UDC 003.26:621.39:530.145

Gnatyuk S.O., Kinzeryavyy V.M., Zhmurko T.O.

EFFICIENCY INCREASING OF THE QUANTUM CRYPTOGRAPHY SYSTEMS BASED ON THE PING-PONG PROTOCOL

In this paper the efficiency problems of quantum secure direct communication protocols were describes. The calculation of intercepted information by unauthorized user`s attack on quantum cryptography system (based on ping-pong protocol with pair of entangled qudits) carried out. Two methods of security amplification for quantum cryptography systems were also analyzed. The tests for assessment randomness level of ternary sequences were proposed for their more effective applying in modern quantum technologies of information security.

Keywords: quantum cryptography, ping-pong protocol, privacy amplification, ternary pseudorandom sequence, statistical tests, efficiency.

Introduction. The main features of information security (IS) are confidentiality, integrity and availability (named CIA-model) [1]. Only providing these all gives availability for development secure information and communication systems. Confidentiality is the basic feature of IS, which ensures that information is accessible only to authorized users who have an access. Integrity is the basic feature of IS indicating its property to resist unauthorized modification. Availability is the basic feature of IS that indicates accessible and usable upon demand by an authorized entity. One of the most effective ways to ensure confidentiality and data integrity during transmission is cryptographic systems. The purpose of such systems is to provide key distribution, authentication, legitimate users authorization and encryption. Key distribution is one of the most important problems of cryptography. This problem can be solved with the help of such methods [1-2]: a) Classical information-theoretic cryptography schemes; b) Classical public-key cryptography schemes; c) Classical computationally secure symmetric-key cryptographic schemes; d) Trusted Couriers key distribution; e) Quantum key distribution (QKD) [1-3]. The main advantage of last method is information-theoretic security. No one classical method gives that possibility. That’s why IS systems using QKD are very effective and prospect. According to [2] QKD includes the following protocols: protocols using single (non-entangled) qubits (two-level quantum systems) and qudits (d-level quantum systems, d >2), protocols using entangled states, decoy states and some other protocols. Well-known and proven fact [1, 3] than QKD protocols can generally provide higher information security level than appropriate classical cryptographic schemes.

Quantum technologies of information security and its efficiency problems. There are many others quantum technologies of IS but in practice they have not been extended beyond laboratory experiments yet. Despite this, some of them provide high information security level up to the information-theoretic security. For example, quantum secure direct communication (QSDC) protocols remove the secret key distribution problem because they do not use encryption. One of these is the ping-pong protocol [1, 4] and its improved versions. This protocol does not require qubit transfer by blocks. In its first variant entangled pairs of qubits and two coding operations that allow the transmission of one bit of classical information for one cycle of the protocol are used in [4]. The usage of quantum superdense coding allows transmitting two bits for a cycle. The subsequent increase in the informational capacity of the protocol is possible by the usage instead of entangled pairs of qubits their triplets, quadruplets etc. in Greenberger-Horne-Zeilinger (GHZ) states. The informational capacity of the ping-pong protocol with GHZ-states is equal to n bits on a cycle where n is the number of entangled qubits. Another way of increasing the informational capacity of ping-pong protocol is using entangled states of qudits. Thus, the corresponding protocol based on Bell’s states of three-level quantum system (qutrit) pairs and superdense coding for qutrits is introduced in [4].

The advantages of QSDC protocols are a lack of secret key distribution, the possibility of data transfer between more than two parties, and the possibility of attack detection providing a high level of information security (up to information-theoretic security) for the protocols using block transfer. The main disadvantages are difficulty in practical realisation of protocols using entangled states (and especially protocols using entangled states for *d*-level quantum systems), slow transfer rate, the need for large capacity quantum memory for all parties (for protocols using block transfer of qubits), and the asymptotic security of the ping-pong protocol. Asymptotic security of the ping-pong protocol (which is one of the simplest QSDC protocols from the technical viewpoint) can be amplified by using methods of classical cryptography. The main task of this paper is searching methods of the efficiency increasing for quantum cryptography systems based on QSDC.

