A General Threshold Signature Scheme Based on Elliptic Curve

Yulian Shang, Xiujuan Wang, Yujuan Li, Yufei Zhang
College of Information Engineering, Taishan Medical University, Taian 271016, China
E-mail: shangyulian@163.com

Abstract**—**Based on Elliptic Curve cryptosystem, a threshold signature scheme characterized by (*k*, *l*) joint verification for (*t*, *n*) signature is put forward. After being signed by a signer company employing (*t, n*) threshold signature scheme, the information *m* is transmitted to a particular verifier company, and then the signature is verified through the cooperation of *k* ones from the verifier company with *l* members, so as to realize a directional transmission between different companies. Finally, the application examples of the company encryption communication system, the generating polynomial of company private key and public key were given. The security of this scheme is based on Shamir threshold scheme and Elliptic Curve system, and due to the advantages of Elliptic Curve, the scheme enjoys wider application in practice.

Keywords-Elliptic Curve; Threshold signature; Company-oriented; Interpolation polynomial

I. Introduction

The research is based on the following fact in digital contracts.

A contract between two companies will be signed and verified. This contract can not be exposed to any outsider, otherwise it will have been altered and forged risk. In other words, the verifier company group user must be determined.

In view of the above fact, it's stipulated that there are n members in a signer company, and only through the cooperation of at least t members can some information be effectively signed; On the other hand, only through the cooperation of at least k ones from a verifier company with l members can the signature be verified. Thus, the digital signature and verification system [1-6] before can not meet practical needs, thinking that in the signature and verification stage anyone who receives the document can practice verification. Therefore, there shall be a general scheme [7, 8] in which the signer company and verifier company can be regulated under a pre-stipulated security environment.

To solve the problem above, based on Elliptic Curve cryptosystem, a threshold signature scheme characterized by (*k*, *l*) joint verification for (*t*, *n*) signature is put forward. The security of the scheme is based on the intractability of discrete logarithm calculation on Elliptic Curve[9] and Shamir threshold scheme[10], and enjoys the characteristics of reduced communication load and lowered calculation complexity, etc.

II. DESCRIPTION OF THE SCHEME

There are three parties in the whole system, i.e., shared distribution center (SDC), signer company and verifier company. The scheme includes three stages, i.e., generation of parameters, generation and verification of private signatures, and generation and verification of company signatures.

A. Generation of Parameters

In this stage, SDC define the parameters of system member and he firstly select the Elliptic Curve $E: y^2 = x^3 + ax + b(\bmod p)$ and big prime numbers *P* and *n*, where, $a,b\in Z_p, 4a^3 + 27b^2 \neq 0(\bmod p)$, $GF(p) = \{0,\cdots, p-1\}$, and *n* is the *order* of primitive root. The value of $\#E(GF(p))$ is ranged between $p+1\pm 2\sqrt{p}$. *G* is base point, and represents a primitive root of the Elliptic Curve, where, $G\in E(GF(p))$ and *order* is *n*. p,n,G are used and made public by the company. Next, SDC accepts the registration of a group of signer or verifier, of whom parameter properties are marked by subscript *s* or *v*. $G_s = \{u_{s1}, u_{s2}, \cdots, u_{sn}\}$ and $G_v = \{u_{v1}, u_{v2}, \cdots, u_{vl}\}$ are respectively the companies combined by *n* singer and *l* verifier. Finally, SDC randomly select interpolation polynomials of the signer company *G*

$$f_s(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0 \bmod n$$

$$f_v(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_1 x + c_0 \bmod n$$

Where, $a_i, c_j \in [1, n-1], 1 \le i \le t-1, 1 \le j \le k-1$ .The private key of the signer company is defined as $f_s(0) = a_0$, with which the public key associated is $Y(s) = f_s(0)G \bmod p$. $x_{si} \in [1, n-1]$ are the randomly-selected integral numbers for every member of the signer company of SDC, whose private shadow $f_s(x_{si}), i = 1,2,\cdots,n$ are calculated and the public key associated with are determined by $y_{si} = f_s(x_{si})G \bmod p, i = 1,2,\cdots,n$. Similarly, the private and public key of the verifier, the private and public key of the verifier group can also be got. On the other hand, in order to generate group signature, it is required for SDC to select a secret polynomials for the signer company:

