КРИПТОГРАФІЯ / CRYPTOGRAPHY

SECURITY AMPLIFICATION OF THE PING-PONG PROTOCOL WITH MANY-QUBIT GREENBERGER-HORNE-ZEILINGER STATES

Yevhen Vasiliu[1], Sergiy Gnatyuk[2], Sergiy Nikolaenko[1], Tetyana Zhmurko[2]

[1]Odesa National Academy of Telecommunications n.a. O.S. Popov
[2]National Aviation University

Yevhen V. VASILIU, Doctor of Science (DSc)

Date and place of birth: 1966, Yalta, Crimea, Ukraine.
Education: Odessa State University named after I.I. Mechnikov, 1990.
Current position & Functions: Full Professor at Automation Dept since 2012.
Research interests: quantum cryptography, quantum key distribution protocols, quantum secure direct communication, error correction coding for quantum cryptography protocols, quantum steganography.
Publications: over 100 scientific publications including papers, conference proceedings, patents.
E-mail: vasiliu@ua.fm

Sergiy O. GNATYUK, Candidate of Science (PhD)

Date and place of birth: 1985, Netishyn, Khmelnytskyi Oblast, Ukraine.
Education: National Aviation University, 2007.
Current position & Functions: Associate Professor at IT-Security Dept since 2012.
Research interests: information & aviation security, quantum cryptography, information security incident management, cyber threats to international civil aviation.
Publications: over 90 scientific publications including monograph, papers in domestic & foreign scientific journals, international conferences proceedings, patents & certificates of copyright registration etc.
E-mail: s.gnatyuk@nau.edu.ua

Sergiy V. NIKOLAYENKO

Date and place of birth: 1983, Odessa, Ukraine.
Education: Odessa National Academy of Telecommunications named after O.S. Popov, 2005.
Current position & Functions: Lecturer at IT Dept.
Research interests: quantum cryptography, quantum secure direct communication, web-programming, functional programming.
Publications: over 30 scientific publications including papers, conference proceedings, international conferences materials, patents.
E-mail: serezhanik@gmail.com

Tetiana O. ZHMURKO

Date and place of birth: 1990, Vinnitsa, Ukraine.
Education: National Aviation University, 2012.
Current position & Functions: Postgraduate student.
Research interests: quantum cryptography, cyber threats to international civil aviation.
Publications: over 10 scientific publications including papers, conference proceedings, international conferences materials, patents.
E-mail: taniazhm@gmail.com

Abstract. *In this paper the non-quantum method of security amplification for the ping-pong protocol with many-qubit entangled Greenberger-Horne-Zeilinger states (GHZ-states) is proposed. This method can be used in quantum*

cryptography and consists in invertible hashing of classical message blocks. The necessary sizes of matrices for hashing of message blocks are calculated at some values of the protocol parameters. The proposed method does not require the presence from legitimate users of any pre-established keys. Thus, the main advantage of the quantum secure direct communication protocols, namely the lack of necessity to distribute of secret key remains valid at usage of the proposed method.

Key words: *ping-pong protocol, Greenberger-Horne-Zeilinger states, qubit.*

1. Introduction

One of the modern and effective methods of information security providing based on quantum technologies is the usage of quantum secure direct communication (QSDC) protocols [1–6]. The main feature of QSDC protocols is that there are no cryptographic transformations; thus, there is no key distribution problem (very serious problem in the classical cryptography) in QSDC. In these protocols a secret message is coded by qubits (or qudits) – quantum states, which are sent via quantum channel. QSDC protocols can be divided into several types [3,4]: 1) ping-pong protocol (and its enhanced variants); 2) protocols using block transfer of entangled qubits; 3) protocols using single qubits; 4) protocols using entangled qudits.

According to [1–6] the advantages of QSDC protocols are the 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 unconditional 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 multi-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. That's why the *main goal of this paper* is developing of method to amplify asymptotic security for the ping-pong protocol.

