High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits

Zhengbing Hu[1], Sergiy Gnatyuk[2,3], Tetyana Okhrimenko (Zhmurko)[2], Vasyl Kinzeryavyy[2], Maksim Iavich[4], Khalicha Yubuzova[5]

[1]Central China Normal University, Wuhan, China
[2]National Aviation University, Kyiv, Ukraine
[3]Yessenov University, Aktau, Kazakhstan
[4]Scientific Cyber Security Association, Tbilisi, Georgia
[5]Satbayev University, Almaty, Kazakhstan
hzb@mail.ccnu.edu.cn s.gnatyuk@nau.edu.ua t.zhmurko@nau.edu.ua
v.kinzeryavyy@nau.edu.ua m.iavich@scsa.ge hali4a@mail.ru

Abstract. With the measureless, huge and rapid data exchange in network environments and increasing the attackers capabilities, quantity and quality of violations in cyberspace, information security has become the most important process for data storage and communication. Reliability of traditional methods for ensuring confidentiality is questionable, taking into account contemporary threats. Thereby, search of alternative methods and means for security is urgent issue. Significant interest causes quantum cryptography, which do not depend on computing or other capabilities of intruder, uses specific unique properties of quantum particles, and based on the inviolability of quantum physics laws. One of the most advanced quantum cryptography technology is quantum secure direct communication, which can transmit information directly by open channel, but it has only asymptotic security to non-coherent attacks and, certainly requires some methods for security amplification. In this regard, high-speed privacy amplification method for quantum cryptography protocols was developed. To evaluate the effectiveness of this method was developed a methodology for experimental research, under which comparing of its performance with known method was made. According to the obtained results, the proposed method has a speed faster against analogs at the same level of security against non-coherent attacks.

Keywords: Information and Communication Technologies, Information Security, Quantum Cryptography, Quantum Secure Direct Communication, Qutrit, Deterministic Protocol, Security Amplification.

1. Introduction

Today urgency of the cybersecurity problem is beyond any doubt – every day each citizen is faced with necessity to use information and communication technologies

(ICT) – from using social networks and posting information about personal data online to using ATMs, bank accounts etc. In this regard, the issue of ensuring confidentiality in conditions of growthing quantity and quality of violations in cyberspace acutely raises. Th cyberspace constantly improved and developed along with technologies which in turn, complicates the process of identifying, analyzing and combating them. Reliability of traditional methods to ensure the confidentiality, which is usually provided by means of symmetric (secret key cryptography) [15] and/or asymmetric (public key cryptography) methods, pose a challenge taking into account modern threat. For symmetric methods is typical problem of secret keys distribution and asymmetric methods solve mentioned problem but these methods are slow and need significant computing resources [5, 6, 8, 10, 13]. Moreover, security of traditional cryptosystems depends on the computing capabilities of intruder and based on hypothetical inability to solve a certain class of mathematical problems in polynomial time – factorization and logarithmation in discrete fields of large size etc (exluding post-quantum cryptosystems). However, this hypothesis can be refuted by using, for example, many qubits quantum computers (D-Wave 2X), GRID-technologies, HPC and other modern ICT [6, 8, 9, 13].

Considering all of the aforesaid, quantum cryptography (QC) causes great interest, it is independent from computing power of intruder, uses specific unique properties of quantum particles, and based on the inviolability of the quantum physics laws. Main advantages of QC methods are possibility of the accurate intruder detection and providing, in some cases, theoretical-information security. At present these methods and systems have passed a difficult way from theoretical assumptions and laboratory experiments to full commercial decisions [5, 6, 8, 13].

The most highly developed QC technology is quantum key distribution [5, 7] and other important direction is quantum secure direct communication (QSDC), which can transmit information directly by open channel (without its encryption – the problem of key distribution is neutralized). Today exists large number of QSDC methods [1, 5, 6, 13, 14], which are based on different quantum technologies and can be used for secure information transfering (using qubits or qudits), and also for cryptographic keys distribution.

