SIGNCRYPTION SCHEME WITH THRESHOLD SHARED UNSIGNCRYPTION PREVENTING MALICIOUS RECEIVERS

ZHANG Zhang[1,2] CAI Mian[1,2] QU Jin[1]

[1](National Key Lab. of Integrated Service Networks, Xidian University, Xi'an, China, 710071)

[2](The State Key Lab. of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing, China, 100039)

Email: zzhang74@yahoo.com.cn

Abstract: A new signcryption scheme with (t, n) shared unsigncryption based on discrete logarithm is proposed, which is the integration of Jung et al.'s signcryption scheme and Shamir secret sharing scheme. In this scheme, any t of n receivers can unsigncrypt the message and any t-1 or fewer receivers can not unsigncrypt the message. As compared to Hsu and Wu's authenticated encryption scheme with (t, n) shared verification, the proposed scheme has the following advantages: it is more efficient for signcryption; it can prevent malicious receivers from cheating others.

Key words: signcryption; discrete logarithm; secret sharing

1. Introduction

Secure and authenticated transmit message is one of the major aims of computer and communication security research. The traditional method to achieve this is signature followed by encryption[1]. In 1997, Zheng introduced the concept of signcryption scheme[2], which combines a function of digital signature scheme with a symmetric key encryption scheme. Signcryption does not only provide authenticity and confidentiality in a single step, but also give more efficient computation than the trditional signature-then-encryption. All of the above schemes consist of only single receivers. However, in some practical applications, it is needed to decrypt and verify the signature by some specified receivers. In 1998, Hsu and Wu proposed an authentication encryption scheme with (t, n) shared verification [3]. In Hsu and Wu's scheme, the sender firstly generate the signature then encrypt them to the ciphertext, therefore it is not very efficient. Another drawback of Hsu and Wu's scheme is that it can not prevent some malicious receivers from cheating others. In 2000, Lu and Chen proposed an improvement authenticated encryption scheme with (t, n) shared verification to prevent malicious receivers[4]. However, Lu and Chen's scheme still obeys the principle 'sign first, then encrypt' and it is not very efficient.

In this paper, a new signcryption scheme with (t, n) shared verification based on discrete logarithm is proposed, which is the integration of Jung et al.'s signcryption scheme[5] and Shamir secret sharing scheme[6]. In this scheme, any t of n receivers can unsigncrypt the message and any t-1 or fewer receivers can not unsigncrypt the message. As compared to Hsu and Wu's authenticated encryption scheme with (t, n) shared verification, the proposed scheme has the following advantages: it is more efficient for signcryption; it can prevent malicious receivers from cheating others.

0-7803-7490-8/02/$17.00©2002 IEEE.

2. Preliminaries

Our constructions of signcryption scheme with (t, n) shared unsigncryption are based on the Shamir secret sharing scheme and Chaum-Petersen's signature of equality of discrete logarithms[7]. These two basic tools are briefly described.

2.1 Description of Shamir scheme

A (t, n) secret sharing scheme is a scheme to distribute a secret K into n users in such a way that any subset of t users can cooperate to reconstruct the secret K but that the collusion of t-1 or fewer users can obtain no information on the secret. Shamir's scheme is based on Lagrange interpolation in a field. To implement it, a polynomial f of degree t-1 is randomly chosen in Z_q such that $f(0)=K$. Each user i is given a secret share $f(u_i)$, where u_i is the public information associated with user i. Now any subset of t of n users can reconstruct the secret $K=f(0)$ as:

$$K = \sum_{i=1}^{t} f(u_i) \prod_{j=1, j\neq i}^{t} \frac{-u_j}{u_i - u_j} \qquad (1)$$

2.2 Description of Chaum-Peterson's signature of equality of discrete logarithms

The problem of proof of equality of discrete logarithms has many applications, where the prover proves to a verifier that $\log_{g'} h' = \log_g h$ (i. e. $h'=g'^x$ and $h=g^x$) without revealing $x = \log_{g'} h' = \log_g h$. Here we assume that p is a large prime and q is a large prime divisor of p-1. Let g, g' be a generator with order q in Z_p^* and $h'=g'^x \bmod p$ and $h=g^x \bmod p$ for $x \in Z_q^*$. Let $H:\{0,1\}^* \rightarrow Z_q^*$ be a one-way hash function.

