საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 12, №2, 2018
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 12, no.2, 2018

Informatics

Naive Algorithm to Bos-Chaum One-Time Signature Scheme

Nick Inassaridze[*], Maksim Iavich[**], Emzar Khmaladze[§], George Iashvili[**]

[*]*A.Razmadze Mathematical Institute, Ivane Javakhishvili Tbilisi State University; Georgian Technical University;Tbilisi Centre for Mathematical Sciences, Tbilisi, Georgia*
[**]*Bank of Georgia University, Tbilisi, Georgia*
[§]*A.Razmadze Mathematical Institute, Ivane Javakhishvili Tbilisi State University; University of Georgia; Tbilisi Centre for Mathematical Sciences, Tbilisi, Georgia*

(Presented by Academy Member Hvedri Inassaridze)

ABSTRACT. Digital signature schemes are fundamental cryptographic primitives, which are building blocks in the design of secure protocols and other cryptographic objects. Digital signature is information in digital form, attached to another digital information, which should be signed. Digital signature associated with such information is used to identify the person signing this information. The main task of digital signature is to confirm the authorship of some document and to confirm that the document was not changed after it was signed. The traditional digital signature schemes that are used now are vulnerable to quantum computers attacks since their security is based on the problems of factoring large composite integers and computing discrete logarithms. E.g. the RSA scheme with four thousand-bit keys is considered useful to protect information from attacks of classic computers, but is not safe against attacks of quantum computers.Hash-based digital signature schemes offer a very promising alternative to RSA and elliptic curve signature schemes, which were invented by Merkle. Merkle started from fundamental, one-time signature scheme proposed by Lamport and Diffie. One-time signature schemes have found numerous applications: in ordinary, online/offline, and forward-secure signatures, in multicast and broadcast authentication.One-time signature schemes proposed by Bos and Chaum and by Reyzin and Reyzin generalizing that of Lamport and Diffie, are safe against attacks of quantum computers. In this article we give a naive algorithm of the mapping S, computation of which is the most expensive part of the Bos-Chaum's and Reyzin-Reyzin's schemes. We show that our algorithm of computation of function *S* is linear time and the Bos-Chaum scheme with our algorithm incorporated could be used in the construction of the Merkle tree.

Key words: one-time signature scheme, mapping S, algorithm

Nowadays digital signatures have become a key technology for making the internet and other IT-infrastructures secure. Instead of outdated traditional physical signatures, digital signatures are turning more important tools to implement secure and correct signs. Providing authenticity, integrity, and non-repudiation of data, digital signatures are widely used in identification and authentication protocols.

Therefore, the existence of secure signature algorithms is crucial for maintaining IT-security. The digital signature algorithms that are used in practice today are RSA [1], DSA [2], and ECDSA [3]. They are not quantum immune since their security relies on the difficulty of factoring large composite integers and computing discrete logarithms.

Hash-based digital signature schemes offer a very promising alternative to RSA and elliptic curve signature schemes, which were invented by Merkle [4]. Merkle started from fundamental, one-time signature schemes from [5]. One-time signature schemes proposed by Lamport-Diffie and Rabin [6] were among the earliest signatures based on the idea of committing to private keys by one-way functions.

In this article we discuss one-time digital signature schemes proposed by Bos and Chaum [6] and Reyzin and Reyzin [7] generalizing that of previously invented by Lamport and Diffie. In Section 2 we recall the schemes of Bos and Chaum and Reyzin and Reyzin. In Section 3 we give our algorithm of the mapping S and calculate its efficiency, showing that with it the scheme of Bos and Chaum is similar to that of Lamport and Diffie and can be used in the multiple-time signature scheme of Merkle.

Bos-Chaum and Reyzin-Reyzin One-Time Signature Schemes. In this section we recall the one-time digital signature scheme proposed by Reyzin and Reyzin, called the RR scheme, and which is a generalization of that given by Bos and Chaum.

Let *b, t, k* be integers such that $\binom{t}{k} \geq 2^b$. Let [*t*] denote the set {1, 2, ... , *t*} while I_t^k denote the set of k-subsets of [*t*]. Let $g : \{0,1\}^* \to \{0,1\}^b$ be a cryptographic hash function and $S : \{0,1\}^b \to I_t^k$ an injective mapping. Let $f : \{0,1\}^l \to \{0,1\}^l$ be a one-way function operating on *l*-bits strings, for a security parameter 1^l. The RR scheme works as follows:

Key generation. For the given security parameter 1^l, the private key k_{priv} consists of random *t* bit strings of length *l*

$$k_{priv} = (s_1, \ldots, s_t)$$

Then the public key of the scheme is

$$k_{pub} = (v_1, \ldots, v_t),$$

where $v_i = f(s_i), i \in [t]$.

