A NEW METHOD FOR CONSTRUCTING DIGITAL SIGNATURE SCHEME BASED ON NEW HARD PROBLEM

The Truyen Bui[1], *Duc Thuy Nguyen*[2], *Hong Dung Luu*[1], *Khac Huan Dao*[3,*]

doi:10.56651/lqdtu.jst.v11.n02.535.ict

Abstract

Research in the field of public key cryptography in general and digital signatures in particular is often considered and evaluated at two levels: The first level is considering the mathematical basis for constructing cryptographic and digital signature algorithms, especially these difficult problems: factorizing a large integer into prime factors, finding root problem, discrete logarithm problem, discrete logarithm problem on elliptic curve... The second level is constructing cryptographic and digital signatures algorithms on these hard problems including RSA, DSA, Schnorr, GOST R34.10-94.

At the first level, research focuses mainly on improving algorithms for finding large primes, structures for strong primes and algorithms to attack these problems efficiently. At the second level, the research concentrates on improving the existing algorithms to enhance the safety or effective performance of the algorithm.

In this article, the authors propose a solution to improve the security of digital signature schemes, implemented in both levels of digital signatures. At the first level, the authors propose a new hard problem - different from the hard problems used before and hasn't been solved by anyone so far (except by "brute force attack" method). At the second level, the authors propose a method to construct new digital signature algorithms that can help create not only one but also a family of new digital signature algorithms with high security level for practical applications.

Index terms

Digital signature, digital signature scheme, discrete logarithm problem, dinding root problem, discrete logarithm combining finding root problem.

1. Introduction

Digital signatures have now been widely applied in fields such as e-Government, e-commerce, etc. or in telecommunications systems and computer networks. However, the research and development of digital signature schemes to improve the security of

[1]Faculty of Information Technology, Le Quy Don Technical University.
[2]Faculty of Information Technology, Ho Chi Minh City Technical and Economic College, HCM city, Vietnam.
[3]Institute of Information Technology, 17 Hoang Sam, Cau Giay, Hanoi, Vietnam.
[*]Corresponding author, email: generalhuan@gmail.com.

the algorithm are always necessary when the ability to attack public-key cryptosystems in general and digital signature systems, in particular, are continuously increasing as a result of developments in electronic technology and information technology.

Through the published research results [1] - [8], it can be seen that the basic solution to improve the security of signature schemes is based on the difficulty of solving simultaneously two problems, which are the problem of analyzing a large integer into prime factors and the problem of discrete logarithms on prime finite field F_p. However, in the authors' opinion, this approach is not practical. Because when one of the two problems still has no practical solution (no polynomial-time algorithm), the simultaneous use of two problems will significantly reduce the performance of the signature algorithm. Furthermore, once an attacker has the ability to solve one problem, he will also be able to solve the other.

In this article, a new hard problem that currently has no mathematical solution is proposed, as a basis for constructing digital signature algorithms. Here, it is called the discrete logarithm combining finding root problem on F_p). The authors also propose a new method to constructing digital signature algorithms based on this new hard problem by designing a specific signature scheme. This method can be used to generate a family of digital signature schemes similar to the ElGamal signature family [9].

2. Discrete logarit combining finding root problem on F_p

From the discrete logarithm problem F_p [10]:

$$g^x \bmod p = y$$

We see that if the parameter g is also kept secret, then the discrete logarithm problem on F_p will become an unsolvable problem, here called the discrete logarithm combined finding root problem. In the simplest case, it is possible to choose the secret key x itself for the role of the parameter g, then the discrete logarithm problem combined with root extraction is stated in the first form as follows:

a. *Given p is a prime number, for each positive integer y in F_p, find the number x that satisfies the following equation:*

$$x^x \bmod p = y$$

On the other hand, if the right side of the equation:

$$g^x \bmod p = y$$

is also a variable of the form $x^b \bmod p$, then the discrete logarithm problem on F_p also becomes an unsolvable problem. From this, the discrete logarithms combined with finding root problem can be stated in the second form as follows:

b. *Given p is a prime number, and a, b are positive integers in F_p, find the number x that satisfies the following equation:*

$$a^x \equiv x^b \bmod p$$

It is easy to see those existing algorithms for the discrete logarithm problem or rooting on F_p cannot be used to solve this problem. At present, there is no other solution to this problem other than the "brute force attack" method with computational complexity $\boldsymbol{O}(2^n)$, where $n = |p|$.
In the proposed digital signature scheme construction method, the first form of the hard problem is used to generate the public and private key pairs of the signer in the Key generation algorithm, while the second form of this hard problem is used as the basis for construction the Verification algorithm.