Attacks on the ping-pong protocol. Eve's (violator, unauthorized user – legal authorized users will be Alice & Bob) information at attack with usage of auxiliary quantum systems (probes) on the ping-pong protocol with entangled *n*-qubit GHZ-states is defined by von Neumann entropy [1]:

$$I_0 = S(\rho) \equiv -Tr\{\rho \log_2 \rho\} = -\sum_i \lambda_i \log_2 \lambda_i, \tag{1}$$

where λ_i are the density matrix eigenvalues for the composite quantum system «transmitted qubits - Eve's probe».

For the protocol with Bell pairs and quantum superdence coding the density matrix ρ have size 4x4 and four nonzero eigenvalues:

$$\begin{aligned} \lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16 p_1 p_2 d(1-d)}, \\ \lambda_{3,4} &= \frac{1}{2}(p_3+p_4) \pm \frac{1}{2}\sqrt{(p_3+p_4)^2 - 16 p_3 p_4 d(1-d)}. \end{aligned} \tag{2}$$

For the protocol with GHZ-triplets a density matrix size is 16x16, and a number of nonzero eigenvalues is equal to eight. At symmetrical attack, their kind is [1]:

$$\begin{aligned} \lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16 p_1 p_2 \cdot \frac{2}{3} d\left(1-\frac{2}{3}d\right)}, \\ \lambda_{7,8} &= \frac{1}{2}(p_7+p_8) \pm \frac{1}{2}\sqrt{(p_7+p_8)^2 - 16 p_7 p_8 \cdot \frac{2}{3} d\left(1-\frac{2}{3}d\right)}. \end{aligned} \tag{3}$$

For the protocol with *n*-qubit GHZ-states, the number of nonzero eigenvalues of density matrix is equal to 2^n, and their kind at symmetrical attack is [6]:

$$\begin{aligned} \lambda_{1,2} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16 p_1 p_2 \cdot \frac{2^{n-2}}{2^{n-1}-1} d\left(1-\frac{2^{n-2}}{2^{n-1}-1}d\right)}, \\ \lambda_{2^n-1,2^n} &= \frac{1}{2}\left(p_{2^n-1}+p_{2^n}\right) \pm \frac{1}{2}\sqrt{\left(p_{2^n-1}+p_{2^n}\right)^2 - 16 p_{2^n-1} p_{2^n} \cdot \frac{2^{n-2}}{2^{n-1}-1} d\left(1-\frac{2^{n-2}}{2^{n-1}-1}d\right)}, \end{aligned} \tag{4}$$

where *d* is probability of attack detection by legitimate users at one-time switching to control mode; p_i are frequencies of *n*-grams in the transmitted message.

The probability of that Eve will not be detected after *m* successful attacks and will gain information $I = mI_0$ is defined by the equation [7]:

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)}\right)^{I/I_0}, \tag{5}$$

where *q* is a probability of switching to control mode.

In fig. 1 dependences of $s(I,q,d)$ for several *n*, identical frequencies $p_i = 2^{-n}$, *q* = 0.5 and $d = d_{\max}$ are shown [6]. $d_{\max}$ is maximum probability of attack detection at one-time run of control mode, defined as

$$d_{\max} = 1 - \frac{1}{2^{n-1}}. \tag{6}$$

At $d = d_{\max}$ Eve gains the complete information about transmitted bits of the message. It is obvious from fig. 2 that the ping-pong protocol with many-qubit GHZ-states is asymptotically secure at any number *n* of qubits that are in entangled GHZ-states. A similar result for the ping-pong protocol using qutrit pairs is presented [4].

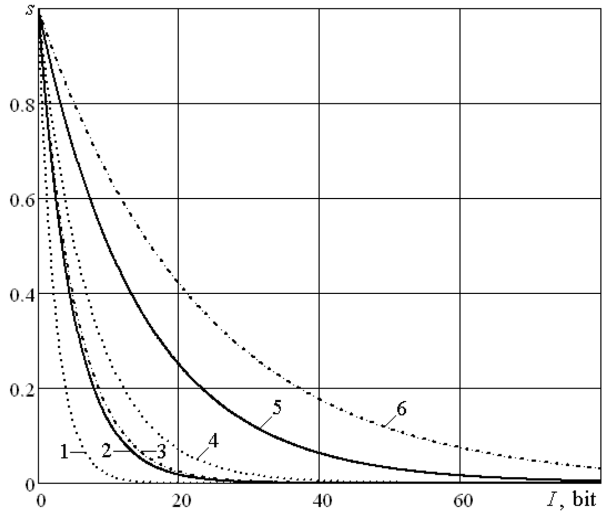


Fig. 1. Composite probability of attack non-detection s for the ping-pong protocol with many-qubit GHZ-states: n=2, original protocol (1); n=2, with superdense coding (2); n=3 (3); n=5 (4); n=10 (5); n=16 (6). I is Eve's information

