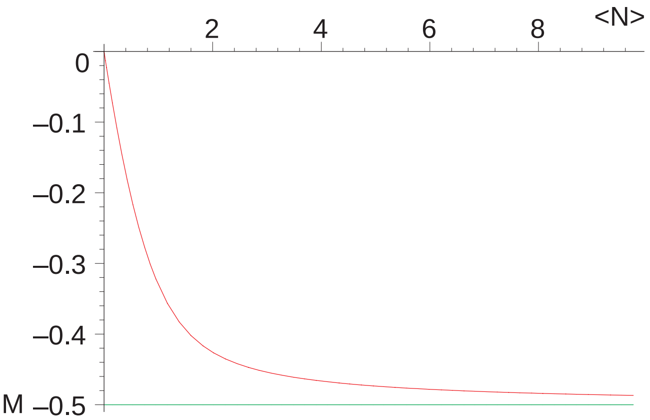

Fig. 2. Mandel parameter vs the average number of photons for a TMCC-beam

of some sequence of bits (Fig.3). As has become traditional in the literature on quantum communications, we name them Alice and Bob. Alice has a laser which creates two beams in a TMCC-state. The optical channel is organized in such a way that Alice receives one of the modes, for example, the first one. That is, $\varphi_A \equiv \varphi_1$, $\varphi_A(x_A, t_0) = 1$. Bob receives the other one, i.e. $\varphi_B \equiv \varphi_2$, $\varphi_B(x_B, t_0) = 1$ at every moment of the measurement t_0. Here, x_A and x_B are the positions of Alice and Bob, respectively. In addition, Alice does not receive the mode of Bob and vice versa: $\varphi_B(x_A, t_0) = 0$, $\varphi_A(x_B, t_0) = 0$.

As was mentioned, TMCC-beams reveal the correlation between the observables of both modes which can be conveniently characterized by the coefficient of relative correlation

$$\rho_{AB} = \frac{\langle N_A N_B \rangle - \langle N_A \rangle \langle N_B \rangle}{\sqrt{\langle N_A^2 \rangle - \langle N_A \rangle^2}\sqrt{\langle N_B^2 \rangle - \langle N_B \rangle^2}}. \tag{8}$$

As an important feature of TMCC-beams, we indicate the fact that their coefficient of relative correlation ρ_{AB} equals 1. That is, the results of individual measurements of each of the two modes not only give the identical average values, but have the same deviation from the average.

A laser beam is a semiclassical emission with well-defined phase. But, due to the principle of uncertainty for the number of photons and the phase, there exists a rather great uncertainty of the number of photons. Therefore, one must observe a noise similar to the Schottky noise in electron tubes. In the TMCC-emission, the characteristics of such a noise are well correlated each with other for each mode. This fact allows the usage of such an emission for the generation of a random code which will be equally well received by two mutually remote detectors.

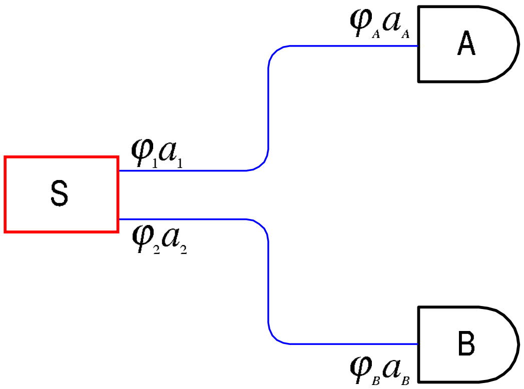

Fig. 3. Quantum channel on the base of a TMCC-beam

3.1. Protocol

The following scheme can be used for a protocol on the base of TMCC-states. Let a laser be tuned so that it can create a constant average number of photons during the whole time interval of transmission of a key, and both the sides know this number. At some time moment, Alice and Bob begin to measure. They determine the numbers of photons per unit time by measuring the integral intensity of the corresponding beam. If the number of photons in some unit time interval is more than the known average value (at the expense of the Schottky noise), then the next bit of the generated code is considered to be equal to 1. If the measured number is less than the average value, the next bit is taken to be equal to 0:

$$B = \begin{cases} \{n \le [\langle N \rangle]\} \to 0, \\ \{n > [\langle N \rangle]\} \to 1. \end{cases} \tag{9}$$

After the reception of a sufficient amount of bits (of the code), Alice and Bob divide this sequence into two halves by deriving two sequences of bits (semicodes). Bob encodes one sequence with the other one by using the logical operation XOR (excluding OR) and sends the encoded semicode to Alice through some public channel. Alice uses any of the own semicodes in order to decode the semicode she received from Bob (by the same operation XOR). She compares the result of the decoding with her other semicode. If all the bits coincide, this means that Alice and Bob have the same full code that can be used as a cryptographic key for the encoding of their further exchange by information. In other case, they must repeat the procedures of generation and transmission of a key and must check the channel for a possible interception, if this procedure will be unsuccessful again.