3. Construction digital signature scheme based on the discrete logarithms combined with finding root problem

In this section, the method of construction new digital signature algorithm is presented through design a specific signature scheme, including:

3.1. Key Generation Algorithm

The prime numbers p and q as system or domain parameters are chosen similarly to the US DSS [11] standard or the Russian Federation GOST R34-90.10 [12]. To generate a private or public key pair, each signer first needs to choose a value which $\alpha \in \mathbb{Z}_p^*$, then compute the secret key x according to the formula:

$$x = \alpha^{\frac{p-1}{q}} \bmod p$$

The public key y is generated from x and p as:

$$y = x^{-x} \bmod p \tag{1}$$

The algorithm for generating parameters and keys is described as follows:

Algorithm 1:

Input: L_p, L_q.
Output: p, q, x, y.

1 **generate:** p, q : len$(p) = L_p$, len$(q) = L_q, q|(p-1)$
2 **select** $\alpha : 1 < \alpha < p$
3 $x \leftarrow \alpha^{\frac{p-1}{q}} \bmod p$
4 $y \leftarrow x^{-x} \bmod p$
5 **if** *(*$y = 1$ ***OR*** $gcd(y, p-1) = 1$*)* **then**
6 | **go to** 2
7 **return** $\{p, q, x, y\}$

Note:

- len(.): function to calculate length (in bits) of an integer.

- L_p, L_q: length (in bits) of prime numbers p and q.
- p, q : system parameter/domain parameters.
- x, y : private key and public key of the signer.

3.2. Signing algorithm

Assuming (r, s, z) is the signature on the message to be signed M and the condition for (r, s, z) to be recognized as valid, also means is the message M authenticated for origin and integrity:

$$(r)^z \equiv (z)^{s \times e} \times (y)^{r \times z^s} \bmod p \tag{2}$$

where e is the representative value of the message to be signed M (the hash value of M). The z component of the signature is calculated according to the following formula:

$$z = x^k \bmod p \tag{3}$$

where k is a randomly chosen value in the range $(1, q)$.

Also, assume that the component r is generated from a value u according to the formula:

$$r = (z)^u \bmod p, \tag{4}$$

where u is also a randomly chosen value in the range $(1, q)$.

The generation of the s component of the signature is done as follows:

Based on (3) and (4) we have:

$$r \times (z)^s \bmod p = z^{u+s} \bmod p. \tag{5}$$

Set

$$t = (u + s) \bmod q \tag{6}$$

then (5) will become:

$$r \times (z)^s \bmod p = z^t \bmod p \tag{7}$$

From (1), (3), (4) and (7) we have:

$$(x)^{k \times u \times z} \equiv (x)^{k \times s \times e} \times (x)^{-x \times (z^t \bmod p)} \bmod p \tag{8}$$

From (8) we deduce:

$$k \times u \times z \equiv \left(k \times s \times e - x \times (z^t \bmod p)\right) \bmod q \tag{9}$$

On the other hand, from (6) we have:

$$u = (t - s) \bmod q \tag{10}$$

Substituting (10) into (9) we get:

$$k \times z \times (t - s) \equiv \left(k \times s \times e - x \times (z^t \bmod p)\right) \bmod q \tag{11}$$

Then we deduce:

$$s = \left[k \times t \times z + x \times (z^t \bmod p)\right] \times [k \times (e + z)]^{-1} \bmod q \tag{12}$$

From (10) and (12), the r value is calculated according to:

$$r = (z)^{t-s} \bmod p \tag{13}$$

Then the signing algorithm is described as follows:

Algorithm 2:

Input: p, q, x, y, M.
Output: (r, s, z)

1 $e = H(M)$
2 **select** $k, t : 1 < k, t < q$
3 $z = x^k \bmod p$
4 $s = [k \times t \times z + x \times (z^t \bmod p)] \times [k \times (e + z)]^{-1} \bmod q$
5 $r = (z)^{t-s} \bmod p$.
6 **return** (r, s, z)

Note:

- M : message to sig, with $M \in \{0, 1\}^{\infty}$.
- $H(.)$: hash function with $H : \{0, 1\}^* \longmapsto \mathbb{Z}_h, q < h < p$.
- (r, s, z) : signature on M.