Requirements for QSDC protocols security is considerably higher than for quantum key distribution protocols, because in QSDC protocols every bit of information is confidential and shouldn't be intercepted by eavesdropper. Thus, although QSDC protocols completely eliminates the problem of secret cryptographic keys distribution, these have only asymptotic security from non-coherent attacks [12] and certainly require security amplification methods [13, 14]. Since the probability to detect this attack after a single eavesdropping control is less than "1" for all known QSDC protocols, and errors in eavesdropping control mode will be created not only by attack, but also by natural noise in quantum communication channel, it follows that it is necessary to perform a certain amount of rounds of eavesdropping control before it can confidently detect an attack. As far as both modes (eavespropping control an message sending) should necessarily be alternated randomly, a certain amount of information can be intercepted by eavesdropper [6, 13]. Obviously that its necessary to apply additional procedures and methods to enhance security. In [13, 14] known privacy amplification methods (PAM) for QSDC protocols is described, but this method uses procedures that significantly slow down protocol work, as far as it is necessary to apply reverse hashing using reversible ternary matrices. Generating of

such matrices requires more time and resource costs (significant number of mathematical transformations over the Galois field).
From the perspective of information capacity the most effective methods are those that are use trit quantum systems. Due to relative natural-logarithmic information density (Fig. 1), which is described by function

$$Y(a) = \frac{\ln y(a)}{a} = \frac{\ln a}{a},$$

where *a* is radix, it follows that system with base equal to the base of natural logarithms (i.e. is equal to *e*) has the highest information density. For fixed-point representation system it's ternary system [2], in the case of quantum systems it's three-level quantum system named *qutrits.*

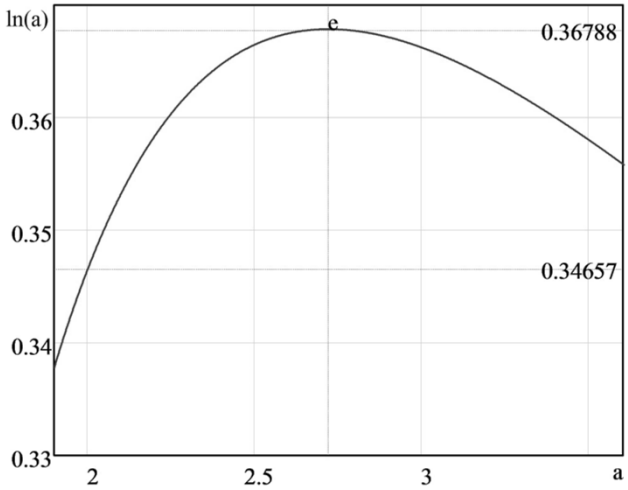

Fig. 1. Relative natural-logarithmic information density

The purpose of this paper is developing a high-speed PAM for QC protocols using pairs of entangled qutrits and conducting experimental research to evaluate its effectiveness.

2. New Privacy Amplification Method Development

Assume it's necessary to send message $A \in V_n$ by QSDC protocol (using both PAM), where $V_n = \{0,1,2\}^n$, $n = r \cdot l$, $r \in N$ is data block size, and $l \in N$ is amount of data blocks. To compare the speed of messages A transmission by QSDC protocol (with switching frequency q) were evaluated runtime of each specific stage. To evaluate the runtime of each phase following designations was used: V_{gen} are trit sequences generating speed; V_{kv} and V_{kl} are trit sequences transfer speed by quantum and classical channels respectively; V_x is execution speed for arithmetic operations in the $GF(3)$ field.

Consider proposed high-speed PAM for QC protocols (Fig. 2) [5, 12, 14], will assume that Alice and Bob are legitimate users, Eve is eavesdropper.