4. Security of a Channel

The security of a channel is its stability against the attempts to intercept. Let some interceptor (by tradition, we call her Eve) try to receive a secret key that is transmitted through a quantum channel to Alice and Bob. Eve ca use various techniques of interception. But, in any case, his interference in the channel changes statistical properties of the state, which can be described in terms of the density matrices.

The density matrix of a TMCC-source is as follows:

$$\rho_s = |\lambda\rangle \otimes \langle\lambda| = \frac{1}{I_0(2|\lambda|)} \sum_{n,m=0}^{\infty} \frac{\bar{\lambda}^m \lambda^n}{m!n!} |mm\rangle \otimes \langle nn.| \quad (10)$$

It includes nondiagonal elements which correspond to a correlation between the modes. The detector of Alice reduce the source state in states of the mode of Alice,

$$\rho_s \longrightarrow \rho_2 = {}_1\langle k|\, \rho_s\, |k\rangle_1\,, \quad (11)$$

and makes nondiagonal elements to be zero. Thus,the density matrix of the mode which is measured by Bob looks as

$$\rho_B = \langle \rho_s \rangle_A = Tr_A \rho_s =$$

$$= \frac{1}{I_0(2|\lambda|)} \sum_{k=0}^{\infty} \frac{|\lambda|^{2k}}{k!^2} |k\rangle \otimes \langle k| = \sum_{k=0}^{\infty} P_k\, |k\rangle \otimes \langle k|. \quad (12)$$

When Eve makes decision to intercept, she begins to measure one of the modes (e.g., the mode of Bob) with the own detector. The density matrices which describe the results of measurements for each of the detectors are

$$\tilde{\rho}_A = \mathrm{Tr}_{BE}\rho_s, \quad \tilde{\rho}_B = \mathrm{Tr}_{AE}\rho_s, \quad \tilde{\rho}_E = \mathrm{Tr}_{AB}\rho_s. \quad (13)$$

If Eve intercepts the mode of Bob, its interference does not change the density matrix of Alice, i.e. $\tilde{\rho}_A = \rho_A$.

We now determine the distance between the density matrices with the help of the Hilbert-Schmidt norm as $D^2 = ||\rho_B - \tilde{\rho}_B||^2$ or the weak norm $d = |\rho_B - \tilde{\rho}_B|$. Since both matrices are diagonal, we calculate the distance by the weak norm as the maximum of the difference modulus. These observables can be useful for the discovery of the interception of information or for the determination of the success of the interception. They can be derived from the probability distributions

$$D^2 = \sum_{n=0}^{\infty} (P_n^{(orig)} - P_n^{(B|E)})^2, \quad (14)$$

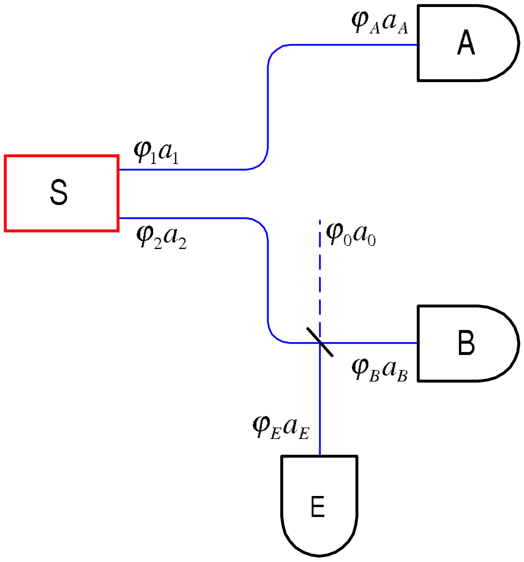

Fig. 4. Intercepting attack on a TMCC-channel

$$d = \max_{n=0..\infty} (|P_n^{(\mathrm{orig})} - P_n^{(B|E)}|). \quad (15)$$

4.1. Attack with the Splitting of a Beam

The most simple type of interception is the splitting of a beam, when Eve splits and takes aside a part of the beam moving, for example, to Bob and determines its intensity by mounting a detector on her side (Fig. 4.).

