A Digital Signature Scheme based on Elliptic Curve Cryptosystem

Yan-Tsang Wu [#1], Ming-Chang Wu [#2], Jyh-Horng Wen*[3]

[#1, 2] *Department of Network System, Toko University*

No.51, Sec. 2, Syuefu Rd., Puzih City, Chiayi County 61363, Taiwan

[1]E-mail: buddyswu @ hotmail.com

[2]E-mail: mcw.mcw @ msa.hinet.net

[*3]*Department of Electrical Engineering, Tunghai University*

No. 181, Taichung Harbor Rd., Section 3, Taichung 40704, Taiwan

[*3]E-mail:jhwen @ thu.edu.tw

[*3]Corresponding author: Jyh-Horng Wen

***Abstract*— People develop science very fast today and the network communication is grown very rapidly. The signature of digitization has extended already to apply on the network communication and the digital signature designing scheme of all kinds are proposed for this thing. Chung et al. proposed an ID-based digital signature scheme on elliptic curve cryptosystem in 2007. In 2008, Yang et al. proposed an article of weakness of Chung et al.'s scheme. Yang et al. use the linear Diophantine equation successfully to avoid touching the elliptic curve discrete logarithm problem (ECDLP) in Chung et al.'s scheme. As the result, the Chung's scheme becomes insecure. Hence, we propose a new scheme to delete the weakness and our scheme is designed by using elliptic curve cryptosystem (ECC). We use the elliptic curve discrete logarithm problem for the security of system in order to prevent the outside attack such that we can set up a secure digital signature system.**

***Keywords*— Elliptic curve, Information security, Digital signature, Hash function.**

1. INTRODUCTION

With popularization of the network communication, the signature of digitization has been used on the network communication. It is represented the signature scheme of digitization with Elgamal signature [1], Schnorr signature [2] and DSA (Digital Signature Algorithm) signature [3-5]. In 1985, Elgamal proposed a public key cryptosystem and the signature scheme is based on discrete logarithms [1]. He operates the signature scheme with exponential function. After, Schnorr proposed an efficient identification and signatures for smart cards in 1990 [2]. He also operates his scheme with exponential function. In 1991, National Institute of Standard and Technology (NIST) announced Digital Signature Standard (DSS) [4] in the digit signature of American to adopt with Digital Signature Algorithm (DSA) [5]. As the result, the length of signature text of Elgamal is reduced by DSA. In other words, they all use the exponential functional operation in these three signature scheme [6, 7]. Later, the elliptic curve cryptosystem (ECC) [8] is applied to digital signature scheme. Under the same secure condition, the digital signature scheme of elliptic curve cryptosystem is fewer bits than that of the exponential functional operation [9]. This is an advantage of the digital signature scheme of elliptic curve cryptosystem. Hence, we also use the elliptic curve cryptosystem to construct a digital signature scheme in this text.

In 1987, Koblitz [8] first proposed an elliptic curve cryptosystem and the cryptosystem is based on elliptic curve operation. If we take two points over the elliptic curve to add operation, we can produce third point in which it exists over the elliptic curve. A designer can select a point over the elliptic curve as you wish. The point is called

as the base point [10]. When anyone knows the third point over the elliptic curve, he/she wishes to get its basic point in which is very difficult. That is said to be elliptic curve discrete logarithm problem (ECDLP) [11-13].

In 2007, Chung et al. [14] use elliptic curve to construct a digital signature scheme and the scheme is designed by elliptic curve discrete logarithm problem for protection security of system. In 2008, Yang et al. [15] proposed a thesis in which they pointed out a weakness of Chung et al. scheme. An attacker can obtain the secret code of signer, but he/she needn't involve the elliptic curve discrete logarithm problem that it is described behind chapter. Thus, Chung et al.'s scheme is broken by attacker. As the result, the scheme becomes insecure.

We propose a new scheme to delete this weakness in this text and we use the elliptic curve discrete logarithm problem for protection security of system too. We wish that the digital signature scheme can pass through anyone attack and it becomes an effective secure digital signature scheme. In the rest of the paper, the relevant research is given in the following section. Our scheme is described in Section 3. Finally, the conclusion is given in Section 4.

2. RELEVANT RESEARCH

The relevant research is included the brief introduction of linear Diophantine equation, Chung et al.'s digital signature scheme and Yang et al. proposed the weakness of Chung et al.'s digital signature scheme. They are illustrated as follows:

2.1. Brief Introduction of Linear Diophantine Equation

A linear Diophantine equation [16, 17] is shown as $lx + my = n$ where l, m and n are integer. If the l and m have the largest common divisor a in which it is shown as $a = GCD(l, m)$. The linear Diophantine equation have a solution in which it is shown as $x' = \alpha n / a$ and $y' = \beta n / a$, where α and β need to be conformed to a's condition in which a is shown as $a = \alpha l + \beta m$. Then, we can obtain all solution (x, y) in the linear Diophantine equation and the solution is shown as $x = x' + (m/a)w$ and $y = y' - (l/a)w$, where w is an integer.