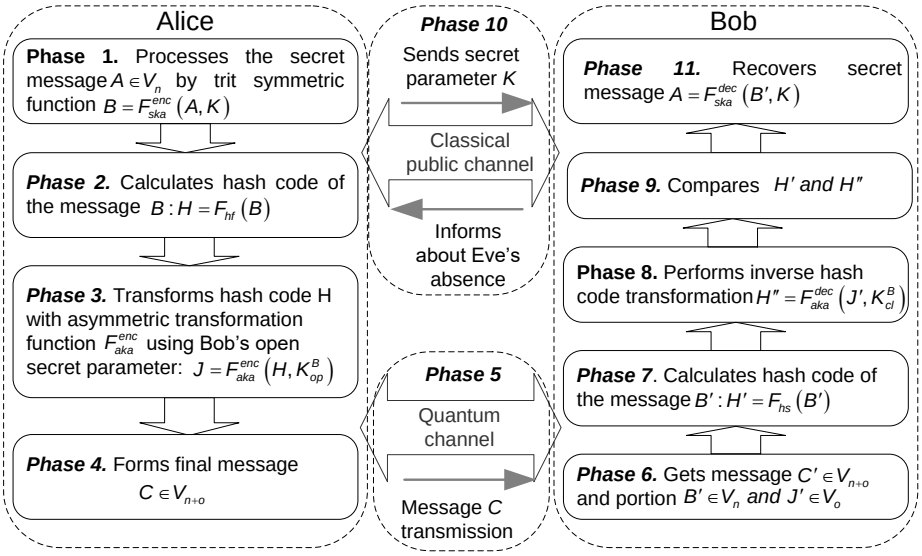

Fig. 2. Scheme of PAM for QSDC protocol realization

In accordance to scheme described on Fig. 2, Alice sends message A to Bob using following *Phases*:

Phase 1. Alice processes secret message $A \in V_n$ ($V_n = \{0,1,2\}^n$, $n \in N$) with trit symmetric transformation function $F_{ska}^{enc} : B = F_{ska}^{enc}(A, K)$, where K is secret parameter, $K \in V_k$, $k \in N$, $k < n$, F_{ska}^{enc} is symmetric transformation function, $F_{ska}^{enc} : V_n \to V_n$, B is transformed secret message $B \in V_n$.

Phase 2. Alice calculates hash code of the message $B : H = F_{hf}(B)$, where F_{hf} is trit hash function, $F_{hf} : V_n \to V_h$, $h \in N$, $h < n$, H is hash code of the message B, $H \in V_h$.

Phase 3. Alice transformes hash code H with asymmetric transformation function F_{aka}^{enc} using Bob's open secret parameter: $J = F_{aka}^{enc}(H, K_{op}^{B})$, where K_{op}^{B} is Bob's open secret parameter, $K_{op}^{B} \in V_p$, $p \in N$, F_{aka}^{enc} is asymmetric transformation function, $F_{aka}^{enc} : V_h \to V_o$, $o \in N$, J is transformed hash code H, $J \in V_o$.

Phase 4. Alice forms final message $C \in V_{n+o}$ for transmitting it to Bob: $C = (B, J)$, where $B \in V_n$, $J \in V_o$.

Phase 5. Occurs message C transmission by quantum channel using QSDC protocols from Alice to Bob. Even if Eve intercept part of the message C and still be not detected, then, not knowing the secret parameter K, she can not restore the original message A. It should be noted, that Alice and Bob can previously choose

such a value of switching frequency q between modes of QSDC protocols (from message transmission mode to eavespropping control mode), with which the probability of Eve's successful attack would be insignificant.

Phase 6. Bob gets message $C' \in V_{n+o}$ and portion $B' \in V_n$, $J' \in V_o$ and $J' \in V_o$.

Phase 7. Bob calculates hash code of the message $B' : H' = F_{hs}(B') :\ H' = F_{hs}(B')$, where F_{hf} is trit hash function, $F_{hf} : V_n \to V_h$, H' is hash code of the message B', $H' \in V_h$.

Phase 8. Bob performs inverse hash code transformation H'' by asymmetric transformation function F_{aka}^{dec} using his private secret parameter: $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$, where K_{cl}^{B} is Bob's private parameter, $K_{cl}^{B} \in V_p$, F_{aka}^{dec} is asymmetric function of inverse transformation, $F_{aka}^{dec} : V_o \to V_h$.

Phase 9. Bob compares H' and H'' and H''. If $H' \neq H''$ it means that message was modified during transmission. Immediately assumed that Eve interfered in communication session. So Bob and Alice interrupted session. Acording to non-cloning theorem, eavesdropper can not make an exact copy of quantum systems, which are transmitted by communication channel, to conduct measurements over a copy and send the original to legitimate user, without making measurements of it. This forces intruder to measure state of the quantum systems, which are transmitted (or entangle them with their quantum samples) that, according to postulate of measurement, causes change of their conditions (in such case $B' \neq B$ and $H' \neq H''$). If $H' = H''$ it means that there was no Eve interference and $B' = B$.

Phase 10. Bob informs Alice that during message transmission was no unauthorized access. Alice in turn by open communication channel sends to Bob secret parameter K.