$$f_b(x) = b_{t-1}x^{t-1} + b_{t-2}x^{t-2} + \cdots + b_1 x + b_0 \bmod n$$

Where, $f_b(x_{si})$ are the session keys of the signer member, with which the public values associated are $y_{bi} = f_b(x_{si})G \bmod p$ .The company value $y_{si} = Y(b) = f_b(0)G \bmod p$ is made public. For safety purposes, SDC select a one-way hash function *h* ( ) and make it public. To sum up, all the parameters of the system are shown as follows:

1. Public information in SDC: $p, n, G, h(\,)$
2. Secret information in SDC: $f_s(x), f_v(x), f_b(x)$
3. Public information of members: x_{si}（or x_{vj}），y_{si}（or y_{vj}），y_{bi}
4. Secret information of members: $f_s(x_{xi}), f_v(x_{vi}), f_b(x_{si})$
5. Public information of the companies: Y_s(or Y_v)，Y_b
6. Secret information of the companies: $f_s(0)$, $f_v(0)$

B. Generation and Verification of Private Signatures

According to the security strategy, any *t* members are allowed to sign a piece of information on behalf of the company in this scheme, and the members can simultaneously and independently sign the information. Without loss of generality, we express the *t* members for signing as u_{s1}， u_{s2}， …， and u_{st}. Every member u_{si}， $1 \le i \le t$, carries out the following calculation with its own private key $f_s(x_{si})$ and the public key of the verifier company Y_v.

$$r_{si} = (Y_v) \cdot f_s(x_{si}) \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod P \qquad (1)$$

The result $\{r_{si}\}$ is transmitted to the members participating in signing through security channel, and every member can calculate *r* as follows:

$$r = \prod_{i=1}^{t} r_{si} \bmod P \qquad (2)$$

Then, every member u_{si} signs the information *m* using his private key $f_s(x_{si})$ and the session key $f_b(x_{si})$ through Elliptic Curve signature scheme, i.e., calculates his private signature with the following formula:

$$s_i = h(m) f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{si}}{x_{si} - x_{sj}} - r f_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod n \qquad (3)$$

To verify the validity of private signature s_i, one member is randomly selected as the secretary to be responsible for the verification of private signatures and calculation of company signatures. Following formula is employed to verify private signatures by the secretary:

$$h(m) y_{si} \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \overset{?}{=} s_i G + r y_{bi} \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod p \qquad (4)$$

If the equation is right, the private signature of the information is legitimate.

It's testified as follows:

$$h(m) y_{si} \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} = h(m) \cdot f_s(x_{si}) \cdot G \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \qquad (5)$$

It's known from (3) that:

$$h(m) f_s(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{si}}{x_{si} - x_{sj}} = s_i + r f_b(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \text{ ;}$$

Substituted to (5):

$$h(m) \cdot y_{si} \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{si}}{x_{si} - x_{sj}} = s_i G + r f_b(x_{si}) \cdot G \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}}$$

$$= s_i \cdot G + r \cdot y_{bi} \cdot \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod p$$

End.

C. Generation and Verification of Company Signatures

After *t* private signatures are verified, the secretary calculates the company signatures.

$$s = \sum_{i=1}^{t} s_i \bmod q \qquad (6)$$

The company signatures of information *m* are transmitted to the verifier company G_v, and any *k* ones of the *l* members in company G_v can cooperate to verify the validity of the signatures. Every member u_{vi}， $1 \le i \le k$, carries out the following calculation with its own private key $f_v(x_{vi})$ and the public key of the signer company Y_s.

$$r_{vi} = f_v(x_{vi}) \cdot (Y_s) \cdot \prod_{j=1, j\neq i}^{k} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod P \qquad (7)$$

Similarly, a secretary is randomly selected in the verifier company to calculate:

$$r = \prod_{i=1}^{k} r_{vi} \bmod P \qquad (8)$$

Then, the company signatures can be verified as follows:

$$h(m) \cdot Y_s \overset{?}{=} s \cdot G + r \cdot Y_b \bmod P \qquad (9)$$

Theorem 1.1 if (9) is true, information *m* is verified.