The prover chooses $k \in_R Z_q^*$ and computing : $r=H(h'\|h\|g'\|g\|g'^k\|g^k)$ and $s=k-rx \bmod q$, where the symbol $\|$ denotes the concatenation of two binary strings. The signature can be verified by checking $r=H(h'\|h\|g'\|g\|g'^s h''\|g^s h^r)$. The scheme has following properties. If we do not have $h'=g'^x \bmod p$ and $h=g^x \bmod p$, it is impossible (computational hard) to generate r and s such that $r=H(h'\|h\|g'\|g\|g'^s h''\|g^s h^r)$ and it is hard to get extra information about x from the given r and s. Foe simplicity, we use $EQ(x, h', h, g', g)$ to denote the Chaum-Petersen's signature of equality of discrete logarithms.

3. The proposed signcryption scheme with (t, n) shared unsigncryption

3.1 The proposed scheme

Our scheme requires a system authority (SA), which is responsible for defining system parameters and making them public. The system consists of three parties: the SA, the sender and the receivers group. The procedure of the scheme contains three phases: the system initialization phase, the signcryption phase and the unsigncryption phase.

System initialization: SA selects two large prime numbers p and q such that q is a divisor of p-1, and selects a generator g with order q in Z_p^*. Let E and D denote the encryption and decryption algorithms of a private key cipher such as SPEED[8]. Encrypting a message m with a key k is indicated by $E_k(m)$ while decrypting a cipher c with a key k is denoted by $D_k(c)$. Let H be a one-way hash function. Let KH denote the k-ed hash algorithm[9]. We use $KH_k(m)$ denote hashing a message m with KH under a key k. SA makes p, q, g, E, D , H and KH public.

Let A be the sender, G=(U_1, U_2, ……, U_n) be the group of n receivers, and $ID_i \neq 0$ be the identity associated with U_i. SA randomly selects an integer $x_A \in Z_q^*$ to be the secret key for A and computes the corresponding public key as $y_A = g^{x_A} \bmod p$. For the receivers group G, SA randomly selects an integer $x_G \in Z_q^*$ to be the secret key for G and computes the corresponding public key as

$y_G = g^{x_G} \bmod p$. After that, SA randomly generates a (t-1)-degree polynomial

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

where $a_i \in_R Z_q^* \ (i = 1, \cdots, t-1)$, and computes the secret key $x_i = f(ID_i) \bmod q$ and public key $y_i = g^{x_i} \bmod p$ for each U_i. Finally SA delivers x_A and x_i to A and U_i via a secure channel and publishes y_A, y_i and y_G.

Signcryption: To send message m to the receivers group, A randomly picks $x \in Z_q^*$ and computes (c, R, s) as follows:

(1) $k = H(y_G^x) \bmod p$, split it into k_1 and k_2, e.g. let $(k_1 \| k_2) = H(k)$.

(2) $r = KH_{k_2}(m, bind\_infor)$, where *bind_infor* is information to identify receivers group, such as the group's public key.

(3) $s = x/(r + x_A) \bmod q$. (2)

(4) $R = g^r \bmod p$. (3)

(5) $c = E_{k_1}(m)$.

unsigncryption: Without loss of generality, let G'=(U_1, U_2, ……, U_t) be t receivers of G that want to cooperatively unsigncrypt the message. Firstly each U_i uses his own secret key to compute

$$F_i = (y_A R)^{sJ_i} \bmod p \quad (4)$$

where

$$J_i = x_i \prod_{j=1, j \neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \bmod q \quad (5)$$

and presents it to other participants in G'. With the knowledge of

$$F = \prod_{i=1}^{t} F_i \bmod p \quad (6)$$

the message can be unsigncrypted as follows

(1) $k = H(F)$ and split it into k_1 and k_2.