3.3. Verification algorithm

The verification algorithm of the schema is construction on the assumption:

$$(r)^z \equiv (z)^{s \times e} \times (y)^{(r \times z^s) \bmod p} \bmod p \tag{14}$$

That is, if M and the signature (r, s, z) satisfy the equality (14), then the signature is considered valid, and the message is verified for origin and integrity. Otherwise, the signature is considered forged, and the message to be verified is denied in terms of origin and integrity. Therefore, if the left-hand side of the verification equality is computed as:

$$A = (r)^z \bmod p$$

And the right-hand side of the verification equality is:

$$B = (z)^{s \times e} \times (y)^{(r \times z^s) \bmod p} \bmod p$$

Then the condition for a valid signature is: $A = B$.

The verification algorithm of the schema is described as follows:

Algorithm 3:

Input: $p, q, y, M, (r, s, z)$.
Output: *TRUE, FALSE.*

$e = H(M)$
$A = (r)^z \bmod p$
$B = (z)^{s \times e} \times (y)^{(r \times z^s) \bmod p} \bmod p.$
if $(A = B)$ **then**
  return (TRUE)
else
  return (FALSE)
end

Note:

- $M, (r, s)$: message and signatures to be verified.
- If the result is TRUE, then the integrity and origin of M are asserted. Otherwise, if the result is FALSE, then M is denied for origin and integrity.

3.4. The correctness of the proposed new schema

What needs to be proved here is: if

$$A = (r)^z \bmod p \tag{15}$$

and

$$B = (z)^{s \times e} \times (y)^{(r \times z^s) \bmod p} \bmod p \tag{16}$$

then $A = B$. Indeed, substituting (3) and (13) into (15) we have:

$$A = x^{k \times z \times (t-s)} \bmod p.$$

Similarly, substituting (1), (3) and (7) into (16) we get:

$$B = x^{k \times s \times e - x \times (z^t \bmod p)} \bmod p.$$

Now what to prove would be:

$$k \times z \times (t - s) \equiv \left[k \times s \times e - x \times (z^t \bmod p)\right] \bmod q$$

It is equivalent to:

$$k \times z \times t + x \times (z^t \bmod p) \equiv s \times [k \times (e + z)] \bmod q.$$

Therefore, it can be re-stated what needs to be proved as follows: if

$$C = k \times z \times t + x \times (z^t \bmod p) \bmod q \tag{17}$$

and

$$D = s \times [k \times (e + z)]^{-1} \bmod q \tag{18}$$

then $C = D$.

Indeed, substituting (12) into (18) we get:

$$\begin{aligned} D &= \left[k \times t \times z + x \times (z^t \bmod p)\right] \times [k \times (e+z)]^{-1} \times [k \times (e+z)] \bmod q \\ &= \left[k \times t \times z + x \times (z^t \bmod p)\right] \bmod q. \end{aligned} \tag{19}$$

From (17) and (19) we deduce: $C = D$. Thus, the correctness of the schema has been proved.

3.5. Security level of the new signature scheme

The security level of the new signature scheme can be assessed through its ability to resist some types of attacks such as:

a. Secret key attack

A secret key attack can be made on the key generation algorithm (Algorithm 1) and the steps 2, 4 of the signing algorithm (Algorithm 2). In step 3 of the Signing algorithm, since k is also a secret parameter, finding x from step 3 of the Signing algorithm is as difficult as finding x from the Key generation algorithm, which is a hard problem with no solution. In step 4 of the Signing algorithm, in addition to x being the secret parameter to be found, k and t are also secret parameters, so finding x from step 4 of the Signing algorithm is impossible now. Thus, to find the secret key, the attacker is forced to solve the above hard problem by the "brute force attack" method with a computational complexity of $\boldsymbol{O}(2^n)$ where $n = |p|$.

b. Signature forgery attack

From the verification algorithm (Algorithm 3) of the proposed new scheme, a set of 3 values (r, s, z) will be recognized as a valid signature with the message to be verified M if the following condition is satisfied:

$$(r)^z \equiv (z)^{s \times e} \times (y)^{(r \times z^s) \bmod p} \bmod p \tag{20}$$

From (20) we see that, pre-selecting 2 out of 3 values (r, s, z) and then calculating the remaining 3rd value is the 2nd form of the hard problem mentioned in Section 2, as it is known this is a type of hard problem that currently in mathematics there is no other solution than the "brute force attack" method.