2. Eve's information at the symmetrical attack on the ping-pong protocol with *n*-qubit GHZ-states

Eve's information at attack using auxiliary quantum systems (probes) on the ping-pong protocol is defined by von Neumann entropy [5]:

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

where λ_i are eigenvalues of the density matrix ρ 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 [6]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 d(1-d)} \quad ,$$
$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16 p_3 p_4 d(1-d)} \quad , \qquad (2)$$

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

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 [7,8]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 \cdot \frac{2}{3} d\left(1 - \frac{2}{3} d\right)} \quad ,$$
$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16 p_3 p_4 \cdot \frac{2}{3} d\left(1 - \frac{2}{3} d\right)}$$
$$\lambda_{5,6} = \frac{1}{2}(p_5 + p_6) \pm \frac{1}{2}\sqrt{(p_5 + p_6)^2 - 16 p_5 p_6 \cdot \frac{2}{3} d\left(1 - \frac{2}{3} d\right)}$$
$$\lambda_{7,8} = \frac{1}{2}(p_7 + p_8) \pm \frac{1}{2}\sqrt{(p_7 + p_8)^2 - 16 p_7 p_8 \cdot \frac{2}{3} d\left(1 - \frac{2}{3} d\right)} \quad , \qquad (3)$$

where p_i are frequencies of trigrams in the transmitted message. 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 [9]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm$$
$$\pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 \cdot \frac{2^{n-2}}{2^{n-1} - 1} d\left(1 - \frac{2^{n-2}}{2^{n-1} - 1} d\right)} \quad ,$$
$$\lambda_{2^n - 1, 2^n} = \frac{1}{2}\left(p_{2^n - 1} + p_{2^n}\right) \pm \qquad (4)$$
$$\pm \frac{1}{2}\sqrt{\left(p_{2^n - 1} + p_{2^n}\right)^2 - 16 p_{2^n - 1} p_{2^n} \cdot \frac{2^{n-2}}{2^{n-1} - 1} d\left(1 - \frac{2^{n-2}}{2^{n-1} - 1} d\right)} \quad ,$$

where 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 $I = m I_0$ is defined by the equation [1,5,7–9]:

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

where q is a probability of switching to control mode.

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

$$d_{\max} = 1 - \frac{1}{2^{n-1}} \quad . \qquad (6)$$

At $d = d_{\max}$ Eve gains the complete information about transmitted bits of the message.

It is obvious from fig. 1 that the ping-pong protocol with many-qubit GHZ-states is asymptotically secure at any number n of qubits, which are in entangled GHZ-states.

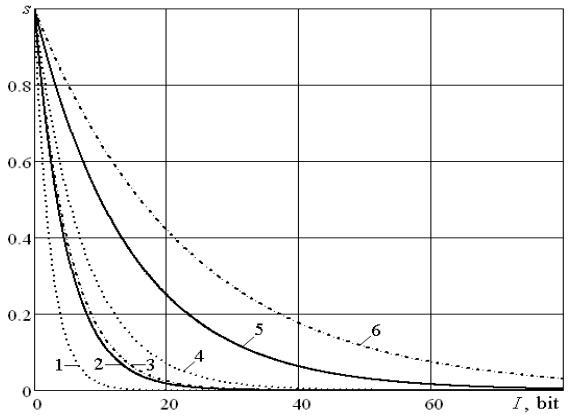

Fig. 1. The composite probability of attack undetection *s* for the ping-pong protocol with many-qubit GHZ-states: *n*=2, original protocol (1); *n*=2, with superdense coding (2); *n*=3 (3); *n*=5 (4); *n*=10 (5); *n*=16 (6). *I* is Eve's information.

3. Non-quantum method of security amplification

As follows from outcomes of the previous section, Eve can gain some information before her attack will be detected, and quantity of information grows with increase of entangled qubits number used in the protocol. Therefore, for practical usage of the protocol a method which will make the information gained by Eve useless for her is necessary. Such method can be 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 will be some analogy of the Hill cipher [10].

Before the transmission Alice divides the binary message on *l* blocks of some fixed length *r*, we will designate these blocks through 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):

$$b_i = K_i a_i . \qquad (7)$$

Blocks b_i are transmitted on the quantum channel using the ping-pong protocol. Even if Eve will manage to intercept one (or more) from these blocks remained undetected, then not knowing used matrices K_i Eve cannot reconstruct source blocks a_i . For reaching of sufficient security level the block length *r* and accordingly the size of matrices K_i should be selected so that Eve's probability of undetection *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 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 should also be noted that if the Shannon entropy of the source data block a_i is small, then multiplication by a random matrix significantly increase entropy, so the transmitted block b_i will look like a random string.