Privacy amplification. A *non-quantum method of security amplification for the ping-pong protocol* is suggested in [6]. Such method has been developed on the basis of a method of privacy amplification which is utilized in quantum key distribution protocols. In case of the ping-pong protocol this method can be some kind of analogy of the Hill cipher. Before the transmission Alice divides the binary message on *l* blocks of some fixed length *r*, we will designate these blocks as a_i (*i*=1,…*l*). Then Alice generates for each block separately random invertible binary matrix K_i of size $r \times r$ and multiplies these matrices by appropriate blocks of the message (multiplication is performed by modulo 2):

$$b_i = K_i \cdot a_i. \tag{7}$$

Blocks b_i are transmitted on the quantum channel with the use of the ping-pong protocol. Even if Eve, remained undetected, manages to intercept one (or more) from these blocks and without knowledge of used matrices K_i Eve won't be able to reconstruct source blocks a_i. To reach a sufficient security level the block length *r* and accordingly the size of matrices K_i should be selected so that Eve's undetection probability *s* after transmission of *one* block would be insignificant small. Matrices K_i are transmitted to Bob via usual (non-quantum) open authentic channel after the end of quantum transmission but only in the event when Alice and Bob were convinced lack of eavesdropping. Then Bob inverses the received matrices and having multiplied them on appropriate blocks b_i he gains an original message. Let's mark that described procedure is not message enciphering, and can be named inverse hashing or hashing using two-way hash function, which role random invertible binary matrix acts. It is necessary for each block to use individual matrix K_i which will allow to prevent cryptoanalytic attacks, similar to attacks to the Hill cipher, which are possible there at a multiple usage of one matrix for enciphering of several blocks (Eve could perform similar attack if she was able before a detection of her operations in the quantum channel to intercept several blocks, that are hashing with the same matrix). As matrices in this case are not a key and they can be transmitted on the open classical channel, the transmission of the necessary number of matrices is not a problem. Necessary length *r* of blocks for hashing and accordingly necessary size $r \times r$ of hashing matrices should correspond to a requirement $r > I$, where I is the information which is gained by Eve. Thus, it is necessary for determination of r to calculate I at the given values of n, s, q and $d = d_{\max}$. Let's accept $s(I,q,d) = 10^{-k}$, then:

$$I = \frac{-kI_0}{\lg\left(\dfrac{1-q}{1-q(1-d)}\right)}. \qquad (8)$$

The calculated values of I are shown in tab. 1:

Eve's information I at attack on the ping-pong protocol with n-qubit GHZ-states at $s = 10^{-6}$ (bit)

Table 1

n	$q = 0{,}5$; $d = d_{\max}$	$q = 0{,}5$; $d = d_{\max}/2$	$q = 0{,}25$; $d = d_{\max}$	$q = 0{,}25$; $d = d_{\max}/2$
2	69	113	180	313
3	74	122	186	330
4	88	145	216	387
5	105	173	254	458
6	123	204	297	537
7	142	236	341	620
8	161	268	387	706
9	180	302	434	793
10	200	335	481	881
11	220	369	529	970
12	240	403	577	1059
13	260	437	625	1149
14	279	471	673	1238
15	299	505	721	1328
16	319	539	769	1417
17	339	573	817	1507
18	359	607	865	1597
19	379	641	913	1686
20	399	675	961	1776

Thus, after transfer of hashed block, the lengths of which are presented in tab. 1, the probability of attack non-detection will be equal to 10^{-6}; there is thus a very high probability that this attack will be detected. The main disadvantage of the ping-pong protocol, namely its asymptotic security against eavesdropping attack using ancilla states, is therefore removed.