Thus, to generate a forged signature corresponding to a given message, the attacker has no choice but to randomly choose a set of three values (r, s, z) satisfying (20), which in fact, this is also an " brute force attack" method.

3.6. The performance of the proposed signature scheme

The performance of the scheme proposed here is basically evaluated by comparing the computational cost of this scheme with the computational cost of the DSA digital signature scheme in the US DSS standard [11] and GOST R34.10-94 of the Russian Federation [9].

The computational cost or cost is the number of operations to be performed, where the symbols are defined as follows:

N_{exp} : the number of modulo exponentiations,
N_{mul} : the number of modulo multiplications,
N_{inv} : the number of modulo division (inversion),
N_h : the number of hash operations.

Note:

The algorithm for generating parameters and keys only needs to be done once for every schema. Therefore, the computational cost for the key and parameter generation algorithms can be ignored when comparing the costs of the schemas.

The cost for the signing algorithm and the verification algorithm of the DSA and GOST schema R34.10-94 compared with the proposed scheme (LQD V22.09-10) is shown in table 1 and table 2 as follows:

Table 1. Cost of signing algorithms

	N_{exp}	N_{mul}	N_{inv}	N_h
DSA	1	2	1	1
GOST R34-10.94	1	2	0	1
LQD V22.09-10	2	3	2	2

Table 2. Cost of verification algorithms

	N_{exp}	N_{mul}	N_{inv}	N_h
DSA	2	3	1	1
GOST R34-10.94	3	3	0	1
LQD V22.09-10	3	2	0	2

Comment: Comparing the cost of the proposed new scheme (LQD V22.09-10) with the DSA and GOST schemes R34.10-94 as shown in table 1 and table 2, it shows that the performance of the proposed scheme is lower than that of DSA and GOST R34.10-94. It can be seen that this is the cost of improving the security of the proposed scheme.

4. Conclusion

In this article, the authors propose a solution to improve the security of the digital signature scheme based on a new type of hard problem, which is developed from the discrete logarithm problem and the finding root problem, should be called a discrete logarithm combining finding roots problem on the finite field F_p. Currently, this is a hard problem that belongs to the class of unsolvable problems. On the other hand, the signature scheme construction here is carried out according to a completely new

method, which is also an important factor allowing to improve the security of the digital signature scheme according to this new solution. From the proposed new solution, it is possible to generate a family of highly security digital signature schemes suitable for different choices in practical applications.

References

[1] W. Qiu-xin, Y. Yi-xian, and H. Zheng-ming, "New signature schemes based on discrete logarithms and factoring," *Journal of Beijing University of Posts and Telecommunications*, vol. 24, no. 1, p. 61, 2001.

[2] Z. Shen and X. Yu, "Digital signature scheme based on discrete logarithms and factoring," *Information Technology*, vol. 28, pp. 21–22, 2004.

[3] S. Wei, "Digital signature scheme based on two hard problems," *International Journal of Computer Science and Network Security*, vol. 7, no. 12, pp. 207–209, 2007.

[4] E. S. Ismail, N. Tahat, and R. R. Ahmad, "A new digital signature scheme based on factoring and discrete logarithms," *Journal of mathematics and statistics*, vol. 4, no. 4, p. 222, 2008.

[5] Q. Yanlin and W. Xiaoping, "New digital signature scheme based on both ecdlp and ifp," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009. doi: 10.1109/ICCSIT.2009.5234697 pp. 348–351.

[6] S. Verma and B. K. Sharma, "A new digital signature scheme based on two hard problems," *International Journal of Pure and Applied Sciences and Technology*, vol. 5, no. 2, pp. 55–59, 2011.

[7] S. Vishnoi and V. Shrivastava, "A new digital signature algorithm based on factorization and discrete logarithm problem," *International Journal of Computer Trends and Technology*, vol. 3, no. 4, pp. 653–657, 2012.

