საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 11, №4, 2017
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017

Informatics

Novel Version of Merkle Cryptosystem

Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili

* *Bank of Georgia University, Tbilisi, Georgia*

(Presented by Academy Member Archil Prangishvili)

ABSTRACT. In recent years active work is carried out to develop quantum computers. Quantum computers are capable to break cryptosystems, which are based on the problem of factoring integers. It means that quantum computers can break the RSA system, which is one of the most common public-key cryptosystems. One of the alternatives to RSA are Hash Based Digital Signature Schemes based on hashing. The Merkle signature scheme is the most relevant crypto system from Hash Based Digital Signature Schemes family. In this paper we offer the idea of improvement of post-quantum Merkle system. Scientists proposed to use pseudo random number generator (PRNG) in Merkle crypto system in order to optimize it. It is possible to doubt the safety of this scheme. Many PRNGs can be broken by quantum computers; these PRNGs were considered safe against attacks of standard computers. Polynomial quantum computers time attack on Blum-Micali PRNG was shown. The PRNG was considered safe against classic computers attacks. We suggest to use PRNG based on quantum random walks. The PRNG is based on the equations of quantum random walks (QRW). The generation algorithm is simple and the calculation speed is fast. The PRNG has advantages, such as, higher statistical complexity and repeatability. We show that Merkle system, that uses this PRNG is safe and more efficient. *© 2017 Bull. Georg. Natl. Acad. Sci.*

Key Words: cyber attacks, security, cryptosystems, post-quantum, Merkle, hash based

Recently, active work is carried out to develop quantum computers. The organizations Google, NASA and Universities Space Research Association signed a contract with the producer of D-Wave quantum processors. D-Wave 2X is a new quantum processor with 2048 physical qubits. 1152 qubits are used to process calculations in this quantum computer's model. Each additional qubit twice enlarges the search space implying to increase the speed of the calculations. By the end of 2017, Google would release new CPU. 20-qubit processor is currently undergoing tests, and the corporation appears to be on schedule to have its working 49-qubit chip ready by the end of 2017. Before trialing the 20-qubit chip, Google's most powerful quantum chip was the 9-qubit effort from 2015. Theoretically, quantum computers will be able to solve quickly the problems that other computers can solve only in thousands of years. This technology can change the world we are familiar with. The important difference of the new version of quantum computer is that it will be very easy to scale it, we can do it by

