Critical Analysis of Hash Based Signature Schemes

A. Gagnidze, [2] M. Iavich, [3] N. Inasaridze, [4] G. Iashvili, [5] V.Vyalkova
[1,2,4] Bank of Georgia University, Kazbegi ave. N14, Tbilisi, 0160, Georgia
[3]Andrea Razmadze Mathematical Institute of I. Javakhishvili Tbilisi State University, 6. Tamarashvili Str., Tbilisi 0177, Georgia
[5]Taras Shevchenko National University of Kyiv, Volodymyrska St. 60, Kyiv, 01033, Ukraine.
gagnidzeavto@yahoo.com [1] , m.iavich@scsa.ge [2], niko.inas@gmail.com [3] , g.iashvili@scsa.ge [4]
,veravialkova@gmail.com [5]

ABSTRACT

Active work is being done to create and develop quantum computers. Traditional digital signature systems that are used in practice are vulnerable to quantum computers attacks. The security of these systems is based on the problem of factoring large numbers and calculating discrete logarithms. Scientists are working on the development of alternatives to RSA, which are protected from attacks by quantum computer.

One of the alternatives are hash based digital signature schemes. In the article hash based one-time signatures are considered, their analysis and comparison are done. It is shown that, using Winternitz one-time signature scheme, the length of the signature and of the keys is substantially reduced. But also this scheme has disadvantages, in the case of generating keys, creating a signature and verifying a signature, one-way function should be used much more times, then in Lamport signature scheme. So, must be paid serious attention at the choice of this function, it should be quickly executed and safe.

KEYWORDS

Cryptography, quantum, hash based, signature, secure.

1 INTRODUCTION

Active work is being done to create and develop quantum computers. Google Corporation, NASA and the Universities Space Research Association (USRA) have teamed up with DWAFE, the manufacturer of quantum processors. D-Wave 2X is a quantum processor that contains 2,048 physical qubits. 1152 qubits are used to perform calculations. Google is working on releasing the new CPU.

20-qubit processor, is currently undergoing tests, and the company appears to be on schedule to have its working 49-qubit chip ready by the end of 2017 as promised. Until it began trialing the 20-qubit chip, Google’s most powerful quantum chip was the 9-qubit effort from 2015[1].

Each additional qubit doubles the data search area, so the calculation speed is significantly. Quantum computers will be able to break most, if not absolutely all conventional cryptosystems, that are widely used in practice.

So traditional digital signature systems that are used in practice are vulnerable to quantum computers attacks. The security of these systems is based on the problem of factoring large numbers and calculating discrete logarithms.

Some cryptosystems for example RSA system with four thousand bit keys are considered useful to protect information from classic computers attacks, but are absolutely not safe against attacks implemented using quantum computers.

RSA cryptosystem is used in many 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 [2].

Quantum computer can break RSA using Shor’s algorithm.

2 SHOR’S ALGORITHM

In 1994, mathematician Peter Shore invented the first quantum algorithm, which could potentially have practical application. Shor's algorithm is designed for the factorization of numbers, that is, their factorization into prime factors. The factorization of numbers is one of the tasks with which traditional computers cope with great difficulty. The larger the number, the longer it takes to determine its multipliers. Also the number of steps necessary to factorize a number of known algorithms exponentially grows with each additional bit and quickly crosses the bounds of the possible.

The cryptography with a public key is based on this property, which is used to protect financial data on the Internet or in the electronic currency Bitcoin.

To break, the RSA cipher, you need to know the multipliers that make up the public key. Since the key is a sufficiently large number, in order to factor it with a conventional computer, it will take years. When the same problem is solved on a quantum computer using Shor’s algorithm, the computation time does not grow exponentially, but much more slowly. Large numbers continue to factor out longer than short ones, but not long enough not to be factored.

Quantum computer allows us to factorize a number consisting of N digits for N^2 operations. Scientists are working on the development of alternatives to RSA, which are protected from attacks by quantum computer.

One of the alternatives are hash based digital signature schemes. These systems use a cryptographic hash function. The security of these digital signature systems is based on the collision resistance of the hash functions that they use [3,4].

Digital signature is a requisite of electronic document, which is obtained by the cryptographic transformation and gives the possibility to check the true value of information from the moment of digital signature formation.

Digital signature (DS) is used in many industries. DS technology is widely used in digital document management systems for various purposes: external and internal exchange, organizational-

administrative, personnel, law-making, commercial, industrial and other.

Digital signature can be used as an analogue of a handwritten signature or a seal on a paper document. DS technology is widely used in digital document management systems for various purposes: external and internal exchange, organizational-administrative, personnel, law-making, commercial, industrial and other.

In the internal document management system DS is used as a means of sighting and approval of digital documents within the framework of internal processes. Digital signatures are used to approve the contract between several parties.

