Lattice based merkle

Maksim Iavich
IT *dept. School of Technology*
Caucasus University
Tbilisi, Georgia
m.iavich@scsa.ge

Avtandil Gagnidze
Faculty of Business Management
Int. Black Sea University
Tbilisi, Georgia
gagnidzeavto@yahoo.com

Giorgi Iashvili
IT *dept. School of Technology*
Caucasus University
Tbilisi, Georgia
g.iashvili@scsa.ge

Sergiy Gnatyuk
IT Security dept. National Aviation University
Kyiv, Ukraine
sergio.gnatyuk@gmail.com

Vira Vialkova
dept.of Cyber Security
Taras Shevchenko National University
Kyiv, Ukraine
veravialkova@gmail.com

Abstract— Scientists are actively working on the creation of quantum computers. Quantum computers can easily solve the problem of factoring the large numbers. As the result of it quantum computers are able to break the crypto system RSA, which is used in many products. Hash based digital signatures are the alternative to RSA. These systems use cryptographic hash function. The security of these systems depends on the resistance to collisions of the hash functions that they use. The paper analyzes hash based digital signature schemes. It is shown, that hash and one way functions must be used many times during the implementation of the hash based digital signature schemes. Great attention must be paid on the security and the efficiency of these functions. Hash functions are considered to be resistant to quantum computer attacks, but the Grover algorithm allows us to achieve quadratic acceleration in the search algorithms. It means that hash functions must be complicated to be secure against quantum computers attacks. Scientists are working on determination of the cost of attacks on SHA2 and SHA3 families of hash functions. It is recommended to use lattice based constructions for one way and hash functions. Lattice based crypto systems are one of the alternatives to RSA. These crypto systems have very reliable security evidence, based on "worst-case hardness", and are resistant to attacks of quantum computers. The security of lattice based crypto system is based on the complexity of lattice problems, the main one of them is the shortest vector (SVP) problem.

It is proposed to use the lattice-based hash function instead of the standard one, and to use lattice based one-way function as a one-way function in hash-based digital signature scheme. It is analyzed the possibility of using the family of one-way functions, suggested by Ajtai. In this paper, it is proposed to use the one-way functions offered by Ajtai and it can be considered as the initial idea. It is worth to consider the idea of using optimized one-way lattice based functions. As the result we get the secure hybrid of lattice based and hash based crypto systems, that can be used in post-quantum epoch.

Keywords— lattice, lattice-based crypto system, hash-based crypto system, Merkle crypto system

I. Introduction

Digital signature is a requisite of the electronic document, which is obtained by the cryptographic transformation and gives the possibility to check the true value of the information from the moment of digital signature formation. Digital signatures are very important in real life. The world leading scientists and experts are actively working on creating quantum computers. Recently it is published an article claiming that the corporations Google and NASA and Universities Space Research Association (USRA) has signed an agreement on cooperation with the producer of D-Wave quantum processors.

D-Wave 2X is the latest quantum processor, which contains 2048 physical qubits. In this model of quantum computer 1152 qubits are used to perform calculations. Each additional qubit also enlarges twice the search space so increases the speed of the calculations.

Quantum computer will be able to destroy most of all or completely all the traditional widely used cryptosystems, concretely, systems based on the integer factorization task (e.g. RSA). Some cryptosystems, such as RSA, with four thousand-bit key are considered to be safe against the classical computers attacks, but they are powerless against the quantum computer attacks. The security of digital signatures is based on the complexity of discrete algorithm solution and the large integers factorization problem. Quantum computers will easily overcome this problem and it will cause the breaking of digital signatures, implying the absolute failure.

II. Lattice based crypto systems

Lattice based crypto systems are one of the alternatives to RSA. These crypto systems have very reliable security evidence, based on "worst-case hardness", and are resistant to attacks of quantum computers. The security of lattice based crypto system is based on the complexity of lattice problems, the main one of which is the shortest vector (SVP) problem [1-3].

