Threshold Signcryption Scheme Based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing

Peng Changgen, Li Xiang
Institute of Computer Science, Guizhou University
Guiyang 550025, China
Email: {sci.cgpeng, lixiang}@gzu.edu.cn

Abstract—**In this paper, we present a signcryption scheme based on elliptic curve cryptosystem, which can perfectly integrate digital signature with public key encryption. Then, based on the proposed signcryption scheme, we design a verifiable (*t*, *n*) threshold signcryption scheme. This threshold signcryption scheme not only has the advantages of threshold scheme but also has the functions that can prevent the cheating of trusted center, the cheating of participants each other, and the cheating that participants modify their private keys. In the message recovery phase, only the specified recipient can recover the signcryption message. Our proposed scheme has small communication cost, and this cost becomes smaller by compressing the points over elliptic curve.**

Keywords-signcryption; threshold scheme; verifiable secret sharing; elliptic curve cryptosystem

I. INTRODUCTION

In the network security and cryptography, the study of confidentiality and authenticity are very important. In general, confidentiality is provided by encryption, and authenticity is guaranteed by digital signature. Traditionally, these two goals are always considered separately. Signcryption is a new paradigm in public key cryptography, which was first proposed by Zheng [1] in 1997. It can simultaneously fulfil both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional "*signature-then-encryption*" [1][2][3]. Signcryption scheme will be suitable for the cases where both confidentiality and authenticity are required.

The Zheng' signcryption scheme had been simultaneously fulfilled both the functions of digital signature and public key encryption. However, the digital signature and public key encryption were separate, in other word, two operations were simply overlapped. Many authenticated encryption schemes and signcryption schemes almost have this weakness. Recently, two threshold signature encryption schemes which can perfectly integrate digital signature with public key encryption were respectively proposed in [4] and [5]. However, they cannot verify the cheating of trusted dealer and the cheating of participants each other. Due to the elliptic curve cryptosystem (ECC for short) has several advantages, such as small key sizes, high security, good flexibility, and easily implemented in hardware. It is becoming more and more important. In this paper, we shall design a verifiable (*t*, *n*) threshold signcryption scheme based on the difficulty of ECDLP. This scheme not only can perfectly integrate digital signature with public key encryption, but also can prevent the cheating of trusted center, the cheating of participants each other, and the cheating that participants modify their private keys, and it has privacy of the receiver. To make the communication cost becomes smaller, we can compress the point over elliptic curve when this scheme is implemented.

Threshold digital signature scheme is a combination of threshold secret sharing and digital signature scheme. In this paper, the (*t*, *n*) threshold scheme is built based on the Shamir' secret sharing [6]. Thus it has following characters:

- A group of *n* signers share a signcryption secret key.
- Only *t* or more participants can rebuild the secret key and generate a valid signcryption.
- Any *t*-1 or fewer participants cannot rebuild the secret key and forge valid signcryption.

II. A NEW SIGNCRYPTION SCHEME BASED ON ECC

In this section, we design a new signcryption scheme based on elliptic curve cryptosystem and Schnorr' signature scheme by employing the idea of authenticated encryption [7]. This signcryption scheme does not use the one-way hash function. The procedure of this scheme contains three phrases: the initialization phase, the signcryption phase, and the verification and message recovery phase.

A. The Initialization Phase

Our scheme requires a trusted center *CA* as a dealer, which is responsible for generating parameters. *CA* chooses a secure elliptic curve $E(F_p)$ over finite field F_p and a base point P on it which has an order of q, where q is a large prime (q≥160bits). Signer A chooses a random integer $d_A \in [1, q\text{-}1]$ as private key and computes corresponding public key $Q_A = d_A \cdot P$, and sends Q_A to *CA*. Similarly, receiver B chooses a random integer $d_B \in [1, q\text{-}1]$ as private key and computes corresponding public key $Q_B = d_B \cdot P$, and sends Q_B to *CA*. Finally, *CA* publishes p, q, $E(F_p)$, P, Q_A and Q_B.

B. Signcryption Phase

Suppose a message $m \in [1, p\text{-}1]$ will be signcrypted by A, and then it will be sent to B. The message m includes redundant

0-7803-9335-X/05/$20.00 ©2005 IEEE

information that can be applied to authenticate its validity. Signcryption operations as follow:

Step 1: Signer A chooses a random integer $k \in [1, q\text{-}1]$ and computes $Y_1 = k \cdot P$, $Y_2 = k \cdot Q_B$.

Step 2: Signer A generates the signcryption (r, s) by

$$r = m \cdot (Y_2)_x \bmod q , \tag{1}$$

$$s = k - d_A \cdot r \bmod q , \tag{2}$$

where $(Y_2)_x$ is a x-coordinate of point Y_2. Finally, signer A sends the signcryption (r, s) and Y_1 to receiver B via public channel. As is shown in (1) and (2), the signcryption (r, s) not only includes the message m (hidden in r), but also includes the signature by private key d_A of signer A.