When building an intercorporate document flow, the presence of DS is a critically important condition for the exchange, since it is the guarantor of legal force. Only in this case the digital document can be recognized as genuine and used as evidence in court proceedings.

The document signed by a reinforced digital signature can also be stored in a digital archive for a long time, while maintaining its legitimacy.

Digital signature is necessary for suppliers on state and commercial sites. DS suppliers and customers guarantee to the participants that they are dealing with real offers. In addition, concluded contracts become legal only when signed by both parties. If there is any dispute between the organizations, digital documents may be used as evidence in court.

Security of digital signatures is based on the complexity of discrete algorithm solution and the large integers factorization problem. As was mentioned above quantum computers will easily overcome this problem, that will cause the breaking of digital signatures, implying the absolute failure

3 LAMPORT–DIFFIE ONE-TIME SIGNATURE SCHEME

Lamport–Diffie one-time signature scheme is hash based digital signature, and represents an alternative for the post-quantum era.

Keys generation in this system occurs as follows: the signature key X of this system consists of 2n lines of length n, and is selected randomly.

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

$(x_{n-1}[0], x_{n-1}[1], \ldots, x_0[0], x_0[1]) \in \{0,1\}^{n,2n}$

Verification key Y of this system consists of 2n lines of length n, and is selected randomly.

$Y= (y_{n-1}[0], y_{n-1}[1], \ldots, y_0[0], y_0[1])$ (2)

$(y_{n-1}[0], y_{n-1}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{n,2n}$

This key is calculated as follows:

$y_i[j] = f(x_i[j])$, 0<=i<=n-1, j=0,1 (3)

f – is one-way function:

$f: \{0,1\}^n \rightarrow \{0,1\}^n$;

To generate the verification key, it is needed to use the function f 2n time.

Document signature:

To sign a message m of arbitrary size, it is transformed into size n using the hash function:

$h(m) = hash = (hash_{n-1}, \ldots , hash_0)$ (4)
Function h- is a cryptographic hash function:

$h: \{0,1\}^* \rightarrow \{0,1\}^n$

The signature is done as follows:

$sig= (x_{n-1}[hash_{n-1}], \ldots, x_0[hash_0]) \in \{0,1\}^{n,n}$ (5)

i-th string in this signature is equals to $x_i[0]$, if i-th bit in

sign is equal to 0. The string is equal to $x_i[1]$, if i-th bit in sign is equal to 1.

Signature length is n^2 and during signature f function is not used.

To verify the signature

$sig = (sig_{n-1}, \ldots, sig_0)$ (6)

is calculated hash of the message

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

and the following equality is checked:

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

If the equation is true, then the signature is correct.

For the verification f function must be used n times.

4 WINTERNITZ ONE TIME SIGNATURE SCHEME

So, in Lamport one-time signature scheme, key generation and signature generation are quite effective, the signature size is equal to n^2 - is quite large. Therefore, the Winternitz one-time signature scheme was proposed.

In this scheme, several bits of the hashed message are signed simultaneously with one string of the key, thereby significantly reducing the length of the signature [5-7].

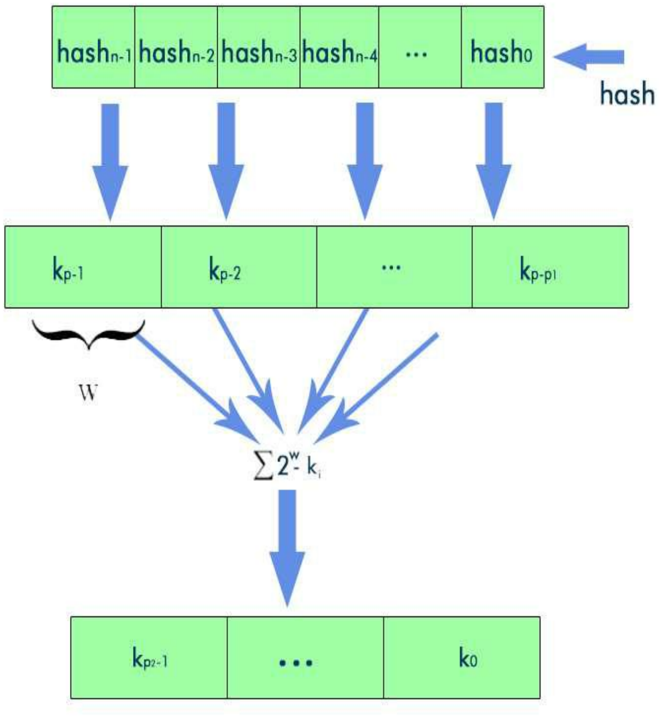

Figure 1. Winternitz signature

Keys generation in this system occurs as follows:

the signature key X of this system consists of p lines of length n, the key is selected randomly.