Signature generation. A message $m \in \{0,1\}^*$ is signed using the private key k_{priv}. At first the message digest $g(m) \in \{0,1\}^b$ of m is computed. Next the mapping S is used to compute. Then the $S(g(m)) = \{i_{1,\ldots,} i_k\} \in I_t^k$ signature of the scheme is given as a sequence $(S_{i_1}, \ldots, S_{i_k})$.

Signature verification. To verify a signature $(s_1^{'}, \ldots, s_k^{'})$ on a message *m*, again $S(g(m)) = \{i_1, \ldots, i_k\} \in I_t^k$ is calculated. Finally, it is checked whether

$$(f(s_1^{'}), \ldots, f(s_k^{'})) = (v_{i_1}, \ldots, v_{i_k}).$$

As we have already mentioned, the RR scheme generalizes the one-time signature scheme proposed by Bos and Chaum [6], if $t=2k$, which in turn is a generalization of the scheme of Lamport and Diffie [5], if $b=k$ and the mapping S is given by the algorithm: for any bit string $m = (m_1, \ldots, m_k)$ of length *k*, compute S(*m*) as $\{1 + m_1, \ldots, 2k - 1 + m_k\}$.

Security. It is easy to see that each message corresponds to a different *k*-element subset of the set I_t^k. Hence, in order to existentially forge a signature on a new message after a one-time adaptive chosen message attack, the adversary is forced to invert the one-way function *f* on at least one of the $t - k$ values in the

public key for which the corresponding value in the secret key has not been revealed. Thus, the security of this scheme relies on one-wayness of *f*.

Looking at the efficiency of this scheme, one deduces that the key generation requires t evaluations of one-way function. The private and public key size is tl bits. The signature is kl bit long. The signing and verifying algorithms take as long as the running time of the algorithm for the mapping S. Reyzin and Reyzin gave two algorithms for implementation of the mapping S:

Algorithm 1. It is based on the following equation:

$$\binom{t}{k} = \binom{t-1}{k-1} + \binom{t-1}{k}$$

and has the computation cost of $0(tk\log^2(t))$, provided $0(k^2\log^2(t))$ bits extra storage available.

Algorithm 2. It is based on the following more complicated equation:

$$\binom{t}{k} = \sum_{i=0}^{k} \binom{[t/2]}{i} \binom{[t/2]}{k-i}$$

and has the computation cost of $0(k^2\log(t)\log(k))$, provided $0(k^2\log^2(t))$ bits extra storage available.

Hence, it is obvious that the most expensive part of this scheme is the computation of the function *S* [2,8].

New Algorithm of *S* Mapping. In this section we present a naive algorithm for the mapping S used in the digital signature schemes of Bos-Chaum and Reyzin-Reyzin from previous section, obtaining a Lamport-Diffie type signature scheme.

Our Algorithm. We compute the mapping

$$S : \{0,1\}^k \to I_{2k}^{k}$$

for any even integer $k > 0$ as follows:

Let v be an element of $\{0,1\}^k$, presented as $v = (v_1,...,v_k)$ with $v_i \in \{0,1\}$, $i \in [k]$. Let $v_{i_1}, v_{i_2},...,v_{i_r}$ be the only 1-s, with $i_1 < i_2 < \cdots < i_r$.

(Step 1) If $r \geq \frac{k}{2}$, then $i_{r+j} = i_j + k$ for all $j \in [k-r]$. Then define

$$S(v) = (i_1,...,i_k)$$

and the algorithm terminates;

(Step 2) Otherwise, $r < \frac{k}{2}$, so set $i_{r+j} = i_j + k$ for all $j \in [r]$;

(Step 3) Set $p = 1$;

(Step 4) If $k + p < i_{r+p}$, then set $i_{r+j+1} = i_{r+j}$ for all $p \leq j \leq r$ and $i_{r+p} = k + p$; if (number of i_j-s) $+1 = k$, then define

$$S(v) = (i_1,...,i_k)$$

and the algorithm terminates;

(Step 5) Otherwise, set $p = p + 1$ and go to the (Step 4)

Theorem 1. *The mapping S defined above in Our Algorithm is one-to-one, while the algorithm itself is deterministic and polynomial-time with the k-bit input and computational cost of* $0(k)$.

