A METHOD FOR CONSTRUCTING DIGITAL SIGNATURE SCHEMES BASED ON NEW HARD PROBLEM ON THE ELLIPTIC CURVE

Hong Dung Luu[1,*], *Anh Tuan Do*[1], *Minh Duc Tong*[1], *The Truyen Bui*[1]

Abstract

In this paper, the authors propose a solution to improve the secure of digital signature schemes, this solution is implemented on two levels of digital signature scheme construction. At the first level, the authors propose a new hard problem, this hard problem belongs to the class of hard problems for which there is currently no solution (except by “brute force attack" method). At the second level, the authors propose a method to construct new digital signature algorithms based on this hard problem.

Index terms

Digital signature, digital signature scheme, discrete logarithm problem, elliptic curve discrete logarithm problem, elliptic curve cryptography.

1. Introduction

In [1], [2], the paper proposed a method for constructing digital signature schemes based on a new hard problem on the prime finite field $\mathbf{F}_p$. In this paper, we continue to propose a new form of that problem on elliptic curves and a method for constructing digital signature schemes based on this new hard problem. With this method, it is possible to generate a new family of highly secure digital signature algorithms for practical applications.

2. The new hard problem on the elliptic curve

2.1. The elliptic curve discrete logarithm problem

The discrete logarithm problem on elliptic curves (ECDLP) is described as follows: Suppose G is a point on an elliptic curve $\mathbf{E}$, generating the cyclic group $\langle G\rangle$. Let point $P \in \langle G\rangle$. Find the integer k such that:

$$P = k \times G.$$

[1]Institute of Information and Communication Technology, Le Quy Don Technical University
[*]Corresponding author, email: luuhongdung@gmail.com DOI: 10.56651/lqdtu.jst.v12.n02.751.ict

2.2. The new hard problem on the elliptic curve

From ECDLP we see that if the point G is also kept secret, then the ECDLP will become an unsolvable problem. In the simplest case, the x-coordinate of $G\,(x_G)$ can be chosen as the secret parameter k, then the new hard problem on the elliptic curve is stated in the first form as follows:

Form 1: Let $\mathbf{E}(\mathbf{F}_p)$ be an elliptic curve defined on the finite field $\mathbf{F}_p$ and G be a point on $\mathbf{E}(\mathbf{F}_p)$ generating the cyclic group $\langle G\rangle$. Give a point P in $\langle G\rangle$, find point G that satisfies the following equation:

$$P = x_G \times G.$$

On the other hand, this hard problem can also be stated in the second form as follows:

Form 2: Let $\mathbf{E}(\mathbf{F}_p)$ be an elliptic curve defined on the finite field $\mathbf{F}_p$ and G be a point on $\mathbf{E}(\mathbf{F}_p)$ generating the cyclic group $\langle G\rangle$. Give a point P in $\langle G\rangle$ and an integer k in $\mathbf{F}_p$, find point G that satisfies the following equation:

$$x_G \times P = k \times G.$$

It is easy to see those existing algorithms for the ECDLP cannot be used to solve this problem. At present, there is no other solution to this problem other than the “brute force attack" method.

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, it is also used to generate signature in the Signing algorithm, while the second form of this hard problem is used as the basis for construction the Verification algorithm.

3. Construction digital signature schemes based on the new hard problem on the elliptic curve

In this section, the method of construction digital signature schemes is presented through design a specific signature scheme, including: the Key generation algorithm, the Signing algorithm and the Verification algorithm, these algorithms are constructed as follows:

3.1. The proposed scheme

3.1.1. The key generation algorithm: The set of domain parameters includes:

- p is a prime number specifying the underlying finite field $\mathbf{F}_p$.
- $\mathbf{E}(\mathbf{F}_p)$ is elliptic curve defined on the finite field $\mathbf{F}_p$ by equation:

$$y^2 = x^3 + ax + b \text{ with: } a, b \in \mathbf{F}_p \text{ and satisfied: } 4a^3 + 27b^2 \neq 0 \bmod q$$

The domain parameters here can be generated as specified in ISO/IEC 15946 [3], ANSI X9.62 [4], FIPS 186 – 4 [5] or GOST R34.10 – 2012 [6].