Winternitz parameter is selected w> = 2, it is equal to the number of bits to be signed simultaneously. Is calculated

$p_1= \lceil n/w \rceil$ (9);

and

$p_2= \lceil (\lfloor \log_2 P_1 \rfloor + 1+ w)/ w \rceil$ (10)

$p= p_1+ p_2$ (11)

The signature key X of this system consists of p lines of length n selected randomly:

$X= (x_{p-1}[0], \dots, x_0) \in \{0,1\}^{n,p}$ (12)

Verification key is following:

$Y= (y_{p-1}[0], \dots, y_0) \in \{0,1\}^{n,p}$ (13),

where

$y_i = f^{2{\wedge}w-1}(x_i)$, 0<=i<=p-1 (14)

The length of the signature and the verification key is equal to np bits, and to generate the verification key, function f must be used $p(2^w-1)$ times.

The signature is as follows:

The message is hashed

hash = h(m) (15)

and prepend to hash the minimum number of zeros in order to get the length of hash devisable by w. Afterwards it is divided into p1 parts of length w.

hash=$k_{p-1}, \dots, k_{p-p1}$ (16)

the checksum is calculated:

$c=\sum_{i=p-p1}^{p-1} 2^w - k_i$ (17)

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

The minimum number of zeros is prepended to its binary representation in order to get the length of representation devisable by w, and divide it into p2 parts of length w.

$c=k_{p2-1}, \dots, k_0$ (18)
the signature of the message m is calculated:

$sig = (f{\wedge}k_{p-1}(x_{p-1}), \dots, f{\wedge}k_0(x_0))$ (19)

In the worst case, for the signature function f must be used, $p(2^{w}-1)$ times.

Signature size is pn.

For signature verification

$sig = (sig_{n-1}, \ldots, sig_{0})$ (20)

bit strings are calculated $k_{p-1},\ldots, k_{0}$.

The following equality is verified:

$(f\hat{}(2^{w}-1-k_{p-1}))(sig_{n-1}), \ldots, (f\hat{}(2^{w}-1-k_{0}))(sig_{0}) =$

$= y_{n-1}, \ldots y_{0}$ (21)

If the signature is correct,

then $sig_{i} = f\hat{}k_{i}(x_{i})$ (22), so

$(f\hat{}(2^{w}-1-k_{i}))(sig_{i}) = (f\hat{}(2^{w}-1))(x_{i}) = y_{i}$ (23)

is equal for every $i = p-1,\ldots, 0$

In the worst case, for the signature verification function f must be used, $p\ (2^{w}-1)$ times.

	Lamport	**Winternitz**
Key size	$2n^{2}$	np
Using f for key generation	2n	$p(2^{w}-1)$
Signature length	n^{2}	np
Using f for signature generation	Not used	$p(2^{w}-1)$
Using f for signature verification	n	$p(2^{w}-1)$

Table 1. Comparison of the Lamport and Winternitz one-off signatures schemes

In Table 1 is illustrated that in Lamport one-time signature scheme (Lotss) the length of the key is $2n^{2}$ and in Winternitz one-time signature scheme (Wotss) the length of the key is np. The message length in Lotss is n^{2} and in Wotss is np.

When the key in Lotss is generated one-way function f must be used 2n times and in Wotss one-way function f must be used $p(2^{w}-1)$ times. When the message is signed in Lotss case f is not used at all, but in Wotss f is used $p(2^{w}-1)$ times. When in Lotss case the signature is verified one-way function f is used n times and in the case of Wotss f is used $p\ (2^{w}-1)$ times.

Because in Winternitz one time signature scheme the size of the signature is significantly reduced[8-10],

$np<n^2$, of course the length of the key is significantly reduced, because:

$np<n^2<2n^2$

Using f for keys generation

In the case of Winternitz signature f must be used $p(2^w-1)$ times, and in the case of Lamport signature – 2n times.

As in the case of Winternitz signature scheme the signature must be decreased, $np<n*n$ $p<n$.

In order to make the signature in Winternitz scheme much smaller, it is necessary to try to reduce the size of p.