[8] A. Berezin, N. Moldovyan, and V. Shcherbacov, "Cryptoschemes based on dificulty of simultaneous solving two diferent dificult problems," *Computer Science Journal of Moldova*, vol. 62, no. 2, pp. 280–290, 2013.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985. doi: 10.1109/TIT.1985.1057074

[10] P. C. Van Oorschot, A. J. Menezes, and S. A. Vanstone, "Handbook of applied cryptography," 1997. doi: 10.1201/9780429466335

[11] C. F. Kerry and P. D. Gallagher, "Digital signature standard (dss)," *FIPS PUB*, pp. 186–4, 2013. doi: 10.6028/NIST.FIPS.186-4

[12] R. GOST, "R34.10-94. russian federation standard," *Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm. Government Committee of the Russia for Standards*, 1994.

Manuscript received 03-06-2022; Accepted 28-10-2022.

■

The Truyen Bui graduated from Le Quy Don Technical University in 2000. He received a doctor's degree in analysis and information processing at Moscow Aviation Institute, Russia in 2008. Currently, he is a lecturer at the Le Quy Don Technical University. His research interests are virtual reality simulation and information security. E-mail: truyenbuithe@lqdtu.edu.vn

Duc Thuy Nguyen graduated in Ho Chi Minh city University of Foreign Languages-Information Technology in 2005, Master degree from Academy of Economics and Business in 2013; Currently working in the Faculty of Information Technology - Ho Chi Minh City Technical and Economic College; Research field: information security. E-mail: thuyphulam2013@gmail.com

Hong Dung Luu graduated in Electronics and Communications from Le Quy Don Technical University in 1989, PhD at Le Quy Don Technical University in 2013; Currently working in the IT department - Le Quy Don Technical University; Research direction: Cryptography and information security. E-mail: luuhongdung@gmail.com

Khac Huan Dao graduated in Mathematics from University of Science - Vietnam National Univesity in 2003, Master at University of Science - Vietnam National Univesity in 2011; Currently working in the Institute of Information Technology - Institute of Military Science and Technology; Research field: Information technology, Theory of Probability and Statistic.

MỘT PHƯƠNG PHÁP XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ DỰA TRÊN BÀI TOÁN KHÓ MỚI

Bùi Thế Truyền, Nguyễn Đức Thụy, Lưu Hồng Dũng, Đào Khắc Huân

Tóm tắt

Các kết quả nghiên cứu trong lĩnh vực mật mã khóa công khai nói chung và chữ ký số nói riêng thường được xem xét và đánh giá ở hai cấp độ: Cấp độ thứ nhất là cơ sở toán học để xây dựng các thuật toán mật mã và chữ ký số. Cụ thể là các bài toán khó như: bài toán phân tích một số nguyên lớn thành các thừa số nguyên tố, bài toán logarit rời rạc, bài toán khai căn, bài toán logarit rời rạc trên đường cong elliptic,... Cấp độ thứ hai là xây dựng các thuật toán mật mã và chữ ký số trên những bài toán khó này, mà với chữ ký số thì điển hình là các thuật toán như: RSA, DSA, Schnorr, GOST R34.10-94.

Ở cấp độ đầu tiên, các nghiên cứu tập trung chủ yếu vào việc cải tiến các thuật toán tìm số nguyên tố lớn, tìm cấu trúc cho các số nguyên tố mạnh hoặc phát triển các thuật toán để tấn công những bài toán khó này một cách hiệu quả. Ở cấp độ thứ hai, các nghiên cứu chủ yếu là cải tiến các thuật toán hiện có để nâng cao độ an toàn hoặc hiệu quả thực hiện của thuật toán.

Trong bài báo này, nhóm tác giả đề xuất một giải pháp nhằm nâng cao tính bảo mật của lược đồ chữ ký số, giải pháp này được thực hiện trên cả hai cấp độ của chữ ký số. Ở cấp độ đầu tiên, nhóm tác giả đề xuất một bài toán khó mới, khác với các bài toán khó đã sử dụng trước đây, và quan trọng là bài toán khó này thuộc loại bài toán khó hiện chưa có lời giải (ngoại trừ phương pháp "brute force attack"). Ở cấp độ thứ hai, nhóm tác giả đề xuất phương pháp xây dựng thuật toán chữ ký số mới, với phương pháp này có thể tạo ra không chỉ một mà là một họ các thuật toán chữ ký số mới với mức độ bảo mật cao cho các ứng dụng thực tế.

Từ khóa

Chữ ký số, lược đồ chữ ký số, bài toán logarit rời rạc, bài toán khai căn, bài toán logarit kết hợp khai căn.