C. Verification and Message Recovery Phase

After B receives the signcryption (r, s), he can verify its validity and recover the message m by following steps:

Step 1: Computes $Y_1' = r \cdot Q_A + s \cdot P$, $Y_2' = d_B \cdot Y_1'$.

Step 2: Verifies whether $Y_1 = Y_1'$ is correct. If it is correct, the signcryption (r, s) is valid, otherwise is invalid.

Step 3: Recovers the message m by

$$m = r \cdot (Y_2')_x^{-1} \bmod p . \tag{3}$$

Then, B checks its validity from redundant information of m.

Theorem 1 as below shows the proof of correctness about this new signcryption scheme.

Theorem 1. If the signer A can strictly carry out above signcryption steps, the signcryption (r, s) can pass the test of validity, and the specified receiver B can also recover the message m.

Proof. If user A can strictly carry out the signcryption steps, then $Y_1' = r \cdot Q_A + s \cdot P = r \cdot (d_A \cdot P) + (k - d_A \cdot r) \cdot P = k \cdot P = Y_1$, that is, the validity of signcryption (r, s) can be verified by $Y_1 = Y_1'$. Thus, we have $Y_2' = d_B \cdot Y_1' = d_B \cdot Y_1 = d_B \cdot (k \cdot P) = k \cdot Q_B = Y_2$, so we can say the specified receiver B with private key d_B can recover the message m by (3).

III. A Verifiable Threshold Signcryption Scheme

In this section, we shall design a verifiable (t, n) threshold signcryption scheme based on our proposed signcryption scheme. In this threshold scheme, there are four phases: the parameters choosing phase, the verifiable secret key split phase, the threshold signcryption phase, and the verification and message recovery phase.

A. Parameters Choosing Phase

In this threshold signcryption scheme, the receiver is still B. However, the signer is changed to a signers' group which is denoted by $G=\{P_1, P_2,\ldots, P_n\}$. That is, G is a set of n signers in which each member can sign the partial signcryption. From the definition of threshold scheme, any t out of n signers ($1\leq t \leq n$) can represent the group G to perform the signcryption. In the threshold signcryption phase, a participant will be randomly selected from group G as a designated clerk, who is responsible for collecting and verifying the partial signcryption, and then computing the group signcryption. The trusted dealer is still denoted by CA. Let C denotes the clerk. CA chooses a random integer $d \in [1, q\text{-}1]$ as a private key of group G, thus the corresponding public key is $Q = d \cdot P$.

In this section, the parameters p, q, $E(F_p)$, P, d_B and Q_B are the same as that of the subsection A in section II. Finally, CA publishes p, q, $E(F_p)$, P, Q and Q_B,

B. Verifiable Secret Key Split Phase

In following steps, we present a verifiable secret key split protocol based on Pedersen's verifiable secret sharing [8][9]. The private key d of group G will be distributed to P_i ($1\leq i \leq n$).

Step 1: The trusted dealer CA randomly generates a secret polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod q$$

over Z_q of degree t-1 satisfying $a_0 = f(0) = d$. Then, CA computes $d_i = f(i)$ as private key of P_i ($1\leq i \leq n$), thus the corresponding public key is $Q_i = d_i \cdot P$. Finally, CA publishes Q_i.

Step 2: CA sends d_i secretly to P_i ($1\leq i \leq n$) and broadcasts $a_j \cdot P$ ($1\leq j \leq t$-1) to all n signers.

Here, "*verifiable*" means each signer can verify his share. This verification is given by

$$d_i \cdot P = \sum_{j=0}^{t-1} i^j (a_j \cdot P) . \tag{4}$$

That is, each signer P_i ($1\leq i \leq n$) may use (4) to verify whether his secret key d_i from CA is correct or not. If this equation holds, the share d_i is accepted, otherwise rejected.

C. Threshold Signcryption Phase

Suppose the message $m \in [1, p\text{-}1]$ will be signcrypted by t participants from group G for the receiver B. Without loss of generality, let $P_1, P_2 ,\ldots, P_t$ are the t participants. In this phase, the group signcryption (r, s) will be generated. This phase includes four steps:

Step 1: Each signer P_i ($1\leq i \leq t$) chooses a random integer $k_i \in [1, q-1]$, then computes $Y_i = k_i \cdot P$ and sends it to clerk C and receiver B via public channel, computes $Z_i = k_i \cdot Q_B$ and sends it secretly to clerk C.

Step 2: Signcryption clerk C computes

$$Z = \sum_{i=1}^{t} Z_i = \sum_{i=1}^{t} k_i \cdot Q_B = k \cdot Q_B , \tag{5}$$

$$r = m \cdot (Z)_x \bmod p , \tag{6}$$

where $k = \sum_{i=1}^{t} k_i$, and broadcasts r to each signer P_i ($1\leq i \leq t$).