Phase 11. Bob recovers secret message A processes trit symmetrical reverse transformation function $F_{ska}^{dec} : A = F_{ska}^{dec}(B', K)$, F_{ska}^{dec} is symmetrical reverse transformation function, $F_{ska}^{dec} : V_n \to V_n$.

As symmetric functions of transformation and reverse transformation can be used or trit block or stream transformation (however, these procedures are not encryption, as far as K transmitted by open channel to establish the legitimacy of the user, which is not conform to the principles of cryptography where key is secret parameter and it doesn't transmit using open channel). Note that in such construction of QSDC protocols, switching frequency q between modes of their work can be reduced to a minimum (from recommended value 0.5 to 0.05, based on the assumption that additional security procedures and functions were implemented), at the same time will increase speed of protocols and and Eve still be detected (on phases 5 and 9).

To study the proposed PAM for QSDC protocols [4] was developed experimental methodology, according to which were made performances comparison with existing PAM [13, 14]. Both methods are using for deterministic protocols with pairs of entangled qutrits.

In Table 1 presented basic stages of QSDC protocols with application of different PAMs (known [13, 14] and proposed, concept and short review of the method developed by the authors in [4]) and the time of their performance.

Table 1. Evaluation of QSDC protocol stages runtime (comparative analisys)

№	*Known method*		*Proposed method*	
	Operation	*Runtime*	*Operation*	*Runtime*
1.	$M_i = F_{gen}\left(K, i, r^2\right)$	$\frac{l \cdot r^2}{V_{gen}}$	$k_i = F_{gen}\left(K, i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
2.	$B_i = A_i \cdot M_i$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$B_i = A_i + k_i$	$\frac{l \cdot r}{V_x}$
3.	$B_i' = F_{kv}\left(B_i, q\right)$	$\left(\frac{l \cdot r}{V_{kv}}\right) \cdot (1+q)$	$H = F_{hf}\left(B\right)$ $J = F_{aka}^{enc}\left(H, K_{op}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
4.	$M_i' = F_{kl}\left(M_i\right)$	$\frac{l \cdot r^2}{V_{kl}}$	$B_i' = F_{kv}\left(B_i, q\right)$ $J' = F_{kv}\left(J, q\right)$	$\left(\frac{l \cdot r + 96}{V_{kv}}\right) \cdot (1+q)$
5.	$\left(M_i'\right)^{-1} = F_{obr}\left(M_i'\right)$	$\frac{l \cdot (4r^3 - 4r^2)}{V_x}$	$H' = F_{hf}\left(B'\right)$ $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
6.	$A_i' = B_i' \cdot \left(M_i'\right)^{-1}$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$K' = F_{kl}\left(K\right)$	$\frac{96}{V_{kl}}$
7.	-	0	$k_i' = F_{gen}\left(K', i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
8.	-	0	$A_i' = B_i' - k_i'$	$\frac{l \cdot r}{V_x}$

Presented in Table 2 formalized operations will be used for experimental study to estimate the speed of known and proposed PAMs.

3. Exprimental Study of Proposed Method and Discussion

Proposed technique for experiments

To study the performance of mentioned methods seven experiments with different parameters r, l, q, V_{gen}, V_{kv}, V_{kl} and V_x were conducted.

Experiments purpose is investigate the efficiency of the developed method in comparison with known and verify its adequacy.

Input parameters: trit sequences generating speed (V_{gen}), speed of trit sequences transfer by quantum channel (V_{kv}), speed of trit sequences transfer by classic channel (V_{kl}), execution speed for arithmetic operations in the field $GF(3)$ (V_x), data block size (r), amount of data blocks (l), switching frequency to listening mode (q), known and proposed PAM for QC protocols, step size of changing for each parameter.

Output parameters: gathered speed statistics for both methods depending on input parameters.
Steps of experiments:
1) Fixed basic system settings: trit sequences generating speed (V_{gen}), speed of trit sequences transfer by quantum channel (V_{kv}), speed of trit sequences transfer by classic channel (V_{kl}), execution speed for arithmetic operations in the field $GF(3)$ (V_x), data block size (r), amount of data blocks (l), switching frequency (q);
2) Next step is simulated performance of all phases of QSDC protocol by using developed software;
3) Collected statistics is used to analyze effectiveness of the proposed method for ensuring the security of QC protocols.
Selecting a step of changing: changing r from 4 to 100 (in increments 4). Changing protocols speed (V_{gen}, V_{kv}, V_{kl} and V_x) from 10^3 to 10^5.

