Quantum cryptography is a technology allowing two distant parties to share a random string of bits, called the encryption key, composed of a large number of digits. The key is used to encrypt and decrypt messages to be transmitted between these two parties. The security of the key is guaranteed by properties of quantum mechanics. 

The basic idea is to encode the key as a series of quantum states, which are then sent over a quantum channel. The receiver can verify the integrity of the key by checking whether the states were correctly transmitted. If the states are not correctly transmitted, the key is discarded, and the process is repeated. This way, the key generation is performed securely, without the need for a trusted channel.
Eve can exploit different strategies for individual eavesdropping, e.g., the simple intercept-resend strategy, where she intercepts a qubit, measures it in a random basis and resends to Bob a qubit, prepared in the measured state. In this way Eve gains some information in exchange to disturbance introduced into Bob’s key. In order not to be detected, Eve is interested in increasing her information and decreasing the Bob’s disturbance. The best known at present strategy for that end is the asymmetric cloning of qubit [6, 7, 8]. In this type of attack Eve attaches to the Alice’s qubit two additional qubits denoted $E$ and $M$, and performs a unitary transformation of all three qubits, and sends the first qubit further to Bob, keeping the other two. After the disclosure of bases used by Alice and Bob, Eve measures her two qubits in the basis chosen by Alice. The cloning transformation, written in “correct” basis, is [6]:

$$\left| \psi_k \right\rangle_A \rightarrow \left| \psi_k \right\rangle_B \left( \frac{\alpha}{\sqrt{2}} (|0\rangle_E |0\rangle_M + |1\rangle_E |1\rangle_M) \right) \quad (3)$$

$$+ \frac{\beta}{\sqrt{2}} \left| \psi_{k+1}\right\rangle_B \left| \psi_{k+1}\right\rangle_M$$

where the two states of the basis are denoted as $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$, and the summation in index is taken modulo 2. The real positive numbers $\alpha$ and $\beta$ are parameters of the cloning machine, they satisfy the relation

$$\alpha^2 + \alpha \beta + \beta^2 = 1. \quad (4)$$

The first term in the r.h.s. of Eq. (3) corresponds to Bob having no error, while the second term corresponds to a flip of Bob’s qubit. After the measurement of her qubits Eve accepts the value of the measurement of qubit $E$ as the corresponding bit in the eavesdropped key. There are three possible outcomes of measurements by Eve and Bob of the state described by Eq. (3): (i) Eve and Bob receive correct values of Alice’s bit with probability $p_0 = (\alpha + \beta)^2 / 2$; (ii) Bob receives the correct value, but Eve receives the incorrect one with probability $p_e = \alpha^2 / 2$; and, finally, (iii) Bob receives the incorrect value, while Eve receives the correct one with probability $p_0 = \beta^2 / 2$. Bob in no way can guess which of the cases takes place (without revealing his bit to Alice). In the meanwhile, Eve can distinguish first two cases from the third one by comparing the outcomes of measurements of her two qubits $E$ and $M$. Let us denote the difference (modulo 2) of these outcomes as $m$. If the outcomes coincide ($m = 0$), then the first or the second case occurs, if they differ ($m = 1$), then the third one takes place. Given $m = 0$ Eve’s probability to get the correct value is $q = p_0 / (p_0 + p_e)$. On the basis of these probabilities one can calculate information got by Bob and Eve. We perform this calculation for keys composed from 2-valued symbols.

First we consider the case of $n = 2$. In this case two qubits are used for sending a 4-valued symbol (quart). Eve clones each qubit separately, measures her qubits in correct basis and keeps the values of $E$ qubits for her key. Besides she calculates differences of outcomes of measuring her qubits $E$ and $M - m_1$ for the first qubit and $m_2$ for the second one. Four possible cases should be distinguished depending on the values of $m_1$ and $m_2$. Let us suppose, without loss of generality, that the value 00 was sent by Alice. Then the four cases are as follows.

