UDC 621.39:003.26

S.O. Gnatyuk, T.O. Okhrimenko (Zhmurko)
(National Aviation University, Ukraine)
B.S. Akhmetov, N.A. Seilova, Kh.I. Yubuzova
(Satbayev University, Republic of Kazakhstan)

Approach to Increase Speed for Deterministic Protocols of Quantum Cryptography

Information transferring in computer networks needs high level of security and the main way of providing it, is using the cryptographic methods and tools. However, recent research has shown that classical cryptography gives a cause to look for new outlooks and it could be quantum cryptography. Among all possible quantum cryptography technologies, quantum secure direct communication (e.g. deterministic protocol) does not use any cryptographic transformations, so there is no key distribution problem and eavesdropping can be detect during transfer, thereby improving information transmitting reliability. In this paper privacy amplification method for deterministic protocol was proposed. This method uses generated ternary pseudorandom sequence and transformations in Galois field. Accordingly, this could increase the protocol asymptotical security and accelerate its work at least 3 times.

Introduction

In recent years, quantum cryptography (QC) [1, 2] has been the object of intensive research activities and now some directions are successfully implemented in contemporary information systems. QC methods guarantee a high level of information security using the laws of quantum mechanics, such as: non-cloning theorem – impossibility duplicate an unknown quantum state; impossibility of taking a measurement without perturbing the system; impossibility simultaneously measure the polarization of a photon in the vertical-horizontal basis; simultaneously in the diagonal basis, etc., thereby providing unconditional security [2].

One of the modern and effective QC methods is using quantum secure direct communication (QSDC) protocols [3]. The main feature of QSDC protocols is that there are no cryptographic transformations; thus, there is no key distribution problem (challenge 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. In addition, the advantages of QSDC protocols are the possibility of data transfer between more than two parties, and it's possible to detect the attack during transferring [1]. QSDC protocols can be divided into several types [2]: deterministic protocol (and its enhanced variants); protocols using block transfer of entangled qubits; protocols using single qubits; protocols using entangled qudits.

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 speed, the need for large capacity quantum memory for all parties (for protocols using block transfer of qubits), and the asymptotic security of the deterministic protocol [2]. The *main objective of this paper* is developing of method to increase efficiency for QSDC protocols in the part of amplifying its asymptotic security and speed level.

Related Papers Analysis

Efficiency increasing of QSDC protocols can be directed on information capacity growing, error control providing and also security (privacy) amplification [1, 2]. The last approach is the most important and critical from viewpoint of information security. Eve (unauthorized user, eavesdropper) can gain some information before her attack (specialized cyberthreat realization [1]) will be detected, and quantity of information grows with increase of entangled qubits number used in the protocol [4]. Therefore, for practical usage of the protocol a method which will make the information gained by Eve useless for her is necessary. Such method was developed on the basis of privacy amplification method which is utilized in quantum key distribution protocols [5]. In case of the deterministic protocol this method will be some analogy of the well-known Hill cipher [2, 5].

Before the transmission Alice (legitimate authorized user, transmitter) divides the binary message on l blocks of some fixed length r, these blocks will designate as a_i (i=1,…l). Then Alice generates for each block separately random invertible binary matrix K_i size $r \times r$ and multiplies these matrices by appropriate message blocks (multiplication is performed by modulo 2): $b_i = K_i \cdot a_i$.

Blocks b_i are transmitted using the quantum channel, by applying deterministic protocol. Even if Eve, is 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 chosen so that Eve's undetection probability s after transmission of one block would be infinitesimal. Matrices K_i are transmitted to Bob (legitimate authorized user, receiver) via usual public (non-quantum) public authentic channel after the end of quantum transmission but only if Alice and Bob were convinced in lack of eavesdropping. Then Bob inverses the received matrices and 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 cryptanalytic attacks, similar to attacks on 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 $I = \dfrac{-kI_0}{\lg\left(\dfrac{1-q}{1-q(1-d)}\right)}$.

The calculated values of *I* are shown in [6] (see Tab. 1-2). Fig. 1 [6] shows the dependence of *I* on *n* and on *q* for $s = 10^{-4}$ and $d = d_{\max}$ [5]. 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.

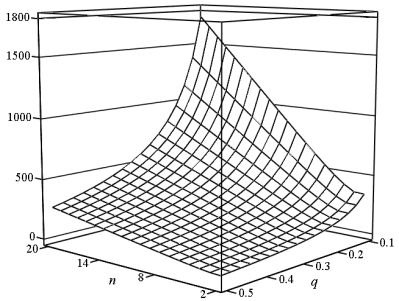

Fig. 1. Amount of Eve's information for the protocol with *n*-qubit GHZ-states at $s = 10^{-4}$ and $d = d_{\max}$ (bit)

Thus, after transfer of hashed block, the lengths of which are presented in Tab. 1 of [6], 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 QSDC protocol, namely its asymptotic security against eavesdropping attack using ancilla states, is therefore removed. But described method seriously decreases QSDC protocols speed.

Proposed Approach Description

On the ground of described method the following one is proposed to remove its disadvantages. In this method in place of matrix K_i of size $r \times r$ the key ternary (trit) sequence k_i of size 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.