Study and discussion

<u>*Experiment 1.*</u> Let $V_x = V_{kl} = 10^6$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0.5$ for known method of ensuring security of QSDC protocols and $q = 0.05$ for proposed method. Probability of switching into eavesdropping control mode for proposed method can be reduced to a minimum – from recommended value 0.5 to 0.05.
Fig. 3 shows the results of *experiment 1* to compare QSDC protocol performance for different PAM.

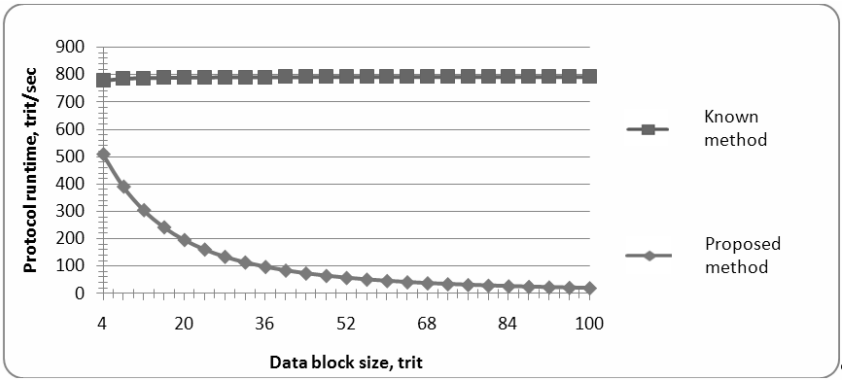

Fig. 3. QSCD protocol speed characteristics comparison (results of experiment 1)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.52 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 4.4 times.

<u>*Experiment 2.*</u> Let $V_x = V_{kl} = 10^5$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 4 shows the results of *experiment 2* to compare QSDC protocol performance for different methods of ensuring its security.

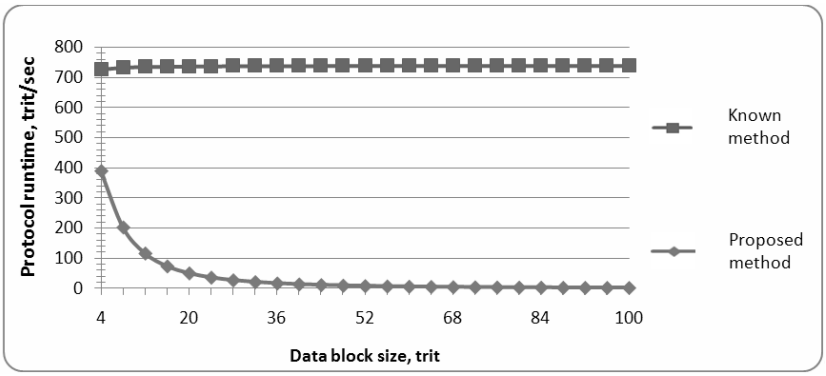

Fig. 4. QSCD protocol speed characteristics comparison (results of experiment 2)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.86 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 14.5 times.

Experiment 3. Let $V_x = V_{kl} = V_{gen} = 10^5$, $V_{kv} = 10^3$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 5 shows the results of *experiment 3* to compare QSDC protocol performance for different methods of ensuring its security.

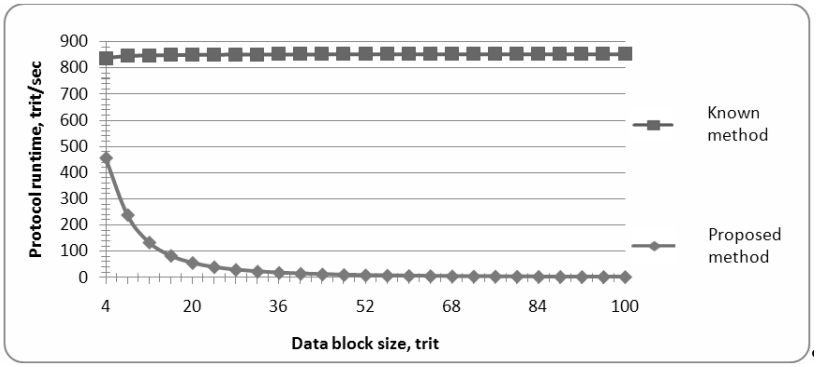

Fig. 5. QSCD protocol speed characteristics comparison (results of experiment 3)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.84 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 15.21 times.