Let’s analyze p

$p1 = \lceil n/w \rceil$ (24)

$p_2 = \lceil (\lfloor \log_2 p_1 \rfloor + 1+ w)/ w \rceil$ (25)

$p = p_1 + p_2$ (26)

$n/w \leq p_1 < n/w + 1$ (27)

n/w is minimum value of p1

n/w + 1 is always more than p1

$(\log_2 p_1 + w) / w < p_2 < (\log_2 p_1 + 1+ w)/w+1$ (28)

$(\log_2 p_1 + 1+ w)/ w +1 =(\log_2 p_1 + 1+ 2w)/w$ (29)

$(\log_2 p_1 + w) / w < p_2 < (\log_2 p_1 + 1+ 2w)/w$ (30)

$(\log_2 p_1 + w) / w$ is always less than p_2

$(\log_2 p_1 + 1+ 2w)/ w$ is always more than p_2

$p_1 + p_2 > (n + \log_2 n - \log_2 w + w)/w$ (31)

$p_1 + p_2 < (n+ \log_2 n - \log_2 w + 1+ w)/ w +2$ (32)

$(n + \log_2 n - \log_2 w + w)/w <p< (n+ \log_2 n - \log_2 w+ + 1+ \quad +w)/ w +2$ (33)

$(n + \log_2 n - \log_2 w + w)/w <p< (n+ \log_2 n - \log_2 w+ 1+ \quad + 3w)/ w$ (34)

$(n + \log_2 n - \log_2 w + w)/w$ is always less than p

$(n+ \log_2 n - \log_2 w + 1+ 3w)/ w$ is always more than p

In order to make these numbers significantly less than n, w must be chosen rather large.

But in the case of Winternitz signature f must be used p (2^w-1) times, so when w is increased, the number of using f needed for key generation in Winternitz signature increases exponentially. So this scheme is relevant in the case of Winternitz signature, if the number of using f significantly exceeds the given number in the case of Lamport signature.

Using f to generate the signature

The number of using f significantly exceeds this number in the case of using the Lamport scheme, because:

$p(2^w-1)>0$

Using f to verify the signature

The number of using f significantly exceeds this number in the case of using the Lamport scheme, because:

$p(2^w-1)>2n>n$

CONCLUSION

In our analyses is shown that, using Winternitz one-time signature scheme, the length of the signature and of the keys is substantially reduced. But also this scheme has disadvantages, in the case of generating keys, creating a signature and verifying a signature, one-way function should be used much more times, then in Lamport signature scheme. So, must be paid serious attention at the choice of this function, it should be quickly executed and safe.

One time digital signature schemes are used in implementation of Merkle signature scheme. Before integrating Winternitz one-time signature scheme Merkle, it is recommended to modify one way function. An effective and safe one way function must be chosen or created. This function must be integrated to Winternitz one-time signature scheme and only after this, it is recommended to use it in Merkle signature scheme.

ACKNOWLEDGEMENT

The Work Was Conducted As A Part Of Research Grant Of Shota Rustaveli NationalScience Foundation [№YS15_2.1.2_9] and Joint Project Of Shota Rustaveli NationalScience Foundation And Science & Technology Center In Ukraine [№ STCU-2016-08]

REFERENCES

1. Google is Closer Than Ever to a Quantum Computer Breakthrough https://futurism.com/google-is-closer-than-ever-to-a-quantum-computer-breakthrough/

2. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Eurasian Journal of Business and Management, 4(4), 2016, pp16-20

3. Gagnidze A.G., Iavich M.P., Iashvili G.U. Post-quantum cryptosystems // Modern scientific researches and innovations. 2016. № 5 [Electronic journal]. URL: http://web.snauka.ru/en/issues/2016/05/67264

4. Gagnidze A.G., Iavich M.P., Iashvili G.U. Improved version of Merkle crypto system // Modern scientific researches and innovations. 2017. № 5 [Electronic journal]. URL: http://web.snauka.ru/issues/2017/05/81949

5. E. Klintsevich, K. Okeya, C.Vuillaume, J. Buchmann, E.Dahmen. Merkle signatures with virtually unlimited signature capacity. 5th International Conference on Applied Cryptography and Network Security – ACNS07, 2007

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

7. D. Naor, A. Shenhav, and A. Wool. One-Time Signatures Revisited: HaveThey Become Practical? Technical Report 2005/442, Cryptology ePrintArchive, 2005. Available at http://eprint.iacr.org/2005/442/ CMSS - An Improved Merkle Signature Scheme. (PDF Download Available). Available from: https://www.researchgate.net/publication/221540869_CMSS_-_An_Improved_Merkle_Signature_Scheme.

8. R.C. Merkle, "A Certified Digital Signature," in Proceedings of Crypto 89, ser. Lecture Notes in Computer Science, G. Brassard, Ed., vol. 435. Springer-Verlag, 1989, pp. 218-238.

9. L. C. Coronado Garc´ıa. On the security and the efficiency of the merkle signature scheme. Technical Report 2005/192, Cryptology ePrint Archive, 2005. Available at http://eprint.iacr.org/2005/192/.

10. Chris Dods, Nigel Smart, and Martijn Stam. Hash based digital signature schemes. In Cryptography and Coding, pages 96–115. Springer Verlag LNCS 3796, November 2005.