It's testified as follows:

Substituted (2), it's known that：

$$r = \sum_{i=1}^{t} f_x(x_{si}) \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod P$$

$$= f_s(0) \cdot f_v(0) \cdot G \bmod P \qquad (10)$$

Multiplied by both sides for $i = 1, 2, \cdots, t$, it's known from (4) that:

$$h(m) \cdot \sum_{i=1}^{t} y_{si} \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} = \sum_{i=1}^{t} s_i \cdot G + r \cdot \sum_{j=1, j\approx i}^{t} y_{bi} \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod p \qquad (11)$$

From Lagrange interpolation polynomials, it's can determine a *t*-1 degree polynomial utterly

$$f(x) = \sum_{i=1}^{t} y_i \cdot \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j}$$

The left of (11) can rewrite by:

$$h(m) \cdot \sum_{i=1}^{t} y_{si} \prod_{j=1, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \cdot G \bmod p$$

$$= h(m) \cdot f_s(0) \cdot G \bmod p = h(m) \cdot (Y_s) \bmod p \qquad (12)$$

For the member of verifier company u_{vi} can calculate r_{vi} from (6), multiplied by both sides for $i = 1,2,\cdots,t$, r' is known from (8) that:

$$r' = \sum_{i=1}^{k} f_v(x_{si}) \prod_{j=1,\, j\neq n}^{k} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \cdot (Y_s) \bmod P$$
$$= f_v(0) \cdot f_s(0) \cdot G \bmod P \qquad (13)$$

The value of r' is equal to r from (2). The company signature can be calculated from (5). On the other hand, the right of (11) can rewrite by:

$$\sum_{i=1}^{t} s_i \cdot G + r \cdot \sum_{j=1,\, j\approx i}^{t} y_{bi} \prod_{j=1,\, j\neq i}^{t} \frac{0 - x_{sj}}{x_{si} - x_{sj}} \bmod p$$
$$= s \cdot G + r \cdot f_b(0) \cdot G \bmod P$$
$$= s \cdot G + r \cdot y_b \bmod P \qquad (14)$$

End..

III. Application of the Scheme

Here we only give the application examples of the company encryption communication system, the generating polynomial of company private key and public key. For the example of the threshold signature scheme characterized by (*k*, *l*) joint verification for (*t*, *n*) signature, it is also very easy to be given; and we omit it.

Suppose that company *S* and company *V* have three members $S = \{s_1, s_2, s_3\}$, $V = \{v_1, v_2, v_3\}$, respectively; *S* is the encryption of plaintext P_m ,the sender of cipher text C_m;*V* is the receiver and decryption of C_m ; $f_s(x_{s1}) = 2$, $f_s(x_{s2}) = 3$, $f_s(x_{s3}) = 5$ are respectively the private key of s_1, s_2, s_3 and $f_v(x_{v1}) = 11$, $f_v(x_{v2}) = 13$, $f_v(x_{v3}) = 17$ of v_1, v_2, v_3; $f_s(0)$ is the private key of company S , and Y_s is the public key of company *S*. $E_{23}(1,1) : y^2 = x^3 + x + 1 \bmod 23$ is the elliptic curve that be common selected by company *S* and *V* . $a = 2, b = 7$ are respectively the primitive roots selected by company *S* and *V*, and p=11 is the mode selected by company *S*. give modular arithmetic to $E_{23}(1,1)$,we get the point of $E_{23}(1,1)$， then：

$$y^2 = x^3 + x + 1 \bmod 23$$

Let $x = 0$, it’s known that:

$$y^2 = 1 \bmod 23$$
$$y = \begin{cases} 1 \bmod 23 = 1 \bmod 23 \\ -1 \bmod 23 = 22 \bmod 23 \end{cases}$$

Then there are two points： $(0,1), (0,22)$; and so on, the points met with $E_{23}(1,1)$ are $(0,1), (0,22)$, $(1,7), (1,16)$, $(3,10)$, $(3,13), (4,0), (5,4), (5,19), (6,4)$, $(6,19), (7,11), (7,12)$, $(9,7)$, $(9,16), (11,3), (11.20)$, $(17,3), (17,20), (18,3), (18,20)$, $(19,5)$, $(19,18)$, the Sequence of who are $n = 7, (n+1) =$ $(27+1)$ $= 28G = O$, O is the infinity point of Elliptic Curve $E_{23}(1,1)$.