Experiment 4. Let $V_x = V_{kl} = V_{gen} = 10^5$, $V_{kv} = 10^4$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 6 shows the results of *experiment 4* to compare QSDC protocol performance for different methods of ensuring its security.

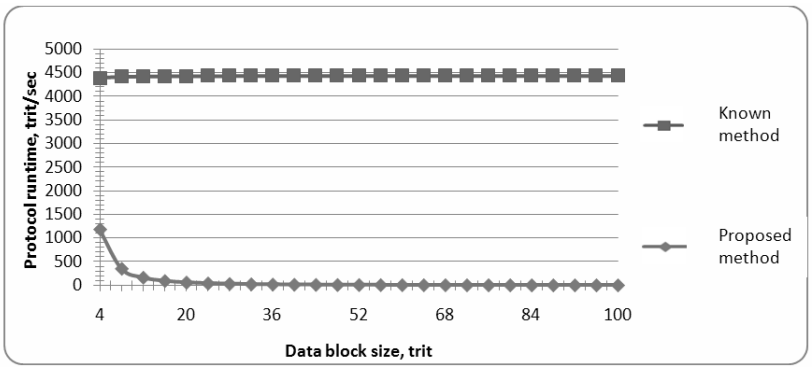

Fig. 6. QSCD protocol speed characteristics comparison (results of experiment 4)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 3.73 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 73.29 times.

Experiment 5. Let $V_x = V_{kl} = V_{gen} = V_{kv} = 10^5$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 7 shows the results of *experiment 5* to compare QSDC protocol performance for different methods of ensuring its security.

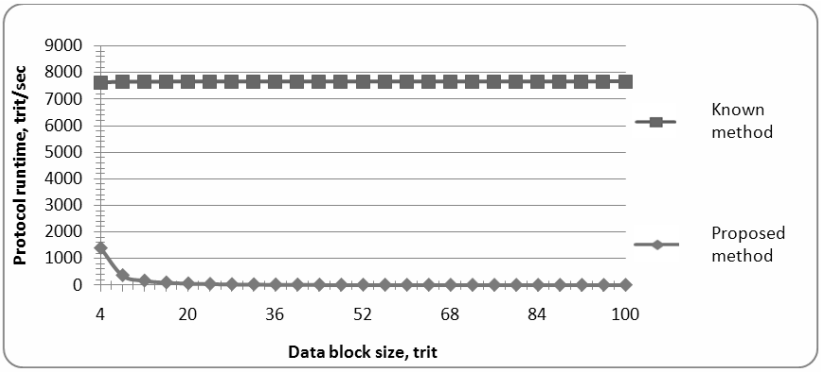

Fig. 7. QSCD protocol speed characteristics comparison (results of experiment 5)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 5.45 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 125.53 times.

Experiment 6. Let $V_x = 10^6$, $V_{kl} = 10^5$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 8 shows the results of *experiment 6* to compare QSDC protocol performance for different methods of ensuring its security.

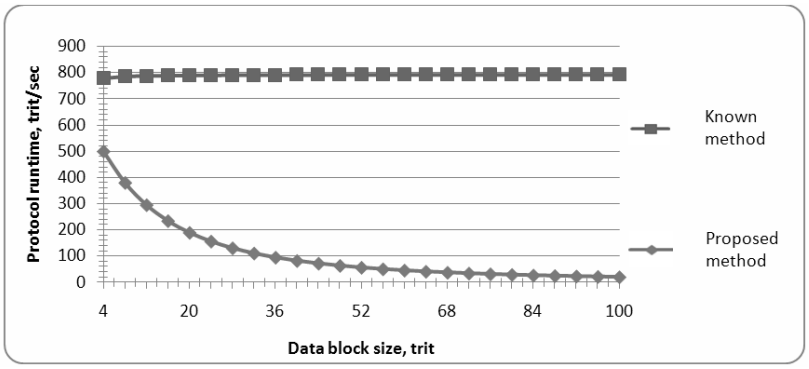

Fig. 8. QSCD protocol speed characteristics comparison (results of experiment 6)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.55 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 4.18 times.