Proof. It is clear that the algorithm is deterministic.

According to the algorithm's (Step 1), if $r \geq \frac{k}{2}$, the algorithm executes at most $\frac{k}{2}$ cycles performing arithmetic operation. Otherwise, if $r < \frac{k}{2}$, according to the algorithm's (Step 2-5), it executes at most $r + k$ cycles performing arithmetic operation. Hence the computation cost of the algorithm is *0(k)*.

Now we have to show that for any $v, v' \in \{0,1\}^k$ with $v \neq v'$ we have

$$S(v) \not\subset S(v').$$

Suppose $v' = (v'_1, ..., v'_k)$ with $v^i_j \in \{0,1\}, j \in [n]$ such that $v'_{j_1}, v'_{j_2}, ...v'_{j_p}$ be the only 1-s, with $j_1 < j_2 < \cdots < j_p$.

Case I: If $\{i_1, i_2, ..., i_r\} \not\subseteq \{j_1, j_2, ..., j_p\}$, then according to the algorithm's (Step 1, 2, 4) the calculation of *S(v)* and *S(v')* implies $\{i_1, i_2, ..., i_k\} \not\subseteq \{j_1, j_2, ..., j_k\}$ which means that our claim is proven.

Case II: Suppose that $\{i_1, i_2, .., j_r\} \subset \{j_1, j_2, ..., j_p\}$. It is easy to see that $p > r$ implying $k - r > k - p$. Hence we have $|\{i_{r+1}, i_{r+2}, ..., i_k\}| > |\{j_{p+1}, j_{p+2}, ..., j_k\}|$. Using the algorithm's (Step 1, 2, 4), we have also the inclusions $\{i_{r+1}, i_{r+2}, ..., j_k\}, \{j_{p+1}, j_{p+2}, ...j_k\} \subseteq \{k+1, k+2, ..., 2k\}$. It is clear that $\{i_{r+1}, i_{r+2}, ..., j_k\} \not\subseteq \{j_1, j_2, ...j_k\}$ implying the correctness of our claim in this case.

Conclusion. Since the most expensive part of the schemes of Bos-Chaum and Reyzin-Reyzin is the computation of the function *S* and our algorithm of computation of *S* is linear time, it could be incorporated in the scheme of Bos-Chaum and used with the same success as the original scheme of Lamport and Diffie, namely in the construction of the Merkle tree.

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, Project N6321[STCU-2016-08].

ინფორმატიკა

ნაივური ალგორითმი ბოს-ჩაუმის ერთჯერადი ხელმოწერის სქემისათვის

ნ. ინასარიძე*, მ. იავიჩი**, ე. ხმალაძე§, გ. იაშვილი**

*ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, ა.რაზმაძის მათემატიკის ინსტიტუტი; საქართველოს ტექნიკური უნივერსიტეტი; თბილისის მათემატიკის მეცნიერების ცენტრი, თბილისი, საქართველო

**საქართველოს განკის უნივერსიტეტი, თბილისი, საქართველო

§ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, ა.რაზმაძის მათემატიკის ინსტიტუტი; საქართველოს უნივერსიტეტი; თბილისის მათემატიკის მეცნიერების ცენტრი, თბილისი, საქართველო

(წარმოდგენილია აკადემიის წევრის ხ. ინასარიძის მიერ)

ციფრული ხელმოწერების სქემები ფუნდამენტური კრიპტოგრაფიული პრიმიტივებია, რომლებიც წარმოადგენს უსაფრთხო პროტოკოლებისა და სხვა კრიპტოგრაფიული ობიექტების დიზაინის სტრუქტურულ ელემენტებს. ციფრული ხელმოწერა არის ინფორმაცია ციფრულ ფორმატში, მიმაგრებული სხვა ციფრულ ინფორმაციასთან, რომელიც უნდა იყოს ხელმოწერილი. ციფრული ხელმოწერა დაკავშირებულია რა ამ ინფორმაციასთან, გამოიყენება ხელმომწერი პირის იდენტიფიცირებისთვის. ციფრული ხელმოწერის ძირითადი ამოცანაა დაადასტუროს დოკუმენტის მფლობელობა და დაადასტუროს, რომ დოკუმენტი ხელმოწერის შემდეგ არ შეცვლილა.