The secret key of the signature entity is a point G of prime order q on the elliptic curve $\mathbf{E}(\mathbf{F}_p)$. The corresponding public key P is:

$$P = (-x_G) \times G. \tag{1}$$

The Key generation algorithm (Algorithm 1.1) is described as follows:

3.1.2. The Signing algorithm: Assuming (R, s, Z) is the signature on the message to be signed M, here: R, Z are points on the elliptic curve $\mathbf{E}(\mathbf{F}_p)$, and s is a value in the range $(1, q)$.

The R component of the signature is calculated according to the following formula:

$$R = k \times G. \tag{2}$$

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

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

$$Z = u \times G. \tag{3}$$

Here, the u is also randomly chosen in the range $(1, q)$.

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

Assuming the condition for (R, s, Z) to be recognized as valid, also means is the message M authenticated for origin and integrity is:

$$\pi(R) \times Z = s \times e \times R + \pi(Z + s \times R) \times P. \tag{4}$$

In (4), $\pi()$ is a function that converts a point on the elliptic curve to an integer. With $\mathbf{E}$ defined on $\mathbf{F}_p$ and Q as a point on $\mathbf{E}$, then $\pi(Q) = x_Q$.

The parameter e is the representative value of the message to be signed M (the hash value of M) and is generated by the hash function $H()$ according to:

$$e = H\left(x_Q, x_R, M\right).$$

In there, x_Q and x_R are the x-coordinates of point Q and point R on $\mathbf{E}(\mathbf{F}_p)$.

From (2) and (3), we have:

$$Z + s \times R = u \times G + s \times k \times G = (u + k \times s) \times G. \tag{5}$$

Set:

$$v = (u + k \times s) \bmod q. \tag{6}$$

Then (5) will become:

$$Z + s \times R = (u + k \times s) \times G = v \times G = Q. \tag{7}$$

From (1), (2), (3), (4) and (7), we have:

$$\pi(R) \times u \times G = s \times e \times k \times G + \pi(v \times G) \times (-x_G) \times G. \tag{8}$$

From (8) deduce:

$$\pi(R) \times u \equiv s \times e \times k + \pi(Q) \times (-x_G) \bmod q. \tag{9}$$

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

$$u = (v - k \times s) \bmod q. \tag{10}$$

Substituting (10) into (9), we get:

$$(v - k \times s) \times \pi(R) \equiv (k \times s \times e - x_G \times \pi(Q)) \bmod q. \tag{11}$$

From (11) deduce:

$$s = (v \times \pi(R) + x_G \times \pi(Q)) \times (k \times (e + \pi(R)))^{-1} \bmod q.$$

Finally, we get:

$$s = (v \times x_R + x_G \times x_Q) \times (k \times (e + x_R))^{-1} \bmod q. \tag{12}$$

From (10) and (12), the component Z is calculated according to:

$$Z = (v - k \times s) \times G.$$

The Signing algorithm (Algorithm 1.2) is described as follows:

Algorithm 1.2:
input: $\mathbf{E}(\mathbf{F}_p), G, P, M.$
output: (R, s, Z)
[1]. **select** $k, v : 1 < k, v < q$
[2]. $R \leftarrow k \times G$
[3]. $Q \leftarrow v \times G$
[4]. $e \leftarrow H\left(x_Q \| x_R \| M\right)$
[5]. $s \leftarrow (v \times x_R + x_G \times x_Q) \times (k \times (e + x_R))^{-1} \bmod q$
[6]. $Z \leftarrow (v - k \times s) \times G$
[7]. **return** (R, s, Z)

Note:

- M is the message to sign which has an arbitrary length ($M \in \{0,1\}^{\infty}$).
- $H()$ is the hash function with $H : \{0,1\}^* \mapsto Z_h, q < h < p$ (eg: SHA-1, SHA-256,... [7]).
- "$\|$" is the operator that concatenates of bit strings.