The company *S* and *V* select the base point $G = (5,4)$ and plaintext $P_m = (9,7) \in E_{23}(1,1)$, where, the true plaintext of P_m has been compressed to a point of $E_m(a,b)$ using by technology of data compression.

The private key $f_s(0)$ and public key Y_s of company *S* are respectively：

$$f_s(0) = 9$$
$$Y_s = f_s(0)G = 72G = 56G + 16G = 16G = (11,3)$$

The private key $f_v(0)$ and public key Y_v of company *V* are respectively：

$$f_v(0) = 10$$
$$Y_v = f_v(0)G = 24G = (18,3)$$

$\{s_1, s_2, s_3\}$ decrypt P_m into C_m and send C_m to company *V*

1. $\{s_1, s_2, s_3\}$ take the positive integer $k = 3$ ， base point $G = (5,4)$, plaintext $P_m = (9,7)$, the public key $Y_v = 24G = (18,3)$ of $\{v_1, v_2, v_3\}$ and give：

$$C_m = \{kG, P_m + kY_v\} = \{3G, 14G + 3\times 24G\}$$
$$= \{3\times 8G, 14G + 72G\} = \{24G, 86G\}$$
$$= \{24G, 2G\} = \{(18,3), (0,22)\}$$

2. $\{s_1, s_2, s_3\}$ send $C_m = \{(18,3), (0,22)\}$ to $\{v_1, v_2, v_3\}$

$\{v_1, v_2, v_3\}$ receive C_m, and decrypt C_m into P_m

$\{v_1, v_2, v_3\}$ take the second term $C_{m,2} = P_m + kY_v$ of C_m, take the product of the first term $C_{m,1} = kG$ of C_m and $f_v(0)$, and give：

$$C_{m,2} - C_{m,1} = P_m + kY_v - f_v(0)(kG)$$
$$= 2G - 10(24G) = 2G - 240G = 2G - 16G$$
$$= 2G + (-16G) = 2G + 12G$$
$$= 14G = (9,7) = P_m$$

Acknowledgment

This work was financially supported in part by Institutes of Higher Education Science and Technique Foundation of Shandong Province (J12LN69), Scientific Research Tasks of Tainshan Medical University General Program (2010ZR100). The authors thank the College of Information and Engineering Taishan Medical University colleagues for manuscript comments. The authors are grateful to the anonymous referees for their valuable comments and suggestions.

References

[1] Harn L.: IEEE Proceedings of Computers andDigital Technique Vol. 141 (1994), p.307-313.

[2] Bin Wang and Jianhua Li: Chinese Journal of Computers Vol. 26 (2003), p. 1581-1583.

[3] R. Tso, C. Gu and T. Okamoto: Cryptology and Network Security 2007(CANS 2007), LNCS 4857. Berlin: Springer-Verlag, 2007, p. 47-59.

[4] Y. Ming and Y. Wang: in Proceedings of the 2009 Fifth International Conference on Information Assurance and Security. Washington: IEEE Computer Society, 2009, p. 87-90.

[5] B. Kang, J. Park, and S. Hahn: Topics in Cryptology - CT-RSA 2004, LNCS 2964. Berlin: Springer-Verlag, 2004, p. 99-111.

[6] J. Zhang: Information Security Practice and Experience 2009, LNCS 5451. Berlin: Springer-Verlag, 2009, p. 47-58.

[7] SCHNEIERB: John Wiley & Sons, Inc., 1994.

[8] GENNAROR: Massachusetts Institute of Technology, Cambridge, 1996.

[9] Jurisic A, Menezes. Dr Dobb's Journal. A pril 1997.22,p. 26-37.

[10] A. Shamir: Communication of the ACM Vol. 22 (1979), p. 612-613.