ტრადიციული ელექტრონული ხელმოწერების სქემები, რომლებიც ამჟამად გამოიყენება, არის სუსტი კვანტური კომპიუტერების თავდასხმების წინააღმდეგ, რადგან მათი უსაფრთხოება ეფუძნება დიდი შედგენილი მთელი რიცხვების ფაქტორიზაციის და დისკრეტული ლოგარითმების გამოთვლის პრობლემებს. **RSA**-ის სქემა ოთხი ათას-ბიტიანი გასაღებებით ითვლება ეფექტურად კლასიკური კომპიუტერების თავდასხმების წინააღმდეგ, მაგრამ იგი არ არის უსაფრთხო კვანტური კომპიუტერების თავდასხმების მიმართ.ჰეშზე დაფუძნებული ციფრული ხელმოწერების სქემები გვთავაზობს **RSA**-ის და ელიფსური წირების ხელმოწერების სქემების ძალიან პერსპექტიულ ალტერნატივას, რომელიც გამოგონილ იქნა **Merkle**-ს მიერ. **Merkle**-დან დაიწყო ფუნდამენტური, ერთჯერადი ხელმოწერის სქემით, რომელიც შემოთავაზებლ იქნა **Lamport** და **Diffie**-ის მიერ. ერთჯერადი ხელმოწერების სქემებმა ნახეს მრავალი გამოყენება: ჩვეულებრივ, **online/offline** და **forward-secure** ხელმოწერებში, **multicast** და **broadcast** აუთენტიფიკაციაში. ერთჯერადი ხელმოწერების სქემები, შემუშავებული **Bos** და **Chaum**-ის და **Reyzin Reyzin**-ის მიერ, რომლებიც ან ზოგადებენ **Lamport** და **Diffie**-ის სქემას, უსაფრთხოა კვანტური კომპიუტერების თავდასხმების მიმართ. წინამდებარე სტატიაში ჩვენ წარმოვადგენთ **S** ფუნქციის ნაივურ ალგორითმს, რომლის გამოთვლა **Bos-Chaum**-ის და **Reyzin-Reyzin**-ის სქემების ყველაზე ტევადი ნაწილია. ჩვენ ვაჩვენებთ, რომ **S** ფუნქციის გამოთვლის ჩვენი ალგორითმი არის წრფივი დროის და **Bos-Chaum**-ის სქემა ჩვენი ალგორითმით შესაძლებელია გამოყენებულ იქნეს **Merkle**-ს ხის კონსტრუქციაში.

REFERENCES

1. Rivest R. L., Shamir A. and Adleman L. (1978) A method for obtaining digital signatures and public-key Cryptosystems. *Communications of the ACM*, 21 (2): 120-126.
2. El Gamal T. (1985) A public key cryptosystem and a signature scheme based on discrete logarithms, advances in cryptology CRYPTO'84. *Lecture Notes in Comp. Sci,* 196 :10-18, Springer.
3. Johnson D. and Menezes A. (1999) The elliptic curve digital signature algorithm (ECDSA). *Technical Report CORR* 99-34, University of Waterloo.
4. Merkle R. C. (1989) A certified digital signature, Advances in cryptology CRYPTO '89. *Lecture Notes in Comp. Sci*, 435: 218-238, Springer.
5. Lamport L. (1979) Constructing digital signatures from a one way function. *Technical Report SRI-CSL*-98. SRI International Computer Science Laboratory.
6. Bos J. N. E. and Chaum D. (1993) Provably unforgeable signatures. Advances in Cryptology CRYPTO'92. *Lecture Notes in Comp. Sci.* 740:1-14, Springer.
7. Reyzin L. and Reyzin N. (1989) Short one-time signatures with fast signing and verifying, Information security and privacy (ACISP02). *Lecture Notes in Comp. Sci*. 2384: 144-153, Springer.
8. Rabin M. O. (1978) Digitalized signatures, foundations of secure communication, 155-168. MIT, Cambridge, USA.
9. Bernstein D. J., Buchmann J., Dahmen E. (2009) Post-quantum cryptography, Springer-Verlag, Berlin, Heidelberg.
10. Rompel J. (1990) One-way functions are necessary and sufficient for secure signatures. *Proceedings of ACM STOC* 90: 387-394.

Received April, 2018