A. Lattice based one-way functions. Ajtai offered a family of one-way functions with the security based on the worst cases of approximate SVP with accuracy nt, where t is an integer[4]. Later Goldreich showed that this function is resistant to collisions, and it gives us the opportunity to use it as a hash function [5]. A lot of work is done to reduce the size of the constant and in recent works the constant is already equal to 1.

The function has parameters n, m, a and b, which are integers. The security of the function depends on the choice of *n*. In the case of hashing *m* must be greater than *nlog a/ log b*.
Matrix K from $Z^{n\times m}_a$ is chosen as a key. One-way function f works as follows:

f(x) = Kx mod a. The function transforms mlog b into nlog a bit. As we can see, all the arithmetic can be performed very effectively without using the precision of integers commonly used in cryptographic functions.

B. Hash-based crypto systems. Hash based digital signatures are also the alternative to RSA. These systems use cryptographic hash function. The security of these systems depends on the resistance to collisions of the hash functions, that they use [6,7].

C. One-time signatures. Lamport–Diffie one-time signature scheme.

Lamport–Diffie one-time signature scheme was offered [8].
For the signature key *X*, *2n* random lines of size *n* are generated.

$$X= (x_{n-1}[0], x_{n-1}[1], \dots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n} \quad (1)$$

Verification key $Y= (y_{n-1}[0], y_{n-1}[1], \dots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n}$

It is calculated as follows:

$$y_i[j] = f(x_i[j]),\ 0<=i<=n-1,\ j=0,1 \quad (2)$$

f – is one way function:

$$f: \{0,1\}^n \rightarrow \{0,1\}^n; \quad (3)$$

As we see, for generating *Y* the one-way function *f* is used *2n* times.

D. Signature of the message. To sign the message m, we hash:

$$h(m)=hash = (hash_{n-1}, \dots, hash_0) \quad (4)$$

h- is a cryptographic hash function:

$$h: \{0,1\}^* \rightarrow \{0,1\}^n \quad (5)$$

The signature is calculated as follows:

$$sig= (x_{n-1}[hash_{n-1}], \dots, x_0[hash_0]) \in \{0,1\}^{n,n} \quad (6)$$

The size of the signature is n^2, one-way function f is not used.

E. Message verification. To verify the signature *sig*, the message is hashed

$$hash = (hash_{n-1}, \dots, hash_0) \quad (7)$$

After that the following equality is verified:

$$(f(sig_{n-1}), \dots, f(sig_0)) = (y_{n-1}[hash_{n-1}], \dots, y_0[hash_0]) \quad (8)$$

If the equation is true, then the signature is correct.
For verification the one-way function *f* is used *n* times.

F. Winternitz one-time signature scheme. In the Lamport scheme key generation and signature generation are efficient, but the signature size is equal to n^2.
Winternitz one-time signature scheme is used to reduce the size [9]. In this scheme several bits of the hashed message are simultaneously signed by one line of the key.

The Winternitz parameter is the number of bits of the hashed message that will be signed simultaneously. It is chosen as *w>=2*.

After that we calculate:

$$p_1=n/w \text{ and } p_2= (\log_2 p_1 +1+w)/w,\ p= p_1+ p_2 \quad (9)$$

The signature keys are generated randomly:

$$X= (x_{p-1}[0], \dots, x_0) \in \{0,1\}^{n,p} \quad (10)$$

The verification key is computed as:

$$Y= (y_{p-1}[0], \dots, y_0) \in \{0,1\}^{n,p},$$
$$\text{where } y_i = f^{2^w-1}(x_i),\ 0<=i<=p-1 \quad (11)$$

G. Signature of the message. The lengths of the signature and the verification key are equal to *np* bits, one-way function *f* is used $p(2^w-1)$ times.