3.1.3. The Verification algorithm: The Verification algorithm of this scheme is also construction from the assumption:

$$\pi(R) \times Z = s \times e \times R + \pi(Z + s \times R) \times P. \tag{13}$$

Here, $e = H\left(x_Q \left\|x_R\right\| M\right)$ and $Q = v \times G$.

It can be seen that the above assumption is completely equivalent to:

$$R = (\pi(R) \times Z - \pi(Z + s \times R) \times P) \times (s \times e)^{-1}.$$

Therefore, if a point $\bar{R}$ on $\mathbf{E}(\mathbf{F}_p)$ is calculated according to the formula:

$$\bar{R} = (\pi(R) \times Z - \pi(Z + s \times R) \times P) \times (s \times \bar{e})^{-1}$$

with $\bar{e} = H\left(x_{\bar{Q}} \left\|x_R\right\| M\right)$ and $\bar{Q} = (Z + s \times R)$, then we can infer: $\bar{R} = R$.

From here, if set: $a = H\left(x_{\bar{Q}} \left\|x_R\right\| M\right)$ and: $b = H\left(x_{\bar{Q}} \left\|x_{\bar{R}}\right\| M\right)$ then the conditions for a valid signature are: $a = b$.

Algorithm 1.3:

input: $\mathbf{E}(\mathbf{F}_p), P, M, (R, s, Z)$.
output: TRUE/FALSE.

[1]. $\bar{Q} \leftarrow (Z + s \times R)$
[2]. $a \leftarrow H\left(x_{\bar{Q}} \left\|x_R\right\| M\right)$
[3]. $\bar{R} \leftarrow (s \times a)^{-1} \times \left(x_R \times Z - x_{\bar{Q}} \times P\right)$
[4]. $b \leftarrow H\left(x_{\bar{Q}} \left\|x_{\bar{R}}\right\| M\right)$
[5]. if $(a = b)$ then return (TRUE)
else return (FALSE)

(14)

Note:

- $M, (R, s, Z)$ are message and signature to be verified, respectively.
- 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.

3.1.4. The correctness of the proposed signature schema: What needs to be proved here is: if $a = H\left(x_{\bar{Q}} \left\|x_R\right\| M\right)$ and $b = H\left(x_{\bar{Q}} \left\|x_{\bar{R}}\right\| M\right)$ with $\bar{R} = (s \times a)^{-1} \times \left(x_R \times Z - x_{\bar{Q}} \times P\right)$, in there: $\bar{Q} = (Z + s \times R)$ then: $a = b$.

Indeed, if the signature to be verified was not forged, we will have:

$$\begin{aligned}\bar{Q} &= (Z + s \times R) = u \times G + s \times k \times G = (v - k \times s) \times G + k \times s \times G \\ &= v \times G - k \times s \times G - k \times s \times G = v \times G = Q.\end{aligned} \tag{15}$$

From (15) if the message to be verified was also not forged, we get:

$$a = H\left(x_{\bar{Q}} \left\|x_R\right\| M\right) = H\left(x_Q \left\|x_R\right\| M\right) = e. \tag{16}$$

From (13) we have:

$$R = (s + e)^{-1} \times (\pi(R) \times Z - \pi(Z + s \times R) \times P). \tag{17}$$

Substituting (16) into (14), we have:

$$\begin{aligned}\bar{R} &= (s \times a)^{-1} \times (x_R \times Z - \pi(Z + s \times R) \times P) \\ &= (s \times e)^{-1} \times (x_R \times Z - \pi(Z + s \times R) \times P).\end{aligned} \tag{18}$$

From (17) and (18), it can be deduced:

$$\bar{R} = R. \tag{19}$$

Finally, from (19) we have:

$$a = H\left(x_{\bar{Q}} \|x_R\| M\right) = H\left(x_{\bar{Q}} \|x_{\bar{R}}\| M\right) = b.$$

Thus, the correctness of the schema has been proved.