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, which 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 satisfy the condition $r > I$, where *I* is the information which is gained by Eve. In addition *r* should be multiple to number of qubits *n* that are used for protocol implementation. Thus, it is necessary for determination of *r* to calculate *I* at the given values of *n*, *s*, *q* and *d*.

Let's accept $s(I,q,d) = 10^{-k}$ and we derive Eve's information *I* from (5):

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

The calculated values of *I* are shown in tab. 1 and tab. 2.

Table 1

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

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

Table 2

Eve's information I at attack on the ping-pong protocol with n-qubit GHZ-states at $s = 10^{-4}$ (bit)

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	46	75	120	209
3	50	82	124	220
4	59	97	144	258
5	70	116	170	306
6	82	136	198	358
7	94	157	228	413
8	107	179	258	471
9	120	201	290	529
10	133	224	321	588
11	147	246	353	647
12	160	269	385	706
13	173	291	417	766
14	186	314	449	826
15	200	337	481	885
16	213	360	513	945
17	226	382	545	1005
18	240	405	577	1065
19	253	428	609	1124
20	266	450	641	1184

Fig. 2 shows the dependence of I on n and on q for $s = 10^{-4}$ and $d = d_{\max}$. We can see that for a given q the dependence of I on n is almost linear, and for a given n the dependence of I on q is exponential.

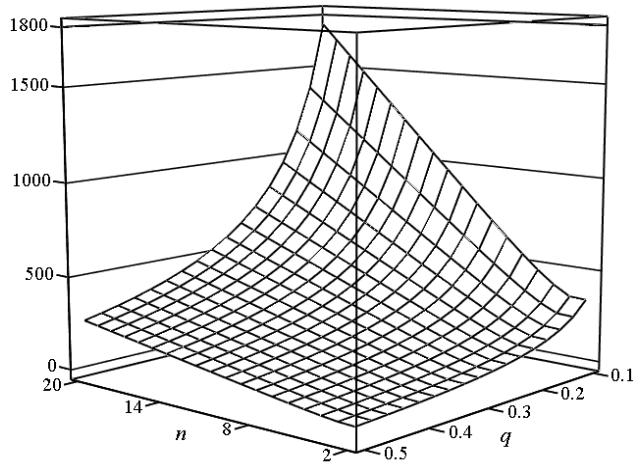

Fig. 2. Amount of Eve's information for the protocol with n-qubit GHZ-states at $s = 10^{-4}$ and $d = d_{\max}$ (bit)

It is obvious from the tab. 1 and tab. 2 that at small n the necessary size of matrices for hashing is small, but quickly enough grows with increase of n. Therefore a question arises about time which is necessary for generation and checkout on invertibility of random binary matrices. This time will be essential depending on probability of that binary matrix which generates in a random way is invertible. Such probability has been calculated by Overbey et al and for matrices on Galois field GF(2) at $r \geq 16$ becomes by a constant which equals to 0.289 [10]. Thus, on the average almost every third binary matrices that generates in a random way at $r \geq 16$ will be invertible that, in our opinion, is fully acceptable.

4. Conclusions

In this paper we have suggested non-quantum method of security amplification for the ping-pong protocol with n-qubit entangled GHZ-states. We have calculated necessary sizes of matrices for hashing of message blocks at some values of the protocol parameters and for values of n from 2 to 20. The proposed method does not require the presence from legitimate users of any pre-established keys. Matrices are not keys, and they are transmitted on the open channel if Alice and Bob were convinced that eavesdropper is absent. Thus, the main advantage of the quantum secure direct communication protocols, namely lack of necessity to distribute of keys (except for a small key for authentication) remains valid at usage of the proposed method.

References

[1] E.V. Vasiliu. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189–202.

[2] O.G. Korchenko, Ye.V. Vasiliu, S.O. Gnatyuk. Modern directions of quantum cryptography // Proceedings of the fourth world congress "Aviation in the XXI-st century" – "Safety in Aviation and Space Technologies". – Kyiv, 2010. – V. 1. – P. 17.1–17.4.

