Eurasian Journal of Business and Management, 5(1), 2017, 16-20
DOI: 10.15604/ejbm.2017.05.01.002

EURASIAN JOURNAL OF BUSINESS AND MANAGEMENT

http://www.eurasianpublications.com

SOME ASPECTS OF POST-QUANTUM CRYPTOSYSTEMS*

Avtandil Gagnidze
Corresponding Author: Bank of Georgia University, Georgia
Email: gagnidzeavto@yahoo.com

Maksim Iavich
Bank of Georgia University, Georgia. Email: webmax2006@yahoo.com

Giorgi Iashvili
Bank of Georgia University, Georgia. Email: goga_wow@yahoo.com

Abstract

The article describes alternatives to RSA system, resistant to quantum attacks. There are described Hash-based Digital Signature Schemes and McEliece system, based on the theory of algebraic coding. We analyzed their advantages and disadvantages, and considered some of the attacks on these systems. It is shown that today we are not prepared to transfer cryptosystems to post-quantum era.

Keywords: Cryptography, Post-Quantum, Cryptosystems, RSA, DSA, McEliece, Merkle, Signature, Scheme, Hash-Based, Digital, Attacks, Error, Decrypt, Encrypt

1. Introduction

Today, many leading scientists and experts are actively working on the creation of quantum computers. Recently, some studies state that GOOGLE Corporation in conjunction with NASA and the association USRA (Universities Space Research Association), signed a contract for the manufacture of the quantum processor with the company D-Wave. The D-Wave 2X System is the newest quantum processor which contains 2048 physical qubits (quantum bit). To perform calculations in the processor are used 1152 qubits.

Each additional qubit doubles the data search area, thus is also significantly increased the calculation speed. Based on the foregoing, quantum computers will probably destroy most, if not absolutely all conventional cryptosystems, that are widely used in practice. Specifically, systems based on the problem of factoring integers (e.g., RSA). Some cryptosystems like RSA system with four thousand bit keys are considered useful to protect the large classic computers from attacks, but are probably absolutely useless against attacks on large quantum computers.

Variety of the RSAs system alternatives that are of "resistant to quantum attacks," are developed. But to date a number of successful attacks is recorded on the given systems. The development and improvement of modern cryptosystems will take years. Moreover, all the time

*This work was conducted as a part of research grant of "Shota Rustaveli National Science Foundation".

is recorded successful attacks on them. When is determined the encryption function, and it becomes standard, it needs the appropriate implementation of the corresponding software, and in most cases, hardware.

During the implementation it is necessary to ensure not only correct work of the function and the speed of its efficiency, but also to prevent any kind of leaks. Recently have been recorded successful "cache-timing" attacks on RSA and AES system, as a result of that Intel has added the AES instructions to its processors. As we can see, for the creation and implementation of safe and effective post-quantum cryptosystems it is necessary to fulfill the rather big work.

2. Core

RSA cryptosystem is used in different products on different platforms and in different areas. To date, this cryptosystem is integrated into many commercial products, the number of which is growing every day. RSA system is also widely used in operating systems from Microsoft, Apple, Sun, and Novell. In hardware performance, RSA algorithm is used in secure phones, Ethernet, network cards, smart cards, and is also widely used in the cryptographic hardware. Along with this, the algorithm is a part of the underlying protocols protected Internet communications, including S/MIME, SSL and S/WAN, and is also used in many organizations, for example, government, banks, most corporations, public laboratories and universities.

RSA BSAFE encryption technology is used approximately by 500 million users worldwide. Since in encryption technology is mostly used the RSA algorithm, it can be considered one of the most common public key cryptosystems being developed together with the development of the Internet. On this basis the RSA destruction will entail easy hacking of most products that can grow into a complete chaos.

Variety of the RSA system alternatives that are of "resistant to quantum attacks" developed. But to date a number of successful attacks is recorded on the given systems. One of alternatives is Hash-based Digital Signature Schemes. The safety of these systems depends on the security of cryptographic hash functions. It was proposed one-time signature scheme - "Lamport One-Time Signature Scheme" (Coppersmith *et al.* 1997).