To be signed the message is hashed: *hash=h(m).* The minimum number of zeros is added to the hash, so that the hash would be a multiple of *w*. Afterwards it is divided into p_1 parts of size *w*.

$$\text{hash}=k_{p-1},\dots, k_{p-p1} \quad (12)$$

The checksum:

$$c=\sum_{i=p-p1}^{p-1}(2^w-k_i) \quad (13)$$

As $c<= p_1 2^w$, the length of its binary representation is less than $\log_2 p_1 2^w+1$

The minimum number of zeros is added the binary representation, so that it would be a multiple of w, and it is divided into p_2 parts of the length *w*.

$$c=k_{p2-1}, \dots, k_0 \quad (14)$$

the message signature is calculated as follows:

$$sig = (f^{k_{p-1}}(x_{p-1}), \dots, f^{k_0}(x_0)) \quad (15)$$

in the worst case f is used $p(2^w-1)$ times. The size of the signature is equal to *pn*.

H. Signature Verification. To verify the signature $sig = (sig_{n-1}, \ldots, sig_0)$ bit string $k_{p-1}, \ldots, k_0$ are calculated.

Then the following equality is verified:

$$(f^{2^w-1-k_{p-1}}(sig_{n-1}), \ldots, (f^{(2^w-1-k_0)})(sig_0) = y_{n-1}, \ldots y_0 \quad (16)$$

In the worst case function f must be used to verify the signature $p(2^w-1)$ times.

Comparison of Lamport and Winternitz one-time signature schemes

	Lamport	Winternitz
Use *f* to generate keys	*2n*	$p(2^w-1)$
Use *f* to calculate the signature	Is not used	$p(2^w-1)$
Use *f* to generate verify the signature	*n*	$p(2^w-1)$

Fig. 1. Comparison of signature schemes.

I. Merkle crypto-system. One time signatures are not convenient in use, because to sign each message a unique key is needed. The Merkle signature scheme allows to sign multiple messages with the same key. This system uses one-time signature and a binary tree a public key as a root.

J. Key generation. The size of the tree must be $H>=2$ and using one public key $2H$ documents can be signed. Signature and verification keys are generated; $Xi, Yi, 0<=i<=2H$. X_i- is the signature key, Y_i- is the verification key. Signature keys are hashed using the hash function $h:\{0,1\}^* \rightarrow \{0,1\}^n$ in order to get the leaves of the tree.

The concatenation of two previous nodes is hashed in order to get the parent node.

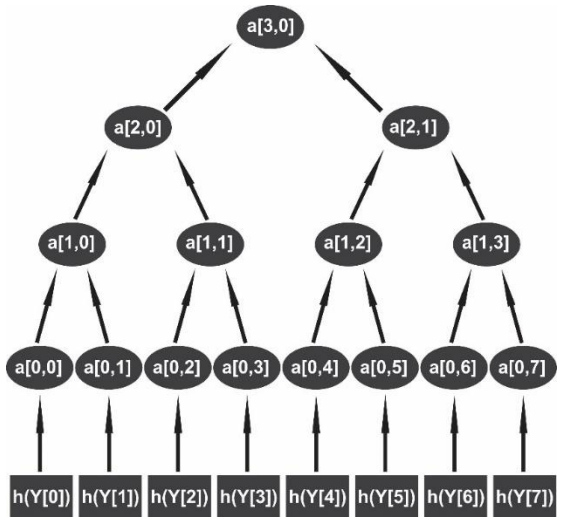

Fig. 2. Merkle tree with $H=3$.

a[i,j] are the nodes of the tree;

$$a[1,0]=h(a[0,0] \,||\, a[0,1]) \quad (17)$$

The root of the tree is the public key of the signature - *pub*, 2^H pairs of signature keys must be generated in order to calculate the public *k*, and the hash function h is used $2^{H+1}-1$ times.