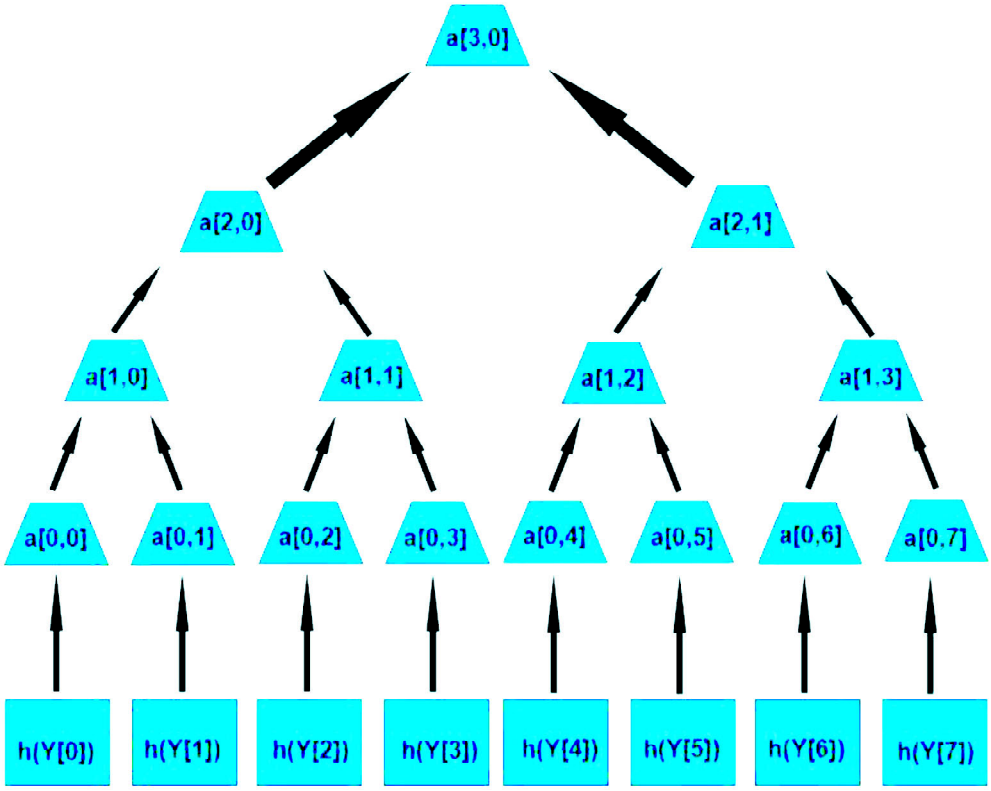

Fig. 1. Merkle tree.

adding atoms and lasers to it. The most important thing is, that it will be possible to build such quantum computer for the implementation of Shor's algorithm. The problem is transferred from the point of view of theoretical physics to the engineering point of view. Using Shor's algorithm, quantum computers are capable to break cryptosystems, which are based on the problem of factoring integers. It means that quantum computers can break the RSA system, which is one of the most common public-key cryptosystems. Hacking RSA cryptosystem will cause complete chaos [1]. One of the alternatives to RSA are Hash Based Digital Signature Schemes based on hashing. The security of these systems is based on the security of the cryptographic hash function. At first, one-time signature scheme – Lamport signature scheme, was proposed. This system works as follows: we choose 2n random numbers $X_{ij,}$ where $1 \le i \le n$ and $j = \{0, 1\}$. We calculate $Y_{ij} = h(X_{ij})$, h – is the hash function: $h: \{0,1\}^* \rightarrow \{0,1\}^s$, Y_{ij} – is the public key, X_{ij} – private key. We encrypt the message $M = (0,1)^n$ using these keys. The keys and the signature in this cryptosystem are very large [2], it makes this system not effective. Another one-time signature scheme Winternitz signature scheme, was proposed to increase the efficiency. This system works as follows: we choose parameter $w \in N$, and calculate $r = [s/w]+[([\log 2\ [s/w]] + 1 + w)/w]$. Afterwards we choose r random numbers: $X_{1,} X_{2, \ldots} X_r \in \{0,1\}^s$, concatenating them, we get the private key - X. Public key Y, is the concatenation of Y_i, where $Y_i = h^{2w-1}(X_i)$. The message M is divided into s/w blocks $b_1, \ldots, b_{s/w}$ of the length w. The checksum is calculated as follows: $C=\sum_{i=1}^{s/w} 2^w - b_i$.

A huge problem of these one-time schemes is the transfer of the public key. Because of it, Merkle cryptosystem was proposed, in this system one public key can be used many times. The number of messages N are signed by one public key K, N must be the power of two $N=2^n$. The keys X_i and Y_i are generated for N records and $h_i=h(Y_i)$ is calculated using the data we build the Merkle tree, Fig. 1.

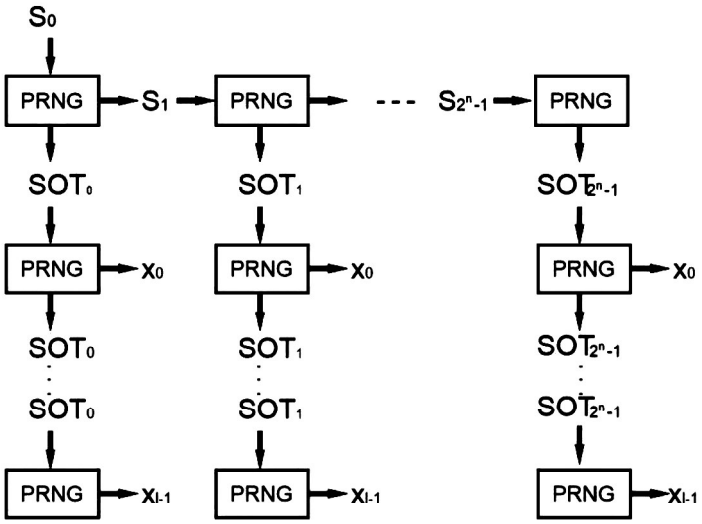

Fig. 2. One time key generation.