3.2. Some assessments of the secure of the proposed signature scheme

The secure of the proposed signature scheme can be evaluated through its ability to resist some types of attacks such as:

3.2.1. Secret key attack: In proposed scheme, a secret key attack can be made on the Key generation algorithm (Algorithm 1.1) and the steps [2], [3], [5], and [6] of the Signing algorithm (Algorithm 1.2). In step [2] and [3] of the Signing algorithm, since k or v is also a secret parameter, finding G from step [2] and [3] of the Signing algorithm is as difficult as finding G from the Key generation algorithm, as it is known this is a type of hard problem that currently there is no solution [8]–[16]. In step [5] and [6] of the Signature algorithm, in addition to x_G being the secret parameter to be found, k and v are also secret parameters, then finding x_G from step [5] and [6] of the Signing algorithms is also impossible.

3.2.2. Signature forgery attack: From the Verification algorithms (Algorithm 1.3) of the proposed scheme, a set of 3 components (R, s, Z) will be recognized as a valid signature with the message to be verified M if the condition is satisfied:

$$\pi(R) \times Z = s \times e \times R + \pi(Z + s \times R) \times P, \text{ here: } e = H\left(x_Q \|x_R\| M\right).$$

It can be seen that, even if 2 of the 3 components (R, s, Z) of the signature are pre-selected, calculating the remaining component that satisfies the above mentioned condition is essentially the second form of the hard problem mentioned in section 2.2. As we know, this is a type of hard problem for which currently in mathematics there is no other solution than the "brute force attack" method [8]–[16].

3.3. Performance of the proposed signature schemes

Performance of the signature scheme constructed according to the proposed method is basically evaluated by comparing the computational cost of this scheme with the computational cost of the ECDSA digital signature scheme in the US DSS standard [5] and GOST R34.10-2012 of the Russian Federation [6].

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

- N_{mp} is the number of multiplications on $\mathbf{E}(\mathbf{F}_p)$.
- $\mathsf{N}_{\mathsf{mul}}$ is the number of modulo multiplications.

- N_{inv} is the number of modulo division (inversion).
- N_h is the number of hash operations.

Note: The Key generation algorithm only needs to be done once for every schema. Therefore, the computational cost for the Key generation algorithm can be ignored when comparing the costs of the schemas.

The cost for the Signing algorithms and the Verification algorithms of the ECDSA and GOST R34.10-2012 compared with the proposed scheme is shown in Table 1 and Table 2 as follows:

Table 1. The computational cost of the Signing algorithms

	N_{mp}	N_{mul}	N_{inv}	N_h
ECDSA	1	2	1	1
GOST R34.10-2012	1	2	0	1
The proposed scheme	3	5	1	1

Table 2. The computational cost of the Verification algorithms

	N_{mp}	N_{mul}	N_{inv}	N_h
ECDSA	2	2	1	1
GOST R34.10-2012	2	2	1	1
The proposed scheme	3	2	1	2

Comment:
Comparing the cost of the proposed schemes with the ECDSA and GOST R34.10-2012, as shown in Table 1 and Table 2, shows that the performance of the proposed schemes is lower than that of ECDSA and GOST R34.10-2012. It can be seen that this is the cost of improving the security of the schemes constructed by the proposed method.

4. Conclusion

In this paper, the authors propose a solution to improve the security of the digital signature scheme based on a new hard problem on the elliptic curve, which is developed from the elliptic curve discrete logarithm problem. 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 the improvement of the security of the digital signature scheme according to this new solution. From the proposed new solution, it is possible to generate a new family of highly secure digital signature schemes suitable for different choices in practical applications.

References

[1] B. T. Truyen, N. D. Thuy, L. H. Dung, and D. K. Huan, "A new method for constructing digital signature schemes based on new hard problem," *Journal of Science and Technique - ISSN 1859-0209*, vol. 11, no. 2, pp. 23–33, Dec 2022. doi: 10.56651/lqdtu.jst.v11.n02.535.ict

[2] N. K. Tuan, N. V. Thai, and L. H. Dung, "A new construction method of digital signature scheme based on the discrete logarithm combining find root problem on the finite field," *Journal of Military Science and Technology*, pp. 164–170, Dec 2022. doi: 10.54939/1859-1043.j.mst.FEE.2022.164-170

[3] *ISO/IEC 15946: Information technology – Security techniques – Cryptographic Techniques Based on Elliptic Curves*. ISO/IEC, 1999.