2.2. Chung Et Al.'S Digital Signature Scheme

Chung et al.'s digital signature scheme [14] is described as an elliptic curve is assumed as $y^2 = x^3 + ax + b \pmod{p}$, where a and b need to be satisfied the condition of the discriminant $D = 4a^3 + 27b^2 \neq 0 \pmod{p}$. Then, they take two points B_1 and B_2 over elliptic curve to apply in their scheme. After, we describe the signature and verification methods of Chung et al.'s digital signature scheme.

2.2.1. Signature phase

Chung et al.'s digital signature method is shown as the following steps.

Step 1: the signer chooses arbitrarily two numbers d_1 and d_2 and then he/she produces a public key Y. The Y is shown as $Y = d_1B_1 + d_2B_2$.

Step 2: the signer chooses arbitrarily two numbers r_1 and r_2 and then he/she computes a number Q. The Q is shown as $Q = r_1B_1 + r_2B_2$.

Step 3: the signer computes a number e and e of the formula is shown as $e = h(m, Q) \in [1, 2^t]$, where h is hash function, t is a integer and m is plain text.

Step 4: the signer computes two numbers s_1 and s_2. The formula is shown as $s_1 = r_1 + d_1e \mod u$ and $s_2 = r_2 + d_2e \mod u$ separately, where u is a big prime number.

Step 5: the signer sends the (s_1, s_2, e) to verifier.

2.2.2. Verification Phase

When verifier gets the (s_1, s_2, e), he/she shall verify by the following steps.

Step 1: verifier computes $Z = s_1B_1 + s_2B_2 - eY$.

Step 2: verifier gets the result Z after. If the Z equals Q, the e can be shown as $e = h(m, Z) = h(m, Q)$. Its significance is indicated the m that is sent by signer.

2.3. Yang Et Al. Proposed the Weakness of Chung Et Al.'S Digital Signature Scheme.

Yang et al. [15] proposed an attacker which does not contact the elliptic curve discrete logarithm problem in Chung et al.'s digital

signature scheme. The attacker also can get the secret code of signer. This is a weakness of Chung et al.'s scheme. Hence, their scheme becomes insecure. We give an example to explain the weakness.

If an attacker gives $s_1 = 17$, $s_2 = 19$, $e = 13$ and $u = 23$ in the $s_1 = r_1 + d_1 e \bmod u$ and then the attacker can get $s_1 = 13d_1 + r_1 = 17$. In the Diophantine equation $lx + my = n$, it corresponds to the $l = 13$, $m = 1$, $x = d_1$, $y = r_1$ and $n = 17$. The attacker can obtain the secret code d_1 and d_2 from the following steps in the Diophantine equation.

Step 1: the attacker computes $a = GCD(l, m) = 1$.

Step 2: the attacker uses Euclidean algorithm and then the attacker can obtain $\alpha = 1$ and $\beta = -12$ from $a = \alpha l + \beta m = 13\alpha + \beta = 1$ [18].

Step 3: the attacker computes $x' = \alpha n / a = 17$ and $y' = \beta n / a = -204$.

Step 4: the attacker can acquire $x = x' + (m/a)w = 17 + w = d_1$ and $y = y' + (l/a)w = -204 - 13w = r_1$, where w is the integer.

Step 5: the attacker gets $s_1 = r_1 + 13d_1 = 3 - 13w + 13(17 + w) = 17 \pmod{23}$.

With the same method, the attacker can get $d_2 = 19 + w' \pmod{23}$ and $r_2 = 2 - 19w' \pmod{23}$, where w' is a integer. Thus, the attacker can use the variables w and w' with a try the mistake method under the number u, and then he/she can obtain the d_1, r_1, d_2, and r_2 in Chung et al.'s scheme. Subsequently, the attacker can acquire Q and Y from equations $Q = r_1 B_1 + r_2 B_2$ and $Y = d_1 B_1 + d_2 B_2$. In other words, the attacker can get the e from $e = h(m, Q)$. In the attack, we do not see that the attacker involves the elliptic curve discrete logarithm problem in order to get d_1, r_1, d_2 and r_2. So, Chung et al.'s scheme becomes insecure.

3. OUR SCHEME

Because Yang et al. proposed the weakness of Chung et al.'s scheme, we propose a new digital signature scheme to delete this weakness. There are the signers A and the verifier B in the scheme. After A signs plain text m, the signer sends it to B. When B receives with the signed plain text m, B needs verify the plain text m whether the m is signed by A. Next, we explain the methods of the signature and verification in our scheme.

3.1. Signature Phase

The method of signature in our scheme is shown as the following steps.

Step 1: A selects a secret key y and a public key k in which y and k need to be satisfied the condition of $1 < y < p$ and $0 < k < q$, where p and q are different large prime number.

Step 2: we choose an elliptic curve $y^2 = x^3 + ax + b \pmod{p}$ for application in our scheme [19], where a and b are satisfied the condition of the discriminant $D = 4a^3 + 27b^2 \neq 0 \pmod{p}$ [20]. Then, we select randomly a point c over elliptic curve as base point.