Step 3: Each signer P_i ($1\leq i \leq t$) computes

$$x_i = \prod_{j=1,j\neq i}^{t} \frac{-j}{i-j} \bmod q, \; e_i = d_i \cdot x_i \bmod q \, , \qquad (7)$$

$$s_i = k_i - e_i \cdot r \bmod q \, , \qquad (8)$$

and then sends the partial signcryption s_i to clerk C.

Step 4: After clerk C receives the partial signcryption s_i, he first computes $Y_i' = r \cdot x_i \cdot Q_i + s_i \cdot P$, and then verifies validity of partial signcryption s_i by

$$Y_i = Y_i' \, . \qquad (9)$$

If this equation holds, s_i is valid, otherwise, is invalid (the proof of correctness is similar to Theorem 1). If all the partial signcryptions are valid, C computes group signature s by

$$s = \sum_{i=1}^{t} s_i \bmod q \, . \qquad (10)$$

Finally, (r, s) as a signcryption of group G is sent to receiver B.

D. Verification and Message Recovery Phase

After receiver B receives the signcryption (r, s), he can verify its validity using public key Q of group G and recover the message m using his private key d_B by following steps:

Step 1: Computes

$$Y = \sum_{i=1}^{t} Y_i = \sum_{i=1}^{t} k_i \cdot P = k \cdot P \, ,$$

$$Y' = r \cdot Q + s \cdot P, \; Z' = d_B \cdot Y' \, .$$

Step 2: Verifies whether $Y = Y'$ is correct. If this equation holds, the signcryption (r, s) is valid, otherwise is invalid.

Step 3: Recovers the message m by

$$m = r \cdot \left(Z'\right)_x^{-1} \bmod p \, , \qquad (11)$$

and checks its validity from redundant information of m.

Following Theorem 2 is the proof of correctness about this threshold signcryption scheme.

Theorem 2. If all signers can strictly carry out the threshold signcryption steps, the signcryption can pass the test of validity and the specified receiver can also recover the message.

Proof. If all signers can strictly carry out the threshold signcryption steps, then

$$\begin{aligned} Y' &= r \cdot Q + s \cdot P \\ &= r \cdot d \cdot P + \sum_{i=1}^{t} s_i \cdot P \\ &= r \cdot d \cdot P + \sum_{i=1}^{t} (k_i - e_i \cdot r) \cdot P \\ &= r \cdot d \cdot P + k \cdot P - r \cdot \sum_{i=1}^{t} e_i \cdot P. \end{aligned}$$

By Lagrange polynomial interpolation, we have

$$\sum_{i=1}^{t} e_i = \sum_{i=1}^{t} d_i \cdot \prod_{j=1,j\neq i}^{t} \frac{-j}{i-j} = f(0) = d \, .$$

Hence $Y' = k \cdot P = Y$, signcryption can pass the test of validity. If the signcryption is valid, then

$$Z' = d_B \cdot Y' = d_B \cdot k \cdot P = k \cdot Q_B = Z \, .$$

Therefore, the receiver B with private key d_B can recover the message m by (11).

E. Security Analysis

1) Verifiable secret key distribution: In the secret key split phase, each participant can verify his share from *CA* using (4). Therefore, this threshold scheme can prevent the cheating of trusted center, the cheating of participants each other, and the cheating that participants modify their private keys. If any attacker wants to forge secret key d_i to make (4) correct, he has to solve the ECDLP problem.

2) Unforgeability of partial signcryption: In the threshold signcryption phase, it is impossible that the signer P_i modifies his secret key d_i or forges the partial signcryption s_i, because of this cheating will be verified from (9). It is also impossible that any attacker forges the partial signcryption s_i to cheat the verification of (9), because of he does not know k_i, he has to solve the ECDLP problem.

3) Unforgeability of group signature: In the threshold signcryption phase, it is impossible that signcryption clerk C or attacker forges group signature s to cheat receiver B, because of he must forge all partial signcryption s_i to make (9) correct. However, he does not know k_i and d_i, so he has to face the ECDLP problem.

4) Confidentiality of private key: Any attacker wants to obtain d, d_i and k_i from all public information in this scheme. The difficulty is equivalent to solving the ECDLP problem.

5) Against conspiracy attack: This threshold scheme has the security of Shamir's secret sharing scheme. Any t-1 or less participants from group G can not rebulid the group secret key and generate a valid group signcryption.

6) Confidentiality and unforgeability of message: Only specified receiver B who owns private key d_B can recover the message m from (11). Any attacker can not forge m to cheat receiver B, because of this cheating can be checked from redundant information of m.