K. Message signature. A message of any size can be signed being transformed to size of *n* by means of hashing $h(m) = hash$,
An arbitrary one-time key X_{any} is used, and the signature is a concatenation of one-time signature, one-time verification key, index of a key and all fraternal nodes according to the selected arbitrary key with the index "any".

$$Signature= (sig||any|| Y_{any}||auth_0, \ldots, auth_{H-1}) \quad (18)$$

L. Signature verification. The one-time signature is checked using the selected verification key, if the verification is true, all the *a[i, j]* are calculated using "auth", index "any" and Y_{any}. The signature is verified, if the root of the tree matches the public key.
The hash function in Merkle is used $2^{H+1}-1$ times, one-way function f is used $3p(2^w-1)$ times in the case of Winternitz, and $3n$ times in the case of Lamport. Hash functions are considered resistant to quantum computer attacks, but the Grover algorithm allows us to achieve quadratic acceleration in the search algorithms. It means that hash functions must be complicated to be secure against quantum computers attacks. Studies are conducted to determine the cost of attacks on SHA2 and SHA3 families of hash functions [10].

CONCLUSIONS

We propose to use the lattice-based hash function and a lattice based one-way function in hash-based digital signature schemes.

The family of one-way functions, suggested by Ajtai, can be used. As the key of hash functions, the matrix K from $Z^{n\times m}{}_a$ is selected, it transforms mlog b into $nlog$ a bits and $h(x)$ is calculated as $Kx \bmod a$.

The matrix K from $Z^{m\times m}{}_b$, is selected as the key of an one-way function,. It transforms $mlog\ b$ bits into $mlog\ b$ bits and $f(x)$ is computed as $Kx \bmod a$.

One-way functions offered by Ajtai are proposed in the paper and it can be considered as the initial idea. It is worth considering the idea of using optimized one-way lattice based functions.

ACKNOWLEDGEMENT

The work was conducted as a part of joint project of Shota Rustaveli National Science Foundation of Georgia and Science & Technology Center in Ukraine [№ STCU-2016-08]

effectively without using the precision of integers commonly used in cryptographic functions.

REFERENCES

[1]. Güneysu T., Lyubashevsky V., Pöppelmann T. (2012) Practical Lattice-Based Cryptography: A signature scheme for embedded systems. *Lecture notes in computer Sci.*, 7428: 530-547, Springer.

[2]. Akinyele, J.A., Garman, C., Miers, I. et al. (2013) Charm: a framework for rapidly prototyping cryptosystems. *Journal of cryptographic engineering*, 3. Springer: 111-128

[3]. Gagnidze A., Iavich M., Iashvili G., (2017) Analysis of post quantum cryptography use in practice. *Bulletin of the Georgian National Academy of Sciences*, 2, 12: 29-36

[4]. Ajtai, M.: Generating hard instances of lattice problems. In Complexity of computations and proofs, volume 13 of Quad. Mat., pages 1–32. Dept. Math., Seconda Univ. Napoli, Caserta (2004). Preliminary version in STOC 1996. 8. Babai, L.: On Lovász lattice reduction and the nearest lattice point problem. Combinatorica, 6:1–13 (1986).

[5]. Goldreich, O., Goldwasser, S., and Halevi, S.: Collision-free hashing from lattice problems. Technical Report TR96-056, Electronic Colloquium on Computational Complexity (ECCC) (1996).

[6]. Bernstein D.J., Buchmann J., Dahmen E., (2009) *Book: Introduction to post-quantum cryptography*, Springer.

[7]. Gagnidze A, Iavich M., Iashvili G., (2016) Some aspects of post-quantum cryptosystems. *Eurasian journal of business and management*, 5, 1: 16-20

[8]. Lamport, L.: Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

[9]. Merkle, R.C.: A certified digital signature. Advances in Cryptology - CRYPTO ’89 Proceedings, LNCS 435, pages 218–238, Springer, 1989.

[10]. Wozniak, M., Polap, D., Borowik, G. and Napoli, C., 2015, July. A first attempt to cloud-based user verification in distributed system. In 2015 Asia-Pacific Conference on Computer Aided System Engineering, pp. 226-231 . IEEE.

[11]. Amy M., Di Matteo O., Gheorghiu V., Mosca M., Parent A., Schanck J. (2017) Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. *Lecture notes in computer science*, 10532: 10-31, Springer.