Other similar method of privacy amplification of the ping-pong protocol was proposed in paper [8]. In this method in place of matrix K_i of size $r \times r$ the key ternary (trit) sequence k_i of size r using was proposed. The message will be calculated by the equation $b_i = k_i + a_i$, where $a_i = b_i - k_i$ («+» & «–» are operations of trit addition and subtraction by modulo 3). Key ternary sequence k_i will be formed by means of ternary pseudorandom generator and 96-trit one-time key. The trit key (instead matrices K_i) are transmitted to Bob via usual (non-quantum) open channel after the end of quantum transmission but only in the event when Alice and Bob were convinced lack of eavesdropping. Using of this method can increase the security of pong-pong protocol and its work rate at least 3 times than mentioned method [6].

Assessment of randomness for ternary sequences in quantum cryptography. Randomness is very significant in providing IS. Random (pseudorandom) sequences are applying anyway in every security system. However, binary random sequences are studied at a high level. Nevertheless, ternary or trinary sequences (by analogy to a bit, although it contains «0», «1», «2»), which is more advisable to use in QC protocols (particularly in mentioned ping-pong protocol), are badly highlighted. Besides, the existence of the assessment tool is low-to-nonexistent. Therefore, methods of assessing ternary pseudorandom sequence need to be considered. For today, exists a number of different valuation techniques for binary pseudorandom sequences, for example: graphics tests; NIST statistical test suite; methods of testing RIPE; methods of testing FIPS 140-2 (NIST PUB FIPS 140-2); methods of D. Knuth; statistical tests DIEHARD; CRYPT-S etc. However, in the analyses of these techniques there is no possibility to estimate the ternary pseudorandom sequences. These tests have been developed in [9]. Before evaluating, first necessary to form a pseudorandom ternary sequence (fig. 2). Accordingly, generator of such sequence was developed and detailed description of it is represented in paper [8]. Let's consider the tests proposed in [9].

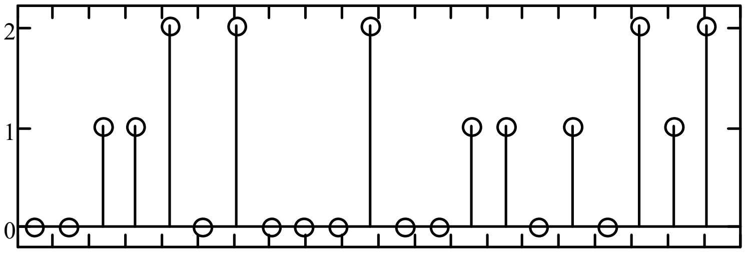
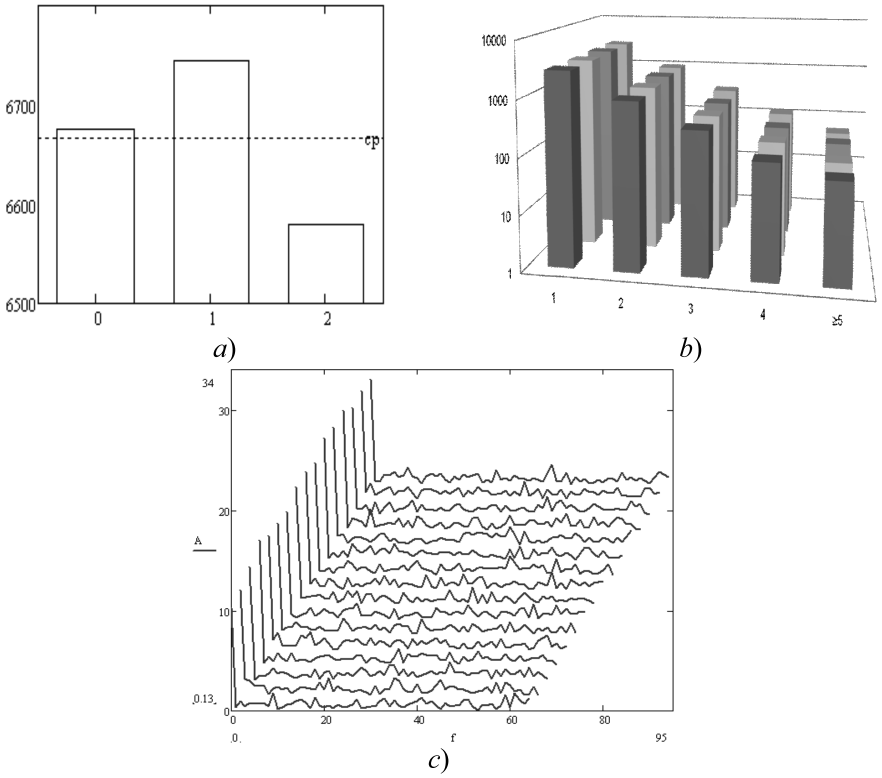