Experiment 7. Let $V_x = 10^5$, $V_{kl} = 10^6$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0.5$ for known privacy amplification method of QSDC protocols, $q = 0.05$ for proposed method.

Fig. 9 shows the results of *experiment 7* to compare QSDC protocol performance for different methods of ensuring its security.

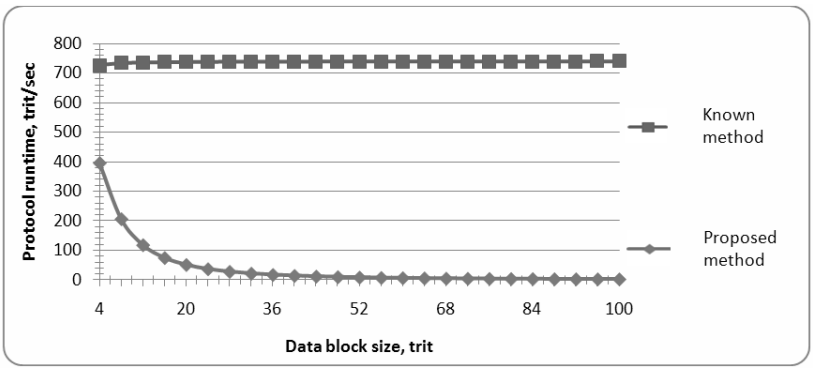

Fig. 9. QSCD protocol speed characteristics comparison (results of experiment 7)

According to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.83 time is higher than speed of the known method (for $r = 4$). Moreover, with increasing r performance improvements would be even more significant. For example, when $r = 20$ performance of the proposed method is higher in 14.39 times.

As can be seen from the above, according to experimental results, speed of QSDC protocol with the proposed PAM at least in 1.52 time is higher than the speed of the known method (Fig. 10).

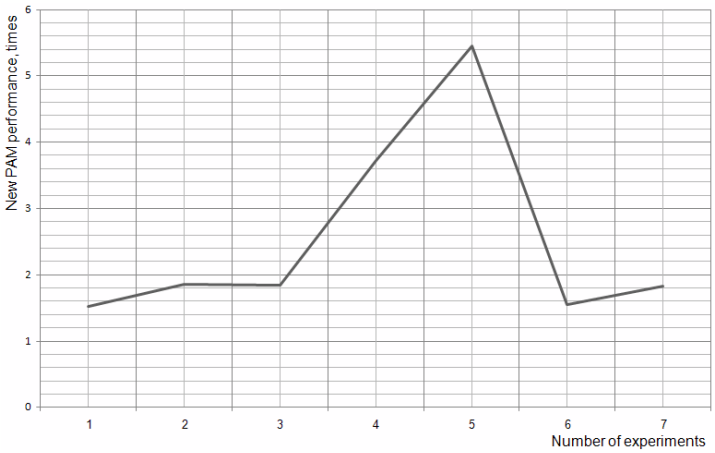

Fig. 10. Comparative analysis of efficiency for QSCD protocols with different PAMs for $r = 4$

However, it should be noted that these results were obtained for $r = 4$. In the paper [4] mentioned, that legitimate users can choose the protocol parameters (block size r, switching probability to control listening mode q and other parameters) in a way that probability of Eve's successful non-coherent attack after transmission one block size r was negligibly small value. Can be concluded, that for effective use of known and proposed PAM for QC protocols recommended size is $r \geq 20$, in that case the speed of the proposed method at least higher in 4.4 times.

4. Conclusions

Advanced many qubits quantum computers are threats for traditional cryptosystems (exluding post-quantum systems) and using of QC is alternative for some security tasks solving (intruder detection, theoretical-information security providing in some cases etc). But through it all QC has some actual probles devoted to high speed and security providing.

In this study high-speed PAM for deterministic QC protocols was developed. It allows to minimize the amount of switching between protocol modes (message transmission and eavesdropping control), and increase protocol speed at least in 1.52 time, while maintaining the security against non-coherent attacks. It is achieved by use of quantum integrity checking function and trit symmetric function, that are developed in this method.