(2) $m = D_{k_1}(c)$

(3) check if $R = g^{KH_{k_2}(m, bind\_infor)} \bmod p$ (7)

Theorem 1 If the sender follows the above signcryption process, the receivers always unsigncrypt the message.

Proof From eqn. 1 and eqn. 5,

$$\sum_{i=1}^{t} J_i = \sum_{i=1}^{t} x_i \prod_{j=1, j \neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \bmod q = x_G$$

so that

$$F = (\prod_{i=1}^{n} F_i \bmod p) \bmod q = (y_A R)^{sx_G} \bmod p$$

From eqn. 2

$$y_G^x = (y_A R)^{sx_G} \bmod p = F \bmod p$$

so that

$$k = H(F)$$

therefore $m = D_{k_1}(c)$ and

$$R = g^r \bmod p = g^{KH_{k_2}(m, bind\_infor)} \bmod p$$

Q. E. D.

3.2 Performance analysis

The proposed scheme requires 2 modular exponentiations in the process of signcryption and 2 modular exponentiation for each receivers in the unsigncryption process. It is superior to Hsu and Wu's (t, n) shared verification scheme that requires 3 and 3 modular exponentiations respectively.

3.3 Preventing malicious receivers

In order to prevent malicious receivers from cheating others, each receivers U_i computes $EQ(x_i, F_i, y_i, (y_A R)^{sJ_i'} \bmod p, g)$, where $J_i' = \prod_{j=1, j \neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \bmod q$. This is only possible if the values F_i is computed as described above.

3.4 Security analysis

Since the signcryption process is the same as the Jung et al.'s scheme, forging a ciphertext for any message m is equivalent to forging Jung et al.'s scheme. In the unsigncryption phase, any t-1 or fewer receivers can not recover the value of $(y_A R)^{sx_G} \bmod p$, thus they can not unsigncrypt the message. Computing the secret key x_i from F_i is equivalent to computing discrete logarithms.

In addition, since any verifier can not compute a fake Chaum-Petersen's signature of equality of discrete logarithms, the proposed

scheme can prevent some malicious receivers from cheating others by present incorrect F_i.

4 Conclusion

In this paper, a new signcryption scheme with (t, n) shared unsigncryption based on discrete logarithm is proposed, which is the integration of Jung et al.'s signcryption scheme and Shamir secret sharing scheme. In this scheme, any t of n receivers can unsigncrypt the message and any t-1 or fewer receivers can not unsigncrypt the message. As compared to Hsu and Wu's authenticated encryption scheme with (t, n) shared verification, the proposed scheme has the following advantages: it is more efficient for signcryption; it can prevent malicious receivers from cheating others.

References

1. Nyberg K. and Rueppel R. A., Message recovery for signature schemes based on discrete logarithm problem, Advances in Cryptology—Eurocrypt'94, Springer-Verlag, 1995, pp. 123-128.

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

3. Hsu C. and Wu T., Authentication encryption scheme with (t, n) shared verification, IEE Proc. Comput. Digit. Tech. 1998, 145 (2): pp. 117-120.

4. Lu J. and Chen H., Improvement of authenticated encryption scheme with (t, n) shared verification, The Proceedings of IEEE COMPSAC' 2000, 2000, pp. 445-448.

5. Jung H., Lee D., Lim J. and Chang K., signcryption scheme with forward security. Proceedings of WISA2001, Springer-Verlag, 2001.

6. Shamir A., How to share a secret, Comm. of ACM. 1979, 24(11): pp. 612-613 .

7. Chaum D. and Peterson T., Wallet databases with observers, Advances in Cryptology— Crypto'92, Springer-Verlag, 1993, pp. 89-105.

8. Zheng Y., The SPEED cipher, Proceedings of Financial Cryptography'97, Springer-Verlag, 1997.

9. Bellare M., Canetti R. and Krawczyk H., Keying hash functions for message authentication, Advances in Cryptology— Crypto'96, Springer-Verlag, 1996, pp. 1-15.