To sign the message $M = (0, 1)^n$ in the given scheme we must choose 2n random numbers $X_{ij,}$ where $1 \le i \le n$, and j = {0, 1}. For all i and j are calculated $Y_{ij} = h(X_{ij})$, where h – is a hash function: $h:\{0,1\}^* \rightarrow \{0,1\}^s$ Y_{ij} – is a public key, X_{ij} – is a private key. For message $M = m_1,m_2, ...,m_n$, where $m_i \in \{0, 1\}$, if $m_i = 0$, then $sig_i = X_{i0}$, otherwise $sig_i = X_{i1.}$ Signature sig – is a concatenation of all sig_i; $sig = (sig_1||sig_2||...||sig_n)$, in the case of signature verification, if $h(m_i) = 0$, then $h(sig_i)$ must be equal to Y_{i0},otherwise $h(sig_i)$ must be equal to Y_{i1}.

The main and serious drawback of this scheme is a great size of the keys. To achieve security $O(2^{80})$, the total size of public and private keys must be $160*2*160$ bits = 51200 bits, that is 51200/1024=50 times larger than in the case of RSA. Also we must note that the size of the signature in the given scheme is also much larger than in the case of RSA.

Winternitz One-time Signature Scheme was proposed to reduce the size of the signature. In this scheme we choose the argument $w \in N$, and is calculated $r = [s/w]+[([\log 2 [s/w]] + 1 + w)/w]$. We choose r random numbers $X_{1,} X_{2, ...} X_r \in \{0,1\}^s$, concatenation of which is X - private key. Are calculated $Y_i = h^{2w-1}(X_i)$, the public key is $Y = h(Y_1||...||Y_r)$. The message M is divided into s/w blocks $b_1, \ldots, b_{s/w}$ with the length w, if it is necessary, on the left are added zeroes. Later is calculated the checksum $C = \sum_{i=1}^{s/w} 2^w - b_i$. It is shown in the Figure 1.

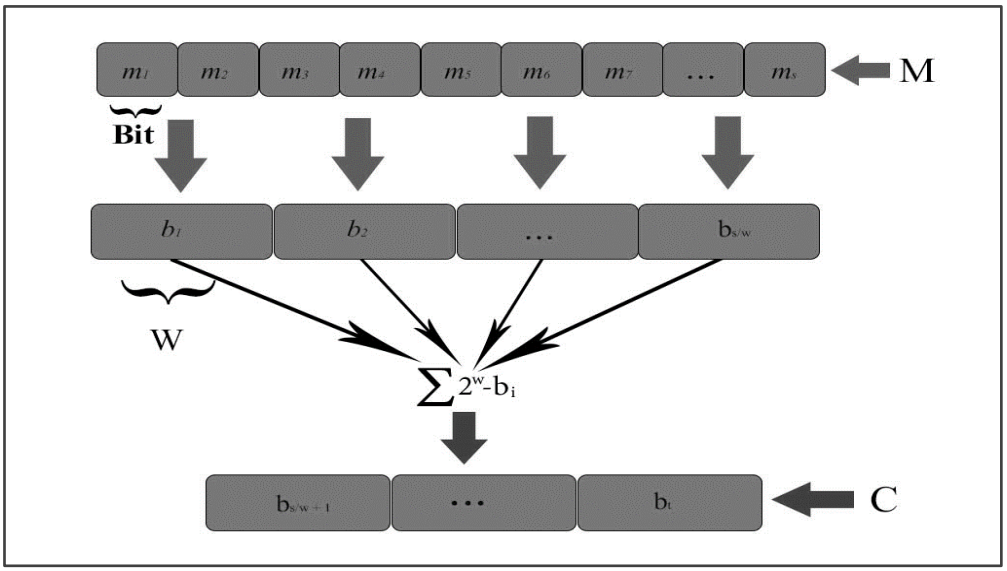

Figure 1. Winternitz One-time Signature Scheme

The binary representation of C is divided into [([log2 [s/w]] + 1 + w)/w] blocks, $b_{s/w+1}$, ..., b_r with the length w. We calculated sigi= $h^{bi}(X_i)$ for i = 1, ..., r, the signature of the letter is sig = (sig_1||...||sig_r). For signature verification are calculated b_1, ..., b_r. For i = 1, ..., r is calculated $signew_i=h^{2w-1-bi}(sig_i) = h^{2w-1-bi}(h^{bi}(X_i)) = h^{2w-1}(Xi) = Y_i$, if $h(signew_1, ..., signew_r)=Y$, then the signature is correct.