For $m_1 = m_2 = 0$, which happens with probability $\xi_{00} = (p_0 + p_e)^2$, the distribution of Eve’s quart is $P_{E}^{(00)} = (q, q(1 - q), q(1 - q), (1 - q)^2)$, while that of Bob’s one is $P_{B}^{(00)} = (1, 0, 0, 0)$. Here we write the distribution in the vector form $(p_{00}, p_{01}, p_{10}, p_{11})$, where $p_{ij}$ denotes the probability for quart to have value $ij$ in binary notation.

Similarly, for $m_1 = 0, m_2 = 1$ (first bit being the major one), which happens with probability $\xi_{01} = p_0 (p_0 + p_e)$, we have $P_{E}^{(01)} = (q, 0, 1 - q, 0), P_{B}^{(01)} = (0, 1, 0, 0)$.

And, finally, for $m_1 = m_2 = 1$, which happens with probability $\xi_{11} = p_0^2$, we have $P_{E}^{(11)} = (1, 0, 0, 0), P_{B}^{(11)} = (0, 0, 0, 1)$.

Now we are ready to calculate the information on Alice’s quart received by Bob and Eve. This information is calculated as $I = 2 - H(P)$, where $H(P)$ is the Shannon entropy function calculated for the distribution $P$:

$$H(P) = - \sum_{i,j=0,1} p_{ij} \log_2 p_{ij}. \quad (5)$$

However, averaging over $m_1$ and $m_2$ is performed differently for Bob and Eve. Bob does not know the values of $m_1$ and $m_2$, and therefore for him the average distribution $\langle P_B \rangle = \sum \xi_{ij} P_{ij}^{(ij)}$ is found first, and then the information for this distribution is calculated $I_B = 2 - H(\langle P_B \rangle)$. Eve, on the contrary, knows the values of $m_1$ and $m_2$ and her information is calculated for each case and then averaged: $I_E = 2 - H(\langle P_E \rangle)$. In this way we obtain

$$\langle P_B \rangle = \left( (1 - p_0)^2, p_0(1 - p_0), p_0(1 - p_0), p_0^2 \right), \quad (6)$$

$$I_B = 2 - 2h(p_0), \quad (7)$$

$$I_E = 2 - 2h(q)(1 - p_0). \quad (8)$$

where $h(q) \equiv -q \log_2 q - (1 - q) \log_2 (1 - q)$. Informations of Bob and Eve are exactly twice that for the case of bits, as could be expected. If one considers the dependence of $I_B$ and $I_E$ from $p_0$ (note that $q$ can be expressed through $p_e$, using Eq. (4)), one finds that $I_E$ decreases with $p_0$ while $I_B$ increases. The intersection of two curves defines the border value of $p_0$, below which Bob’s information exceeds Eve’s one and therefore the standard procedure of privacy amplification if applicable. This value is the solution of equation

$$2 - 2h(p_0) = 2 - 2h(q)(1 - p_0). \quad (9)$$
and is the same as for the 6-state protocol for quantum cryptography with qubits, \( p_0 = 0.1564 \). In the case of generating binary key \( p_0 \) has the sense of disturbance, i.e. probability for Bob to get incorrect symbol in his key. In the case of cryptography with quarts, considered here, the intersection of two curves occurs at the same value of \( p_0 \), but the border disturbance is now \( D^{(4)} = 1 - (1 - p_0)^2 = 0.2883 \). The growth of disturbance reflects the fact that an incorrect quart can be received when only one bit is wrong and another one is correct. This point was mentioned in Ref. [11], but did not deserve a detailed consideration up to now.

The considered cryptographic protocol for generating a key consisting from quart or, be compared to the protocol where 5 mutually unbiased bases in four-dimensional Hilbert space are used [6, 7, 8]. In the latter protocol Alice and Bob use for encoding such bases that the overlap of two any states from different bases is the same. The rest of the protocol resembles BB84. The use of mutually unbiased bases guarantees that no information on the encoded symbol is got if an incorrect basis is chosen for measurement. Therefore the protocol implementing such bases should provide the best security for cryptography with quarts. The analysis of eavesdropping by means of asymmetric cloning of quarts shows that in this case [6, 7]

\[
\langle P_B \rangle = (1 - D, D/3, D/3, D/3),
\]

\[
I_B = 2 + (1 - D) \log_2 (1 - D) + D \log_2 D \frac{D}{3},
\]