[3] O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu and S. Gnatyuk. Quantum Secure Telecommunication Systems // Telecommunications Networks – Current Status and Future Trends (Edited by J.H. Ortiz). – InTech, 2012. – P. 211–236.

[4] O. Korchenko, Ye. Vasiliu, S. Gnatyuk. Modern quantum technologies of information security against cyber-terrorist attacks // Aviation. Vilnius: Technika. – 2010. – Vol. 14, no. 2. – P. 58–69.

[5] K. Bostrom, T. Felbinger: Deterministic secure direct communication using entanglement. – Physical Review Letters. – 2002. – V. 89. – 187902.

[6] F.G. Deng, G.L. Long, X.S. Liu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block // Physical Review A. – 2003. – V. 68. – 042317.

[7] E.V. Vasiliu: Analysis of attack on the ping-pong protocol with Greenberger-Horne-Zeilinger triplets // Scientific works of the Odessa national academy of telecomm. n.a. O.S. Popov. – 2008, issue 1. – P. 15–24.

[8] E.V. Vasiliu: Asymptotic security of the ping-pong quantum direct communication protocol with three-qubit Greenberger–Horne–Zeilinger states // Georgian Electronic Scientific Journal: Comp. Sc. and Telecomm. – 2009, issue 3 (20). – P. 3–15. http://gesj.internet-academy.org.ge/gesj_articles/1427.pdf.

[9] E.V. Vasiliu, S.V. Nikolaenko: Synthesis of the secure system of direct messages transfer based on the ping-pong protocol of quantum communication //

Scientific works of the Odessa national academy of telecomm. n.a. O.S. Popov. – 2009, issue 1. – P. 83–91. http://nbuv.gov.ua/portal/natural/Nponaz/2009_1/files/20091_VasiliyNikolaenko.pdf

[10] J. Overbey, W. Traves, J. Wojdylo. On the keyspace of the Hill cipher // Cryptologia. – 2005. – V. 29. – P. 59–72.

УДК 003.26:621.39:530.145 (045)

Є.В. Василіу, С.В. Ніколаєнко, С.О. Гнатюк, Т.О. Жмурко Підсилення секретності пінг-понг протоколу з багатокубітними станами Грінбергера-Хорна-Цайлінгера

Анотація. *У даній статті представлено неквантовий метод підсилення секретності пінг-понг протоколу з багатокубітними переплутаними станами Грінбергера-Хорна-Цайлінгера (ГХЦ-станами). Даний метод може використовуватися у квантовій криптографії і полягає у оборотному хешуванні класичних блоків повідомлення. Для деяких параметрів пінг-понг протоколу розраховано необхідні розміри матриць для хешування блоків повідомлення. Запропонований метод не потребує наявності будь-яких попередньо встановлених ключів у легітимних користувачів. Таким чином, при використанні даного методу зберігається основна перевага протоколів квантового прямого безпечного зв'язку, а саме відсутність необхідності розподіляти секретні ключі.*

Ключові слова: *пінг-понг протокол, стани Грінбергера-Хорна-Цайлінгера, кубіт.*

Е.В. Василиу, С.В. Николаенко, С.А. Гнатюк, Т.А. Жмурко Усиление секретности пинг-понг протокола с багатокубитнимы состояниями Гринбергера-Хорна-Цайлингера

Аннотация. *В статье представлено неквантовий метод усиления секретности пинг-понг протокола з многокубитными перепутанными состояниями Гринбергера-Хорна-Цайлингера (ГХЦ-состояними). Данный метод может использоваться в квантовой криптографии и представляет собой обратное хеширование классических блоков сообщений. Для некоторых параметров пинг-понг протокола рассчитаны необходимые размеры матриц для хеширования блоков сообщений. Предложенный метод не требует наличия предварительно установленных ключей у легитимных пользователей. Таким образом, при использовании данного метода сохраняется главное преимущество квантовой прямой безопасной связи, а именно отсутствие потребности распределения секретных ключей.*

Ключевые слова: *пинг-понг протокол, состояния Гринбергера-Хорна-Цайлингера, кубит.*

Отримано *8 жовтня 2012 року,* затверджено редколегією *5 листопада 2012 року*
(рецензент д.т.н., професор В.М. Рудницький)