Each node is got by hashing concatenation of its children: $a_{1,0} = h(a_{0,0} || a_{0,1})$; The root of the tree is $a_{n,0}$ – this root is used as public key- public. We get the signature- signew of message M by using one time signature scheme, using keys X_i and Y_i. $a_{0,i} = H(Y_i)$ – is the leaf of the tree. P is the path from the node $a_{0,i}$ to the root, this path consists of n+1 nodes, $P_0 = a_{0,i}$, and $P_n = a_{n,0}$. We need all $P_0, \ldots, P_n$. $P_{n+1} = h(P_i || auth_i)$ to calculate the path, $auth_i$ is the brother node for P_i. The signature of message M is calculated like the following: $sig = (signew || auth_0 || auth_1 || ... || auth_{n-1})$. For the verification of the signature is checked *signew* and are calculated all P_i, if the value of P_n is equal to public, the signature is correct. Private key in Merkle consists of 2^n one time keys, it is rather difficult to save this numbers of keys. Scientists proposed to use PRNG- pseudo random number generator in Merkle crypto systems, in this case it is enough to save only the seed of PRNG. Each one-time signature key must be generated twice, once to generate a public key and in the second time - to sign the message. PRNG receives the seed s_1 and issues a new seed s_2 and a random number r. To generate the key for one time signature we choose the seed s_0 randomly, using s_i we process sot_i, as following:

$$PRNG(s_i) = (sot_i, s_{i+1}) \quad 0 \le i < 2^n.$$

sot_i is changed every time when we run pseudo random number generator. So to find the key Xi it is enough to know only s_i and so on. One time key generation process is shown in Fig. 2.

It is possible to doubt the safety of this scheme. Standard PRNGs that were considered safe against attacks of standard computers, can be broken by quantum computers [3]. A polynomial quantum computers time attack on Blum-Micali PRNG was shown, it was considered safe against the attacks of classic computers. This attack uses Grover method along with the quantum discrete logarithm, and during this attack it is able to restore the previous and future values at the generator output, thereby it hacks it. This attack can be adapted to other PRNGs, such as the Blum-Micali generators, with several predicates with strict queries and to generators of the Blum-Micali design, and it also can be adapted to scenarios where the requirements to bits are simplified. This type of attacks poses a threat to the security of pseudo-random number generators used in many real-world cryptosystems. So, as we can see, this type of Merkle crypto system is not safe against attacks of quantum computers. We offer to use quantum algorithm for generating pseudo random numbers in Merkle scheme. The newest PRNG was proposed, it was based on quantum random walks [4]. This PRNG is based on the equations of quantum random walks

(QRW), and, consequently, the generation algorithm is simple and the calculation speed is fast. As it was mentioned above, to integrate the pseudo random number generator with Merkle crypto system PRNG must work as following:

$$PRNG(s_i) = (sot_i, s_{i+1}),\ 0 \le i < 2^n$$

As the seed s_i we take the parameters $(E, (\alpha, \beta), p, \theta)$ of one-dimensional discrete quantum random walks (QRW) on a circle with E nodes and generate distributions of probability. Here p is the step number of QRW, its value belongs to a positive integer domain. E is the number of the node of the circle, its values also belong to the positive integer domain and the amplitude parameters of the coin states, which are complex numbers and satisfy the constraint:

$$|\alpha^2| + |\beta^2| = 1$$

$\theta \in \{0, 2\pi\}$ – parameter of coin operators.

We transform the distribution of probability into a sequence: $sc_1 = [P_{11}, P_{12}, \dots P_{1E}, P_{21}, P_{22}, \dots, P_{2E}, \dots, P_{K1}, P_{K2}, P_{KK}]$

When we repeat everything all over again, we obtain a sequence and grouping all the generated sequences of probability distributions SC_i into a sequence of random numbers, we obtain $sot = (sc_1, sc_2, \dots, sc_g)$. The proposed PRNG has successfully passed such tests as NIST. This PRNG is based on the equations of quantum random walks (QRW), and, consequently, the generation algorithm is simple and the calculation speed is fast. Being compared to the representative of PRNGs, based on quantum chaotic maps (QCM) [5], this PRNG has advantages, such as higher statistical complexity and repeatability. As we can see Merkle crypto system based on the proposed PRNG, is more safe and more efficient.