\[
I_E = 2 + (1 - D)(1 - \mu) \log_2 (1 - \mu) + (1 - D) \mu \log_2 \frac{\mu}{3},
\]

where \( \mu = D_E / (1 - D) \), \( D \) and \( D_E \) being Bob’s and Eve’s disturbances respectively, connected by the following parametric relations: \( D_E = 3 \hat{\alpha}^2 / 4, D = 3 \hat{\beta}^2 / 4 \), where \( \hat{\alpha} \) and \( \hat{\beta} \) are real positive parameters of the cloning machine for four-level quantum systems, satisfying the normalization relation

\[
\hat{\alpha}^2 + \frac{1}{2} \hat{\alpha} \hat{\beta} + \hat{\beta}^2 = 1.
\]

The solution of equation \( I_B = I_E \) in this case gives the result \( D^{(4)} = 0.2666 \). We see that \( D^{(3)} < D^{(4)} \), that is the cryptographic protocol exploiting quart pairs for generating a key of quarts is more secure against eavesdropping attacks, than the protocol, utilizing four-level systems prepared in one of 5 mutually unbiased bases. Besides, the former protocol provides higher key generation rate, since 1/3 of systems is used for the key, against 1/5 in the latter case.

This result is easily generalized to any value of \( n \). If a sequence of \( n \) quarts is used for generating a key of \( 2^n \)-valued symbols, then Bob’s disturbance corresponding to intersection of informational curves for Bob and Eve is \( D^{(2^n)} = 1 - (1 - p_0)^n \). The corresponding disturbance \( D^{(2^n)} \) for the case where \( 2^n \)-dimensional systems are used, being prepared in a state chosen from \( 2^n + 1 \) mutually unbiased bases, is calculated as a solution of equation \( I_B = I_E \) where [6, 7]

\[
I_B = n + (1 - D) \log_2 (1 - D) + D \log_2 D \frac{D}{2^n - 1},
\]

\[
I_E = n + (1 - D)(1 - \mu) \log_2 (1 - \mu) + (1 - D) \mu \log_2 \frac{\mu}{2^n - 1},
\]

where again \( \mu = D_E / (1 - D) \), but this time \( D \) and \( D_E \) are connected by equations \( D_E = (1 - 2^{-n}) \hat{\alpha}^2, D = (1 - 2^{-n}) \hat{\beta}^2 \), where

\[
\hat{\alpha}^2 + \frac{1}{2^{n-1}} \hat{\alpha} \hat{\beta} + \hat{\beta}^2 = 1.
\]

The both disturbances \( D^{(2^n)} \) and \( D^{(2^n)} \), calculated numerically, are plotted in Fig. 1 as functions of \( n \). The plot shows, that \( D^{(2^n)} \) is always greater than \( D^{(2^n)} \), i.e. a protocol based on quarts is more secure than that based on quarts. Note that for symbols with more than two values the disturbance is not limited by 1/2.

![Fig. 1](image)

The border disturbance for sharing a key composed from \( 2^n \)-valued symbols, using qubits (crosses) and \( 2^n \)-level systems (circles).

One could conjecture that a sequence of qubits encoding one quart could be effectively eavesdropped by a collective attack. But this is not so, since any collective attack produces correlation between attacked qubits, and therefore can be easily detected by Bob. Undetectable collective attack should address randomly chosen quarts, i.e. it may to be expected to be equally successful for quarts and quarts. Moreover, it is still unclear at present, if collective attacks are more effective than individual ones [3].

We conclude that the optimal dimensionality for quantum cryptography is 2, i.e. two-dimensional systems are the best tool for information encoding, like in the classical information theory. This result leads us to two practical
recommendations concerning implementation of quantum cryptography. First, if one has two-level systems available for quantum cryptography, there is no sense in entangling them for producing systems of higher dimensions. Second, if one has multilevel systems at hand, it is more profitable to decompose the states of each system into direct product of two-dimensional spaces and use them for standard cryptographic protocol with qubits. This strategy provides better security and better key generation rate.

Authors gratefully acknowledge support from INTAS, Open call 2001 project 2097 and from Belorussian Republican Foundation for Fundamental Research.