In this case, the field amplitude of the second mode is split in some ratio $p : q$. Thus, the mode is expanded in the basis which is composed from the modes arriving to Bob and Eve. In order to describe the properties of this beam, we add a mode in the basis of Bob and Eve which is orthogonal to φ_2:

$$\varphi_0 = -q\varphi_B + p\varphi_E. \quad (16)$$

Without interception (and thus without a splitter), Eve receives only the mode φ_0, in which a laser does not emit. That is, $\varphi_0 = \varphi_E$ and $\varphi_2 = \varphi_B$.

The next transformation of the operators corresponds to the expansion

$$a_2 = pa_B + qa_E, \quad (17)$$

$$a_0 = -qa_B + pa_E. \quad (18)$$

Hence, we get

$$\varphi_0 a_0 + \varphi_2 a_2 = \varphi_B a_B + \varphi_E a_E \quad (19)$$

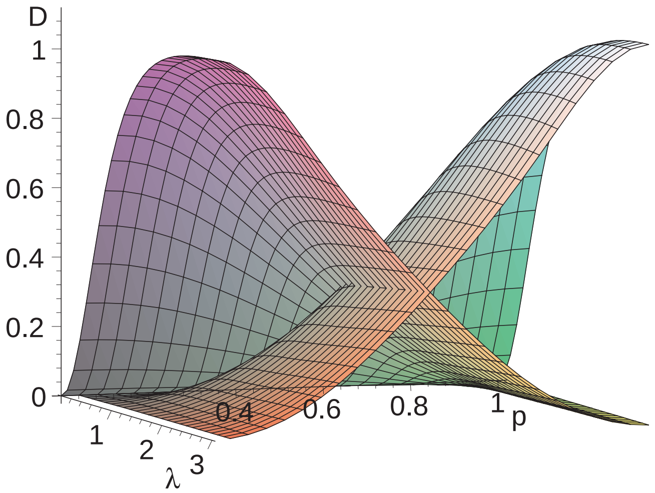

Fig. 5. Distances between the density matrices for the pairs Alice-Bob and Alice-Eve as functions of the source parameter λ and the interception degree $p = cos\psi$

and an analogous relation for the operators conjugate by Hermite.

These transformations change the initial state (5) into

$$|\lambda\rangle = \frac{1}{\sqrt{I_0\left(2\left|\lambda\right|\right)}} I_0(\lambda a_A^+ (p a_B^+ + q a_E^+)\left|0\right\rangle . \qquad (20)$$

Respectively, the probability distributions for the registration of the numbers of photons become

$$\tilde{P_n^B} = \frac{\left|\lambda\right|^{2n}\left|p\right|^{2n} I_n\left(2\left|q\right|\left|\lambda\right|\right)}{\left|q\right|^n n! I_0\left(2\left|\lambda\right|\right)}, \qquad (21)$$

$$\tilde{P_n^E} = \frac{\left|\lambda\right|^{2n}\left|q\right|^{2n} I_n\left(2\left|p\right|\left|\lambda\right|\right)}{\left|p\right|^n n! I_0\left(2\left|\lambda\right|\right)}. \qquad (22)$$

Having known these distributions, we can determine whether the interception with the splitting of the beam was successful, by calculating the distances between the density matrices for the pairs Alice-Bob and Alice-Eve. The dependence of these distances on the beam intensity and the interception degree is given in Fig. 5. It is easy to see that, in the case of a weak interception, the results of measurements of Bob do not practically vary, and the interception is inefficient. If it becomes efficient, Bob feels the loss in the transmission quality, and the channel is broken. In addition, Bob can calculate the distance between the density matrices of the derived and expected states by the weak norm in order to verify whether the beam was split or did not. The dependence of the distance between the derived and expected density matrices by the weak norm on the interception degree is shown in Fig. 6.