The biggest problem of one time signature schemes is the transfer of public key. It is necessary to make sure that the public key has not been changed; therefore it is necessary to use as little number of public keys as possible, and to make them shorter. Merkle proposed the cryptosystem where a public key can be used for the multiple messages. In the given cryptosystem, the public key K is used to sign the concrete number of messages (Buchmann *et al.* 2006; Buchmann *et al.* 2007). The number of messages must be a power of two, i.e. $N=2^n$. First of all, we must generate the keys X_i and Y_i for N records and calculate $h_i=h(Y_i)$, using this data is constructed the tree - Merkle Tree, Figure 2.

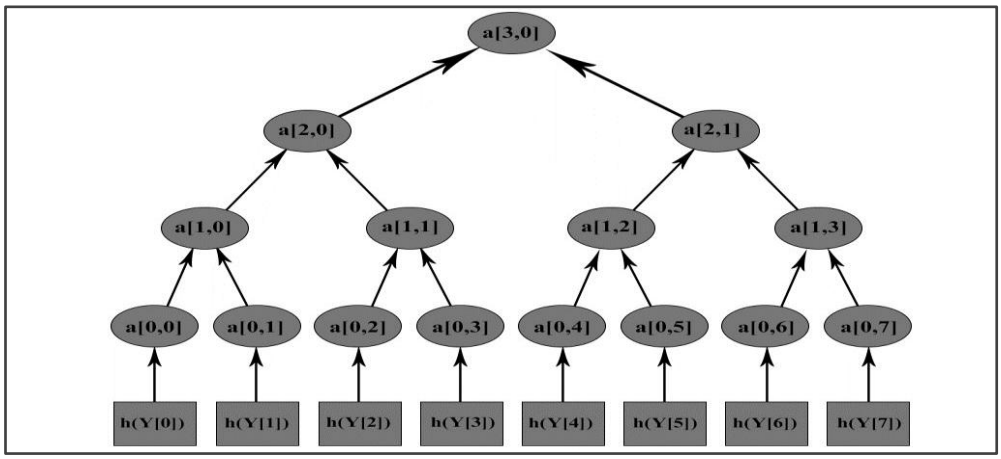

Figure 2. Merkle Tree

a_{ij} – is the node of the tree.h_i – are the leaves of the tree. The nodes of the tree are the concatenation of their children: $a_{1,0} = h(a_{0,0}|| a_{0,1})$; we build the tree with 2^n leaves and 2^{n+1}-1 nodes. The root of the tree $a_{n,0}$ is a public key - public.

The message M is signed with one-time signature system, using the pair of keys X_i and Y_i, as a result we get signew; $a_{0,i} = H(Y_i)$ – is the hash tree leaf. The path from $a_{0,i}$ to the root we will call P, it consists of n+1 nodes, $P_0 = a_{0,i}$, and $P_n = a_{n,0}$ = public. To calculate this path we need all the children of nodes P_0, …, P_n. $P_{n+1} = h(P_i||auth_i)$, where $auth_i$ - is the brother node of Pi. The signature of the letter will be sig = (signew $||auth_0||auth_1||...||auth_{n-1}$). During the verification of record is checked signew of the message M; if it is correct, are calculated P_0, …, P_n, if P_n is equal to the public key (public), the signature is correct.

In recent years scientists have been working on improving Merkle Signature Scheme. Are achieved good results in signature time as well as in verification message time, but despite this, the signature size is very large compared to the DSA and RSA signature schemes.

One more solution of the problems, associated with post-quantum cryptography, is McEliecethe system with public keys, which is based on the theory of algebraic coding. This system was developed in 1978 by Robert Mc Alice. This system is the first encryption system that uses the randomization process. Despite the fact that the algorithm has not received wide acceptance in classical cryptography, it is a candidate for being used in post-quantum cryptography.

In this system the public key is (G_{new}, t), and the private key is (S, G, P), where G is k x n generator matrix for the code C. C is random binary (n, k)-linear code, that is capable to improve t errors. N is the number of code words, k is dimension of C. S is a random k x k binary nonsingular matrix. P is a random n x n binary permutation matrix. $G_{new} = S * G * P$; k x n matrix. To encrypt the message we must encrypt message m as a binary string with the length k; cyp = m x G_{new}; is generated random n-bit error vector v with the weight t. The cypher is calculated as c= cyp+v. For decoding is calculated cyp = $c*P^{-1}$; using decryption algorithm of C is calculated $m_{new} = m*S$ => $m = m_{new}*S^{-1}$.