Step 3: we make an elliptic curve addition operation [21] with y and c and we get a number t. The operation formula is shown as $yc = t \bmod p$ and then the t is made public.

Step 4: signer A operates hash function h to t and m, and we obtain a number e. The operation formula is shown as $e = h(t, m)$.

Step 5: A computes a number s with y and k^{-1}. The operation formula is shown as $s = yk^{-1} \bmod p$, where k^{-1} is k inverse element that is $k^{-1}k = 1 \bmod q$ in which q is a large prime number.

Step 6: A sends (e, s) to B.

3.2. Verification Phase

After B receives A signature (e, s), B needs to make work of verification. The work is in order to verify that the plain text m is signed by signer A. The verification method is shown as follows:

Step 1: B first computes a number t'. The operation formula is shown as $t' = ksc \bmod p$.

Step 2: when A sent (e, s) to B, B can compute $t' = ksc = kk^{-1}yc = yc = t \bmod p$, where both k and c are public, (i.e. $t' = t$). In other words, B acquires $e = h(t', m) = h(t, m)$. The significant of $e = h(t, m)$ is indicated that the plain text m is signed by signer A.

An attacker only can get a pseudo number s' because he/she is not a verifier. The attacker will not acquire $t' = t$ from the $t' = ksc \bmod p$. In other words, the attacker is unable to get true e which is sent by A. Hence, the design of our scheme is proved to be secure from the discussion.

4. CONCLUSIONS

The text first explains the course of the signature and verification of Chung et al.'s digital signature scheme. Then, we also illustrate that Yang et al. proposed the weakness of Chung et al.'s digital signature scheme. Because the weakness is possibly to be happened in Chung et al.'s scheme, it will become insecure. Hence, we propose a new digital signature scheme with elliptic curve cryptosystem. We illustrate the method of the signature and verification in our scheme. We also discuss the reason of security in our scheme that an attacker is not successful to attack the scheme because it is based on the protection of the elliptic curve discrete logarithm problem. Hence, we propose a digital signature scheme of security and practicability.

REFERENCES

[1] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, 4, July 1985.

[2] C. P. Schnorr, *Efficient Identification and Signatures for Smart Cards*, Lecture Notes in Computer Science 435, advances in cryptology: crypto'89, Berlin: Springer-Verlag, 1990.

[3] S. M. Yen, "Improved digital signatures algorithm, *IEEE Transactions on Computers*," vol. 44, 5, pp. 729-730, May 1995.

[4] *Proposed Federal Information Processing Standard for Digital Signatures Standard (DSS)*, Federal Register, vol. 56, 169, pp. 42980-42982, Aug. 30, 1991.

[5] *The Digital Signatures Standard Proposed by NIST*, Communication ACM, vol. 35, 7, pp. 36-40, July 1992.

[6] H. Liang, *Hanging on the Small Stream Loose*, Modern Cryptography and Application, Loose Hillock Computer Books, 1995.

[7] S. Y. Wu, *Information and Network Safe Practice*, Flag Marks Books, 2006.

[8] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of ACM*, vol. 21, 2, pp. 120-126, 1978.

[10] J. H. Wen, M. C. Wu, and T. S. Chen, "A Novel Elliptic Curve Dynamic Access Control System," *IEICE Transactions on Communications*, vol. E90-B, 8, pp. 1979-1987, 2007.

[11] S. A. Vanstone, "Elliptic curve cryptosystem - the answer to strong, fast public-key cryptography for securing constrained environments," Information Security Tech. Rep. vol. 12, 2, 78-87, 1997.

[12] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, 5, pp. 1639-1646, 1993.

[13] N. Koblitz, A. J. Menezes, and S. A. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 19, pp. 173-193, 2000.

[14] Y. F. Chung, K. H. Huang, F. Lai, and T. S. Chen, "ID-based Digital Signature Scheme on Elliptic Curve Cryptosystem," *Computer Standards and Interfaces*, vol. 29, pp. 601-604, 2007.

[15] J. H. Yang and C. C. Chang, "Cryptanalysis of ID-based digital signature scheme on elliptic curve cryptosystem," isda, *2008 Eighth International Conference on Intelligent Systems Design and Applications*, 2008, paper 3, p. 3.

[16] L. E. Dickson, *History of the Theory of Numbers Volume II: Diophantine Analysis*, Bronx, New York: Chelsea Publishing, 1992, vol. 2.

[17] L. J. Mordell, *Diophantine Equations*, New York: Academic Press, 1969.

[18] J. Gathen and J. Gerhard, *Modern Computer Algebra*, 2nd ed., Cambridge University Press, 2003.

[19] A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Boston: Kluwer Academic Publishers, 1997.

[20] A. W. Knapp, *Elliptic Curve*, Princeton University Prece, 1992.

[21] J. H. Silverman, *the Arithmetic of Elliptic Curves*, New York: Springer, 1986.