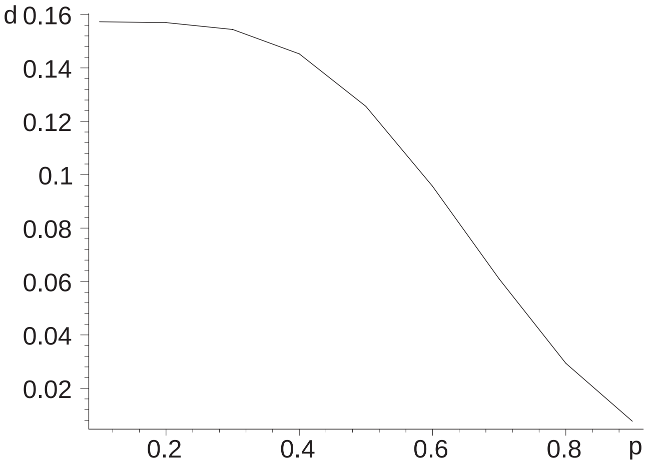

Fig. 6. Distance between the density matrices of the derived and expected states by the weak norm vs the interception degree

4.2. Attacks with the Cloning of the State

Besides a simple interception based on the splitting of the beam, Eve can try to measure the whole mode of Bob which arrives from a laser source and then to clone the state by emitting the same number of photons to Bob by using the own source. However, the statistical properties of a cloned state will not coincide with those of the original state.

We consider that the use of a TMCC-source will give the most efficient means for Eve. In order to clone a state, she must guess which value of the state parameter λ corresponds to the exact number of photons measured by Eve in the next pulse. In this case, the optimum strategy of Eve will consist in the determination of the necessary value of λ from the numerical solution of the equation of state for the given number of photons. Let Eve have measured n photons in the mode of Bob and try to create the same number of photons by tuning her laser to get the calculated state parameter $\lambda(n)$. In the case where Eve is constructing a cloned state, the parameter $\lambda(n)$ includes an arbitrary phase factor which, nevertheless, does not change the density matrix of Bob.

One mode of a cloned state is rejected, and the other mode which will be received and measured by Bob is averaged over the states of the rejected mode (analogously to (12). Since a cloned state, under condition that Eve has registered n photons, will lead to the density matrix $\tilde{\rho}_B^{(n)} = \rho(\lambda(n))$ for Bob, the total density matrix which corresponds to the measurement of Bob is the mixture

$$\tilde{\rho}_B = \sum_{n=0}^{\infty} \tilde{\rho}_B^{(n)} P_{E,n}(\lambda) \tag{23}$$

of cloned states for different n with weights

$$P_{E,n}(\lambda) = \frac{|\lambda|^{2n}}{n!^2 I_0(2|\lambda|)},$$

which are equal to the probabilities of the registration of n photons by Eve. Finally, the density matrix which corresponds to the measurement of Bob has form of a mixture of k-photon states

$$\tilde{\rho}_B = \sum_{k=0}^{\infty} \tilde{P}_k |k\rangle \otimes \langle k| \tag{24}$$

with the probabilities

$$\tilde{P}_k = \sum_{n=0}^{\infty} \frac{|\lambda|^{2n}}{n!^2 I_0(2|\lambda|)} \frac{|\lambda(n)|^{2k}}{k!^2 I_0(2|\lambda(n)|)}. \tag{25}$$

The change in the probability distribution of a state can be easily determined by Bob by comparing the Mandel parameter of the derived beam with the expected value of this parameter. The success of the cloning can be evaluated by calculating the distance between the derived and expected density matrices. The corresponding plots which demonstrate the dependence of these parameters on the source intensity are presented in Fig. 7.

It is easy to see that the attempts to clone a state change the Mandel parameter. Moreover, the density matrix of a cloned state is different from that of the original state even under condition of the optimum strategy of cloning. Thus, an intercepting attack with the cloning of a state on the channel which is based on a TMCC-beam can be registered and therefore is not efficient.

5. Conclusions

Coherently correlated two-mode states of a laser emission (TMCC-states), which are strongly correlated eigenstates of a product of quantum operators of annihilation of modes, manifest some specific peoperties. The relevant beams are characterized by the sub-Poisson statistics, which can help to experimentally identify these states.

Each mode of a TMCC-state is not coherent separately by itself, but the modes are mutually coherent, which causes a full correlation between the independent observables of both modes. This correlation manifests itself in that the measurements give non only the average values of the numbers of photons in both modes, but have the identical deviations from the average values. That is, the Schottky noise of a laser reveals itself identically in both modes. This allows one to use a TMCC-source for the generation and to apply TMCC-beams to the transmission of a secret key to the two mutually remote observers.