In described privacy amplification method [5] to transfer the entire message it's necessary to generate and use a large number of random trit inverse in Galois field matrix. It is a method disadvantage, since it requires more time and resource costs. In

Tab. 1 [6] given the trit matrix size in accordance with total message size m and parameter r. Obviously, to transmit message size m using quantum channel its necessary to use matrix total size $r \cdot m$ trits. For understanding, data overall size in bits, convert ternary system into binary: 10^8 trit approximately equal 20 MB (if convert every 20 trit in 32 bits). Therefore, the total size of the matrix M_i if $r = 28$ is 560 MB, which first need to be generated, performed multiplication M_i on a_i, then transfer classical channel and at the end turn and identify from $b_i - a_i$, that would take too much time.

In this study proposed to use instead of matrix M_i size $r \times r$ key ternary sequence k_i by size r. Messages b_i will be calculated by the formula $b_i = k_i + a_i$, and a_i by $a_i = b_i - k_i$, where operations "+" and "−" means trits addition and modular subtraction by 3. Key ternary sequence k_i would be produced by a pseudorandom ternary sequences generator, and 96-trit key K. After the end of quantum transmission, unless the attack is absent, instead of transfer matrices M_i will be transmitted key K using public channels.

Let's analyze rates of existed and proposed methods. To transmit a message with length $m = r \cdot l$ − trit, where r − data block size, and l − blocks number, set t_1 as key-data generation time. For existing method t_1 is inverse matrix generation time M_i ($i = \overline{1,l}$) with size $r \times r$, and for proposed method t_1 is key sequence generation time k_i with length r. Therefore t_2 − message generation time b_i, t_3 − b_i transmission time over quantum channel with deterministic protocol. Let set t_4 as transmission time of inverse matrix M_i over classic channel for existing method, and for proposed method – transmission time of 96-trit key K. Generation time of inverse matrices M_i^{-1} for existing method or key sequence generation time k_i with length r for proposed method symbolize as t_5. Therefore t_6 is message recovery time a_i. Tab. 2 in [6] shows calculations of t_j ($j = \overline{1,6}$) depending on the trits sequences generation rates V_{gen}, messages transmission rates over quantum V_{kv} and classic V_{kl} channel and execution rates of multiplications and additions in field $GF(3)$ V_x.

Experimental Study

The speed of each approach will be determined by the following formula:

$$V = \frac{r \cdot l}{t_1 + t_2 + t_3 + t_4 + t_5 + t_6} \text{ trits/sec.}$$

For more specifically evaluation of speed for both amplification methods, it was decided to make simulation of the protocol with different rates V_{gen}, V_{kv}, V_{kl}, V_x, r and l [7]. To do this, authors proposed a model, which consists of following steps: 1) Set protocol base following parameters: $V_{kv}, V_{kv}, V_x, V_{gen}$. 2) Select one of the security amplification methods for QSDC protocol. 3) Select message length of m (104, 105, 106) in trits. 4) Select r (4, 12, 20) and compute l. 5) For selected parameters V_{gen}, V_{kv}, V_{kl}, V_x, r and $V_{gen} = V_x = V_{kv} = 10^6$ l compute general rates of deterministic protocol.

Simulation results are presented in Tab. 3 [6]. The speed of proposed method does not change, and the speed of the method [5] is reduced to 6-24 times (depending on the parameters V_{gen}, V_{kv}, V_{kl}, V_x). With the increasing of parameter l speed of methods virtually unchanged. The proposed approach speed compared to existing increases 3-536 times, and depending on V_{gen}, V_{kv}, V_{kl}, V_x, r and l.

Conclusions

Proposed approach provides privacy amplification of QSDC protocol and could increase its speed at least in 3 times compared with the best existed approaches. But this approach as well as existed approach uses ternary sequences and it generates another scientific problem related to its randomness assessment.

References

1. Advanced Technologies of Quantum Key Distribution, Monograph [edited by Sergiy Gnatyuk], London, Great Britain : InTech, 2018, 227 p.
2. O. Korchenko, P. Vorobiyenko, Ye. Vasiliu, S. Gnatyuk and others, Quantum secure telecommunication systems, Telecommunications Networks. Current Status and Future Trends. Monograph [edited by J.H. Ortiz], Rijeka, Croatia : InTech, 2012, 446 p.
3. K. Bostrom and T. Felbinger, Deterministic secure direct communication using entanglement, Physical Review Letters, 2002, vol. 89, issue 18, 187902.
4. Ye. Vasiliu, Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits, Quantum Information Processing, 2011, vol. 10, issue 2, pp. 189-202.
5. Ye.V. Vasiliu, S.O. Gnatyuk, S.V. Nikolaenko and T.O. Zhmurko, Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states, Ukrainian Scientific Journal of Information Security, 2012, vol. 18, issue 2, pp. 84-88.
6. S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.
7. Akhmetov B., Gnatyuk S., Zhmurko T., Yubuzova Kh. Simulation model for deterministic protocol of quantum secure direct communication with error-correcting coding, Vestnik KazNITU, 2018, №5 (129), pp. 150-158.