7) Attack of receiver: It is impossible that the specified receiver B wants to obtain the private key d of group G from signcryption (r, s). By Lagrange polynomial interpolation, we have

$$s = \sum_{i=1}^{t} s_i \bmod q = (k - r \cdot d) \bmod q \, .$$

However, B does not know k, thus he can not computes d.

IV. Algorithm Strategy and Efficiency Analysis

Because of the ECC is applied to design our signcryption scheme, the key sizes can be considerably reduced. Thus it has lower communication complexity.

In order to make the communication cost becomes smaller, we use compression method to transmit the point over elliptic curve. A point $P(x_p, y_p)$ over elliptic curve can be represented more compactly by storing only x-coordinate x_p and a certain bit b_{xy} derived from x_p and y_p. The point $P(x_p, y_p)$ can be recovered from x_p and b_{xy} [10]. By means of such compressing technique, the communication cost can be reduced. The concrete analysis about this as follow:

- In the secret key split phase, to achieve the verifiable function, the dealer *CA* wants to broadcast *t* points *Q*, $a_j \cdot P$ ($1 \leq j \leq t$-1). If no compression, *CA* need broadcast $2t|p|$ bits. However, after these points are compressed, the value can be reduced to $t(|p|+1)$ bits.
- In the threshold signcryption phase, *t* participants need send $t(6|p|+|q|)$ bits, we can reduce it to $t(3|p|+1+|q|)$ bits.

Similarly, due to the property of ECC, the computational cost can be obviously reduced in our scheme. In fact, the modular exponentiation and point multiplication are the most time-costing computation in cryptosystem. When $|p|$=1024 bits, $|q|$=160 bits, the operation of point multiplication is about 8 times faster than the operation of modular exponentiation [11]. Therefore, compare to the signcryption scheme based on the difficulty of computing discrete logarithms, such as scheme in [4], our scheme has higher computational efficiency.

V. Conclusions

In this paper, we proposed a new signcryption scheme, and based this signcryption scheme we built a (*t*, *n*) threshold signcryption scheme. These schemes not only can solve the problem that signature and encryption were separated in early signcryption schemes, but also can provide confidentiality, authenticity, data integrity and anonymity of receiver. Besides, the threshold signcryption scheme has advantages of verifiable threshold scheme, and it can prevent various cheating. In addition, we point out such algorithm technique: compressing the point over elliptic curve, so that the communication cost can become smaller.

In this paper, the threshold signcryption scheme requires a trusted center as a dealer, which is responsible for choosing system parameters and distributing secret key. In fact, our threshold signcryption scheme can be easily converted into a threshold signcryption scheme without trusted center based on our signcryption scheme in section II by employing Pedersen's verifiable secret sharing scheme without trusted center [12]. In such scheme, each participant plays a role as the dealer *CA* in our scheme.

References

[1] Y. Zheng, "Signcryption and its applications in efficient public key solutions," Proc. Information Security Workshop (ISW'97), LNCS 1397, Springer-Verlag, pp. 291-312, 1998.

[2] Y. Zheng, "Digital signcryption or how to achieve cost (signature &encryption)<<cost (signature) +cost (encryption)," *Advances in* Cryptology-Crypto'97 Proceedings, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

[3] Y. Zheng, H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information Processing Letters, vol. 68, no. 5, pp. 227-233, 1998.

[4] CAO Zhen-fu, LI Ji-guo, LI Jian-zhong, "A new (*t*, *n*) threshold signature encryption scheme with specified receiver," Journal of China Institute Communications, vol.24, no.5, pp. 8-12, 2003.

[5] DAI Yuan-jun, YANG Cheng, "(t, n) threshold signature encryption scheme base on elliptic curve cryptosystem," Application Research of Computer, vol. 21, no. 9, pp. 142-146, 2004.

[6] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[7] W. B. Lee, C. C. Chang, "Authenticated encryption scheme without using a one-way function," Electronic Letters, vol. 31, no. 19, pp. 1656-1657, 1995.

[8] T. P. Pedersen, "Distributed provers with applications to undeniable signatures," Proc. of Eurocrypt'91, LNCS 547, Springer Verlag, pp. 221-238, 1991.

[9] K. Takaragi, K. Miyazaki, M. Takahashi, "A threshold digital signature issuing scheme without secret communication," Proc. of the IEEE Conf. [s.1]: IEEE Press, pp. 101-118, 1998.

[10] IEEE P1363, "Standard specifications for public key cryptography," IEEE, 2000. http://grouper.ieee.org/groups/1363/.

[11] N. Koblitz, A. Menezes, S. Vanstone, "The state of elliptic curve cryptography," Designs, Codes, and Cryptography, vol. 19, no. 2-3, pp. 173-193, 2000.

[12] T. P. Pedersen, "A threshold cryptosystem without a trusted party," Proc. of Eurocrypt'91, LNCS 547, Springer Verlag, pp. 522-526, 1991.