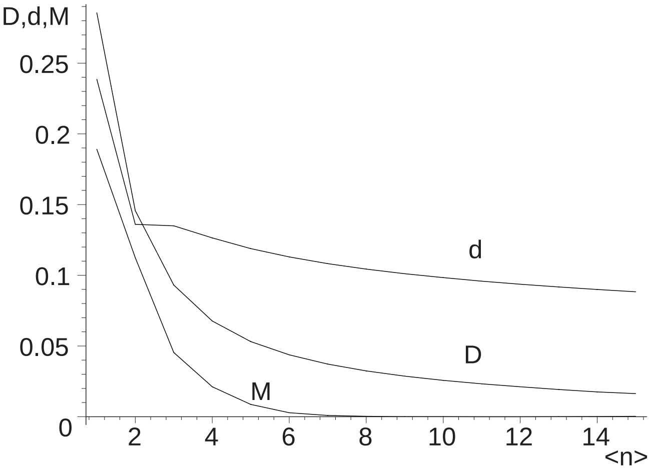

Fig. 7. Mandel parameter of a cloned state (M) and the distances between the density matrices of the cloned and expected states by the Hilbert-Schmidt (D) and weak (d) norms vs the intensity of the initial source

As distinct from the realizations of one-photon or several-photon schemes with a great number of noninformational pulses, every pulse in a TMCC-channel contains some information, which leads to a significant enhancement of the effective rate of transmission of a key.

The analysis of the channel seciruty shows that it is resistant against the ordinary interception with the splitting of a beam, as well as against the cloning of a state.

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* // Rev. Mod. Phys. **74**, 145—195 (2002); arxiv.org/quant-ph/0101098 (2002).

2. *Christandl M., Renner R., Ekert A.* // quant-ph/0402131 (2004.)

3. *Gisin N., Brunner N.* // quant-ph/0312011 (2003).

4. *Bell J.S.* // Rev. Mod. Phys. **38**, 447—452 (1964).

5. *Perelomov A.M.* Generalized Coherent States and Their Applications. — Moscow: Nauka,1987 (in Russian).

6. *Bennett C.H., Brassard G.* // IEEE Conf. Proc. Bangalore, India, 175—179 (1984).

7. *Ekert A.* // Phys. Rev. Lett. **67**, 661 (1991).

8. *Aspect A., Grangier P., Roger G.* // Ibid. **49**, 91—94 (1982).

9. *Freedman S.J., Clauser J.F.* // Ibid. **28**, 938 (1972).

10. *Bennett C.H.* // Ibid. **68**, 3121—3124 (1992).

11. *Naik D.S., Peterson C.G., White A.G. et al.* // Ibid. **84**, 4733 (2000).

12. *Jennewein T., Simon C., Weihs G. et al.* // Ibid., 4729 (2000).

13. *Tittel W., Weihs G.* // QIC, **1**(2), 3—56 (2001); quant-ph/0107156 (2001).

14. *Hong C.K., Mandel L.* // Phys. Rev. Lett. **56**, 58—60 (1986).

15. *Usenko V.C., Usenko C.V.* // J. Russian Laser Research **25**, 361 (2004); quant-ph/0403112 (2004).

16. *Usenko V.C., Usenko C.V.* // Proc. Intern. Conf. on Quantum Communication, Measurement and Computing, Glasgow, UK, 2004, p. 319; quant-ph/0407175 (2004).

17. *Wooters W.K., Zurek W.H.* // Nature, **299**, 802—803 (1982).

18. *Lütkenhaus N.* // Phys. Rev. A, **61**, 052304 (2000).

19. *Funk A.C., Raymer M. G.* // quant-ph/0109071 (2001).

20. *Laurat J., Coudreau T., Treps N. et al.* // Phys. Rev. Lett. **91**, 213601 (2003); quant-ph/0304111 (2003).

21. *Hayasaka K., Zhang Y., Kasai K.* // Opt. Lett., **29**, 14, 1665—1667 (2004); quant-ph/0406113 (2004).

Received 22.12.04.
Translated from Ukrainian by V.V. Kukhtin

КОГЕРЕНТНО-КОРЕЛЬОВАНІ ПРОМЕНІ ТА ЇХ ЗАСТОСУВАННЯ В КВАНТОВИХ КОМУНІКАЦІЯХ

В. К. Усенко, К. В. Усенко, Б.І. Лев

Резюме

Описано статистичні властивості двомодових когерентно-корельованих станів лазерного променя та можливість застосування цих станів для побудови захищених квантових каналів. Проведено аналіз стабільності та захищеності відповідного квантово-криптографічного протоколу.