Acknowledgement. The work was conducted as a part of research grant of Shota Rustaveli National Science Foundation [№ YS15_2.1.2_9] and joint project of Shota Rustaveli National Science Foundation and Science & Technology Center in Ukraine, project N6321 [contract № STCU-2016-08]

ინფორმატიკა

Merkle-ს კრიპტოსისტემის ახალი ვერსია

ა. გაგნიძე*, მ. იავიჩი*, გ. იაშვილი*

** საქართველოს ბანკის უნივერსიტეტი, თბილისი,საქართველო*

(წარმოდგენილია აკადემიის წევრის ა. ფრანგიშვილის მიერ)

ბოლო წლების განმავლობაში საკმაოდ აქტიური სამუშაო არის ჩატარებული კვანტური კომპიუტერების შესაქმნელად, რომელთაც შეუძლიათ დიდი რიცხვების ფაქტორიზაციის პრობლემებზე დაფუძნებული კრიპტოსისტემების დანგრევა. ეს იმას ნიშნავს, რომ კვანტურ კომპიუტერებს შეუძლია დაანგრიოს RSA სისტემა, რომელიც ერთ-ერთი ყველაზე გავრცელებული საჯარო გასაღების (public-key) კრიპტოსისტემაა. RSA სისტემის ერთ-ერთ ალტერნატივას წარმოადგენს ჰეშზე დაფუძნებული ელექტრონული ხელმოწერის სქემები, რომლებიც ეფუძნება ჰეშირებას. ჰეშზე დაფუძნებული ელექტრონული ხელმოწერების სქემების ოჯახიდან ყველაზე აქტუალური გახლავთ Merkle-ს ხელმოწერების სქემა. მოცემულ სტატიაში წარმოდგენილია Merkle-ს პოსტ-კვანტური სისტემის გაუმჯობესებული ვერსია. სისტემის ოპტიმიზაციისთვის მეცნიერების რჩევაა Merkle-ს კრიპტოსისტემაში PRNG-ფსევდო შემთხვევითი რიცხვების გენერატორის გამოყენება. აღნიშნული სქემის უსაფრთხოება საეჭვოა. არსებობს მრავალი ნაშრომი PRNG-ის დანგრევის თაობაზე კვანტური კომპიუტერების მეშვეობით. ეს PRNG-ები ითვლება უსაფრთხოდ მხოლოდ სტანდარტული კომპიუტერების თავდასხმების წინააღმდეგ. Blum-Micali PRNG-ზე, რომელიც ითვლებოდა დაცულად კლასიკური კომპიუტერის საფრთხეების მიმართ, ნაჩვენები იყო კვანტური კომპიუტერის თავდასხმა პოლინამიურ დროში. ჩვენი რჩევაა PRNG-ფსევდო შემთხვევითი რიცხვების გენერატორის გამოყენება, რომელიც დაფუძნებულია კვანტურ შემთხვევით მოძრაობებზე. ეს PRNG ეფუძნება კვანტური შემთხვევითი მოძრაობების განტოლებას (QRW), მიღებული ალგორითმი მარტივია და მისი გამოთვლის სიჩქარეც არის საკმაოდ მაღალი. წარმოდგენილ კვანტურ ქაოსურ რუკებზე დაფუძნებულ PRNG-თან შედარებით, ამ PRNG-ს გააჩნია უპირატესობები. კერძოდ, უფრო მაღალი სტატისტიკური სირთულე და განმეორებადობა. ვაჩვენებთ, რომ Merkle-ს სისტემა ამ PRNG-ის გამოყენებით დაცული და უფრო ეფექტურია.

REFERENCES

1. Gagnidze A.G., Iavich M.P., Iashvili G.U. (2016) Post-Kvantovye kriptosistemy. *Modern scientific researches and innovations*, 5 (in Russian).
2. Gagnidze A., Iavich M., Iashvili G. (2016) Some aspects of post-quantum cryptosystems. *Euro-Asia Forum in Politics Economics And Business*, **5**, 1:16-20. Belgrade, Serbia.
3. Elloб B., Guedes F. M., De Assis, Bernardo Lula (2013) Quantum attacks on pseudorandom generators. *Mathematical Structures in Computer Science*, **23**(3), 608-634.
4. Yu-Guang Yang & Qian-Qian Zhao (2016) Novel pseudo-random number generator based on quantum random walks. *Scientific Reports* , **6**.
5. Akhshani A., Akhavan A., Mobaraki A., Lim S. C. & Hassan Z. (2014) Pseudo random number generator based on quantum chaotic map. *An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, **87:** 407-425.

Received June, 2017