To date are already found successful attacks on this crypto system. The Ph.D. candidate of Dublin City University (DCU) Neill Costigan with the support of Irish Research Council for Science, Engineering and Technology (IRCSET), together with Professor Michael Scott, Science Foundation Ireland (SFI) member successfully were able to carry out an attack on the algorithm. To do this they needed 8,000 hours of CPU time. In the attack representatives of four other countries took part. Scientists have discovered that the initial length of the key in this algorithm is insufficient and should be increased.

This system cannot be also used to encrypt the same message twice and to encrypt the message when is known it's relation with the other message (Berson, 1997). From the foregoing it is clear that today we are not ready to transfer cryptosystems into post-quantum era. In the near future we cannot be sure in the reliability of the systems.

It should be noted the importance of efficiency spectrum. To date, experts have reached quite good results in the speed algorithm processing. According to the investigation results, it becomes clear that the proposed post-quantum cryptosystems are relatively little effective. Implementation of the algorithms requires much more time for their processing and verification. Inefficient cryptography may be acceptable for the general user, but it cannot be acceptable for the internet servers that handle thousands of customers in the second. Today, Google has already has problems with the current cryptography. It is easy to imagine what will happen when implementing crypto algorithms will take more time.

The development and improvement of modern cryptosystems will take years. Moreover, all the time is recorded successful attacks on them. When is determined the encryption function, and it becomes standard, it needs the appropriate implementation of the corresponding software, and in most cases, hardware.

During the implementation it is necessary to ensure not only correct work of the function and the speed of its efficiency, but also to prevent any kind of leaks. Recently have been recorded successful "cache-timing" attacks on RSA and AES system, as a result of that Intel has added the AES instructions to its processors.

McEliece system is vulnerable to attacks, related to side channel attacks. It was shown the successful timing attack on Patterson (Strenzke *et al.* 2008). This attack does not detect the key but detects an error vector that can successfully decrypt the message cipher.

As we can see, for the creation and implementation of safe and effective post-quantum cryptosystems it is necessary to fulfill the rather big work.

3. Conclusion

We try to describe alternatives to RSA system that are resistant to quantum attacks. Based on the theory of algebraic coding we developed Hash-based Digital Signature Schemes and McEliece system. We analyzed their advantages and disadvantages, and considered some of the attacks on these systems. From our point of view it is clear that today we are not prepared to transfer cryptosystems to post-quantum era.

References

Coppersmith, D., Stern, J., and Vaudenay, S., 1997. The security of the bi- rational permutation signature schemes. *Journal of Cryptology*, 10(3), pp.207-221. http://dx.doi.org/10.1007/s001459900028

Buchmann, J., Coronado García, L.C., Dahmen, E., Doring, M., and Klintsevich, E., 2006. CMSS - An improved merkle signature scheme. *Progress in Cryptology - Indocrypt 2006*, 4329, pp. 349-363.

Buchmann, J., Dahmen, E., Klintsevich, E., Okeya, K., and Vuillaume, C., 2007. Merkle signatures with virtually unlimited signature capacity. In: J. Katz and M. Yung, eds. 2007. *Applied cryptography and network security, 5th international conference, ACNS 2007, Zhuhai, China, June 5-8, 2007 proceedings.* Switzerland: Springer. http://dx.doi.org/10.1007/978-3-540-72738-5_3

Berson, T., 1997. Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. In: Burton S. and Kaliski Jr., eds. 1997. *Advances in cryptology — CRYPTO '97, 17th annual international cryptology conference Santa Barbara, California, USA August 17–21, 1997 proceedings*. Switzerland: Springer.

Strenzke, F., Tews, E., Molter, H.G., Overbeck, R., and Shoufan, A., 2008. Side channels in the McEliece PKC. In: J. Buchmann and J. Ding, ed. 2008. *Post-quantum cryptography second international workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 proceedings.* Switzerland: Springer. http://dx.doi.org/10.1007/978-3-540-88403-3_15