Fig. 2. Graphical view of the ternary pseudorandom sequence

Frequency test. This test carries a proportionate assessment of «0», «1» and «2» (for unbalanced ternary sequence). Specifies whether the number of zeros, ones and twos in the sequence is about the same as in really random in sequence. The result of this test is a histogram of occurrences of zeros, ones and twos in trit sequence shown in fig. 3 a and a report in the form of a table that contains the frequency of occurrence and the deviation the average value.



a)

b)

c)

Fig. 3. Histograms of statistical tests: frequency (a), series (b) & spectral (c)

Assessment series test. Attention in this test focused on the total number of episodes in the entire sequence. The purpose of the test to determine whether the total number of runs of ones, twos and zeros of various lengths is such that expected from a random sequence (fig. 3 b). In the particular case of this test determines whether the oscillations between zeros, ones and twos units are very fast or very slow.

Spectral tests. For searching periodicities in ternary sequences obtained spectrum using FFT on samples from the generated sequence (fig. 3 c).

Other tests are in development now and authors will be informed about them in their future papers in this series.

Conclusion. Accordingly, in this paper the efficiency problems of quantum cryptography (QSDC protocols) were describes. The calculation of intercepted information (quantity) by unauthorized user`s attack on quantum cryptography system (based on ping-pong protocol with pairs of entangled qudits) carried out. In addition, two known methods of security amplification for quantum cryptography systems based on QSDC were analyzed. Besides the tests for assessment randomness level of ternary sequences were proposed in the paper. This results will be interesting for IS experts for assessment security level of QC (QKD & QSDC) systems.

Future researches can be related to organization of effective ternary pseudorandom generator and full suite of statistical tests for trits.

REFERENCES

1. Quantum secure telecommunication systems / [Oleksandr Korchenko, Petro Vorobiyenko, Maksym Lutskiy, Yevhen Vasiliu, Sergiy Gnatyuk] // Telecommunications Networks: Current Status and Future Trends / edited by Jesus Hamilton Ortiz. - Rijeka, Croatia: InTech, 2012, pp. 211-236.
2. Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Ye. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika, 2010, V. 14, № 2, pp. 58-69.
3. Korchenko O. Modern directions of quantum cryptography / O. Korchenko, E. Vasiliu, S. Gnatyuk // «AVIATION IN THE XXI-st CENTURY» - «Safety in Aviation and Space Technologies»: IV World Congress: Proceedings, September 21-23, Kyiv, NAU, 2010, pp. 17.1-17.4.
4. Vasiliu Ye.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits // Quantum Information Processing, 2011, V. 10, №. 2, pp 189-202.
5. Gnatyuk S.O. Assessment of randomness for ternary sequences in quantum cryptography / S.O. Gnatyuk, T.O. Zhmurko // «AVIATION IN THE XXI-st CENTURY» - «Safety in Aviation and Space Technologies»: V World Congress: Proceedings, September 25-27, Kyiv, NAU, 2012, pp. 17.2-17.5.
6. Vasiliu Ye.V. Synthesis of the secure system of direct message transfer based on the ping-pong protocol of quantum communication / Vasiliu Ye.V., Nikolaenko, S.V. // Scientific works of the Odessa national academy of telecommunications named after O.S. Popov, 2009, №1, pp. 83-91.
7. Boström K., Felbinger T. Deterministic secure direct communication using entanglement, Physical Review Letters, 2002, - Vol.89, №18. - 187902.
8. Кінзерявий В.М. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів // Кінзерявий В.М., Васіліу Є.В., Гнатюк С.О., Жмурко Т.О. / Захист інформації. - №2 (55). - 2012. - С. 79-87.
9. Гнатюк С.О. Метод генерування та оцінки випадкових послідовностей для кутритових систем квантового прямого безпечного зв'язку / С.О. Гнатюк, Т.О. Жмурко // Безпека інформаційних технологій (ITSEC-2012): II наук.-техн. конф.: Збірник тез. - К.: НАУ, 2012. - С. 16-17.

Надійшла: 12.08.2012р.

Рецензент: д.т.н., проф. Дудикевич М.М.