Also in the study simulation of QSDC protocol work with proposed and known PAMs for QC protocols to non-coherent attacks was conducted, which confirmed the adequacy of the proposed method and its ability to use for privacy amplification of deterministic QC protocols using pairs of entangled qutrits. According to given results, speed of QSDC protocol with the proposed PAM is higher (when $r = 4$) than the speed of the known method, but as far as in QC recommended size is $r \geq 20$, in that case the speed of the proposed method is higher at least in 4.4 times.

From viewpoint of limitations, for effective practical application of the developed method is necessary to use existing (for example [3, 11]) cryptographically secure generators of pseudorandom sequence or develop new, which would satisfy the relevant requirements including the generation of ternary sequences.

Acknowledgments

This scientific work was financially supported by self-determined research funds of CCNU from the colleges' basic research and operation of MOE (CCNU16A02015), Joint Project of Shota Rustaveli National Science Foundation and Science & Technology Center in Ukraine [№ STCU-2016-08] as well as Ukrainian Young Scientists Project № 0117U006770.

References

1. Bostrom K., Felbinger T. (2002) Deterministic secure direct communication using entanglement, *Physical Review Letters*, vol. 89, issue 18, p. 187902.

2. Deibuk V.G., Biloshytskyi A.V. (2015) Design of a Ternary Reversible / Quantum Adder using Genetic Algorithm, *International Journal of Information Technology and Computer Science*, issue 09, p. 38-45.

3. Gaeini A., Mirghadri A., Jandaghi G., Keshavarzi B. (2016) Comparing Some Pseudo-Random Number Generators and Cryptography Algorithms Using a General Evaluation Pattern, *International Journal of Information Technology and Computer Science*, issue 9, p. 25-31.

4. Gnatyuk S., Zhmurko T., Falat P. (2015) Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the *2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015),* Warsaw, Poland, September 24-26, 2015: vol. 1, p. 468-472.

5. Korchenko O., Vasiliu Ye., Gnatyuk S. (2010) Modern Quantum Technologies of Information Security Against Cyberterrorist Attacks, *Aviation*, vol. 14, issue 2, p. 58-69.

6. Advanced Technologies of Quantum Key Distribution, Monograph [edited by Sergiy Gnatyuk], London, Great Britain : InTech, 227 p. (2018).

7. Mohammad Omer K. Jasim, Abbas Safia, El-Horbaty El-Sayed M., Salem Abdel-Badeeh M. (2015) Innovative Method for Enhancing Key Generation and Management in the AES-Algorithm, *International Journal of Computer Network and Information Security*, issue 4, p. 14-20.

8. Nielsen M.A., Chuang I.L. (2010) *Quantum computation an quantum information*, Cambrige, Cambrige University Press, 708 p.

9. Rahamana Mijanur, Islamb Md. Masudul An Overview on Quantum Computing as a Service (QCaaS): Probability or Possibility (2016) *International Journal of Mathematical Sciences and Computing*, 2016, Issue 1, P. 16-22. DOI: 10.5815/ijmsc.2016.01.02

10. Reddy P. Lokesh Kumar, Reddy B. Rama Bhupal, Krishna S. Rama (2012) Multi-User Quantum Key Distribution Using Wavelength Division Multiplexing, *International Journal of Computer Network and Information Security*, issue 6, p. 43-48.

11. Aleksander M., Dubchak L., Chyzh V., Naglik A. et al (2015) Implementation technology software-defined networking in Wireless Sensor Networks, *Proceedings of 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Warsaw, Poland, September 24-26, 2015.

12. Vasiliu Ye. (2011) Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits, *Quantum Information Processing,* April 2011, vol. 10, issue 2, p. 189-202.

13. Vasiliu Ye., Milchevich V., Nikolayenko S., Milchevich A. (2013) Secured systems for transmission of confidential information on the basis of the quantum cryptography protocols: monograph, Kharkiv: Digital Typography № 1, 168 p. (in Russian).

14. Vasiliu Ye., Nikolayenko S. (2014) Modified Method of Security Amplification for Quantum Direct Communication Protocols, *1st IEEE International Scientific-Practical Conference Problems of Infocommunications Science and Technology,* (PIC S&T '2014), p. 190-191.

15. Gnatyuk S., Kinzeryavyy V., Iavich M., Prysiazhnyi D., Yubuzova Kh. (2018) High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, *CEUR Workshop Proceedings (Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*, Kyiv, Ukraine, May 14-17, 2018), vol. 2104, p. 657-668.