[4] *ANSI X9.62. Public Key Cryptography for the Financial Services Industry: Elliptic Cuve Digital Signature Algorithm (ECDSA)*. ANSI, 1999.

[5] *NIST FIPS PUB 186-4. Digital Signature Standard, National Institute of Standards and Technology, U.S. Department of Commerce*. National Institute of Standards and Technology, 2013.

[6] *GOST R34.10 – 2012, Russian Federation Standard Information Technology. Government Committee of the Russia for Standards, 2012 (in Russian)*, 2012.

[7] "Federal information processing standards publication 180-3 (FIPS PUB 180-3), secure hash standard (SHS)," Tech. Rep., 2008.

[8] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2018.

[9] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC, Aug 2007.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. New York: Springer, 2014.

[11] L. C. Washington, *Elliptic Curves - Number Theory and Cryptography*. Chapman and Hall/CRC, Apr 2008.

[12] D. R. Stinson, *Cryptography*. Chapman and Hall/CRC, Nov 2005.

[13] J. Talbot and D. Welsh, *Complexity and Cryptography*. Cambridge University Press, Jan 2006.

[14] J. H. Silverman, "Elliptic curves and cryptography," *Proc. Sympos. Appl. Math*, pp. 91–112, 2005. doi: 10.1090/psapm/062/2211873

[15] I. Shparlinski, Ed., *Cryptographic Applications of Analytic Number Theory*. Birkhäuser Basel, 2003.

[16] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, Jul 1999.

Manuscript received 25-09-2023; Accepted 21-12-2023.

■

Hong Dung Luu graduated from University in Radio Electronics in 1989, Master in Electronics and Communication Engineering in 2000, Doctorate in Electronic Engineering in 2013 from Le Quy Don Technical University. Currently, he is a lecturer at the Institute of Information and Communication Technology - Le Quy Don Technical University. Research field: cryptography and information security. E-mail: luuhongdung@gmail.com

Anh Tuan Do received the B.S. degree in mathematics from VNU Hanoi University of Science in 2003, and the Ph.D. degree in mathematics from Joseph Fourier University, Grénoble, France, in 2014. He is currently a lecturer in Mathematics at the Institute of Information and Communication Technology - Le Quy Don Technical University. His research interests include number theory and their applications in cryptography. E-mail: doanhtuanktqs@gmail.com

Minh Duc Tong graduated from Le Quy Don Technical University in 2000. He received a doctor's degree from University of Electrical Engineering, Russia, in 2007. He is currently a lecturer at the Institute of Information and Communication Technology - Le Quy Don Technical University. His research interests include image processing, object identification, information security safety. E-mail: ducmta@gmail.com

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

PHƯƠNG PHÁP XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ DỰA TRÊN BÀI TOÁN KHÓ MỚI TRÊN ĐƯỜNG CONG ELLIPTIC

Lưu Hồng Dũng, *Đỗ Anh Tuấn*, *Tống Minh Đức*, *Bùi Thế Truyền*

Tóm tắt

Trong bài báo này, nhóm tác giả đề xuất giải pháp nâng cao tính an toàn của lược đồ chữ ký số, giải pháp này được triển khai trên hai cấp độ xây dựng lược đồ chữ ký số. Ở cấp độ thứ nhất, nhóm tác giả đề xuất một dạng bài toán khó mới, bài toán khó này thuộc lớp bài toán khó mà hiện nay chưa có cách giải (ngoại trừ phương pháp "tấn công vét cạn"). Ở cấp độ thứ hai, nhóm tác giả đề xuất phương pháp xây dựng thuật toán chữ ký số mới dựa trên bài toán khó này.

Từ khóa

Chữ ký số, lược đồ chữ ký số, bài toán logarithm rời rạc, bài toán logarithm rời rạc trên đường cong elliptic, mật mã trên đường cong elliptic.