Identity Based Threshold Proxy Signcryption Scheme

Meng Wang, and Zhijing Liu
School of Computer Science and Technology
Xidian University, Xi'an 710071, China
wangmeng@xidian.edu.cn,liuprofessor@163.com

Abstract

An identity based cryptosystem is a novel type of public cryptographic scheme in which the public keys of the users are their identities or strings derived from their identities. In a (t,n) proxy signature scheme, the original signer can delegate his/her signing capability to n proxy signers such that any t or more proxy signers can sign messages on behalf of the former, but $t-1$ or less of them cannot do the same thing. However, in many situations we want to enjoy confidentiality, authenticity and non-repudiation of message simultaneously. In this paper we propose an identity based threshold proxy signcryption scheme using bilinear pairings. The security of the scheme is also analyzed.

1. Introduction

The idea of an identity-based encryption (IBE) scheme is that an arbitrary string can serve as a public key [1]. The main advantage of this approach is to largely reduce the need for public key certificates and certificate authorities, because a public key is associated with identity information such as a user's email address. For such a system to work there are Trusted Authorities (or Private Key Generators) that generate user's private key from their identity information. Signcryption, first proposed by Zheng [2], is a new cryptographic primitive which simultaneously fulfill both the functions of signature and encryption in a single logical step, and with a computational cost significantly lower than that required by the traditional signature-then-encryption approach. Identity based signcryption scheme is rapidly emerging in recent years ([3], [4], [5]).

A proxy signature scheme allows one user Alice, called original signer, to delegate her signing capability to another user Bob, called proxy signer. After that, the proxy signer Bob can sign messages on behalf of the original signer Alice. Upon receiving a proxy signature on some message, a verifier can validate its correctness by the given verification procedure, and then is convinced of the original signer's agreement on the signed message. In other words, proxy signatures can be distinguished from standard signatures signed by either the original signer or the proxy signer. Proxy signature schemes have been suggested for use in a number of applications, particularly in distributed computing where delegation of rights is quite common, such as e-cash systems, mobile agents for electronic commerce, mobile communications, grid computing, global distribution networks, and distributed shared object systems.

The basic idea of ID-Based proxy-signcryption schemes is as follows. The original signcrypter Alice sends a specific message with its signature to the proxy signcrypter Bob, who then uses this information to construct a proxy private key. With the proxy private key, Bob can generate proxy signcryption by employing a specified standard ID-Based signcryption scheme. When a proxy signcryption is given, a verifier first computes the proxy public key from some public information, and then checks its validity according to the corresponding standard ID-Based signcryption verification procedure.

Recently, Xu et al proposed an identity based threshold proxy signature scheme [6]. A (t,n) proxy signature scheme is a variant of the proxy signature scheme in which the proxy signature key is shared by a group of n proxy signers in such a way that any t or more proxy signers can cooperatively employ the proxy signature keys to sign messages on behalf of an original signer, but $t-1$ or fewer proxy signers cannot. This technology not only allows the original signer to delegate the proxy signing power to a group of proxy signers instead of one single proxy signer, but also lets the original signer to set the threshold value t freely ($1 \le t \le n$). Therefore, the threshold proxy signature approach is more practical, flexible and secure than standard proxy signature schemes.

Proceedings of the 2005 The Fifth International Conference on Computer and Information Technology (CIT'05)
0-7695-2432-X/05 $20.00 © 2005 IEEE

However, in many situations we want to enjoy confidentiality, authenticity and non-repudiation of message simultaneously. Thus, we propose an identity based threshold proxy signcryption scheme. Following the definitions from [7] and [8], a strong ID-based threshold proxy signcryption scheme should satisfy the following properties:

1) Strong unforgeability: A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.

2) Verifiability: The original signer's delegation on the signed message is verifiable using publicly available parameters.

3) Strong identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

4) Strong undeniability: Once a proxy signer creates a valid proxy signature for an original signer, he cannot repudiate his signature creation against anyone else.

5) Prevention of misuse: The proxy cannot use the proxy key for other purposes than generating a valid proxy signature. That is the proxy cannot sign messages that have not been authorized by the original signer.

The rest of this paper is organized as follows. Section 2 contains some formal definitions bilinear Diffie-Hellman problems. Section 3 gives the general identity based signcryption scheme. Our scheme is presented in Section 4. We analyze the security of our scheme in Section 5. Section 6 concludes the paper.

2. Preliminaries

Let $(G_1,+)$ and $(G_2,\cdot)$ be two cyclic groups of prime order q. The bilinear pairing is given as $\hat{e}: G_1 \times G_1 \to G_2$, which satisfy the following properties:

1) Bilinear: For $P, Q, R \in G_1$, there exists $\hat{e}(P+Q,R)=\hat{e}(P,R)\hat{e}(Q,R)$ and $\hat{e}(P,Q+R)=\hat{e}(P,Q)\hat{e}(P,R)$.

2) Non-degenerate: There exists $P,Q \in G_1$ such that $\hat{e}(P,Q) \neq 1$.

3) Computable: There exists an efficient algorithm to compute $\hat{e}(P,Q) \forall P,Q \in G_1$.

Now we specify some versions of Diffie-Hellman problems. The security of our scheme described here relies on the hardness of the following problems.

1) Decisional Diffie-Hellman problem (DDHP) in $(G_1, G_2, \hat{e})$ is to decide whether $h=\hat{e}(P,P)^{abc}$ or not, given (P, aP, bP, cP) and an element $h \in G_2$.

2) Computational Diffie-Hellman problem (CDHP) in $(G_1, G_2, \hat{e})$ is to compute $h=\hat{e}(P,P)^{abc}$, given (P, aP, bP, cP).

3) Discrete Logarithm Problem (DLP): Given two group elements P and Q find an integer n, such that $Q=nP$ whenever such an integer exists.

4) Gap Diffie-Hellman groups: Groups where the CDHP is hard but the DDHP is easy.

No algorithm is known to be able to solve any of them so far

3. General ID-Based Signcryption Scheme

Generally, identity based signcryption schemes are made of four algorithms which are the following.

[Setup]
The PKG picks a security parameter k and generates the system's public parameters and the master-key.

[Extraction]
This algorithm is performed by the PKG when a user requests a secret key corresponding to his identity. The secret key is given to the user in a secure way. This step is done only once for every identity and uses the same Setup data for many different identities.

[Signcryption]
To send a message m to B, A computes Signcrypt(m, d_{ID_A}, Q_{ID_B}) to obtain the ciphertext σ.

[Unsigncryption]
On receiving the ciphertext σ, B computes Unsigncrypt$(\sigma, d_{ID_B}, Q_{IDA})$ and obtains the plaintext m or the symbol $\perp$ if σ was an invalid ciphertext between the two identities.

Of course we require for consistency that if

$$\sigma = \text{Signcrypt}(m, d_{ID_A}, Q_{ID_B})$$

holds then $m = \text{Unsigncrypt}(\sigma, d_{ID_B}, Q_{IDA})$.

4. Our Proposed Scheme

Our scheme is based on LQ-IBS (Libert-Quisquater Identity based signcryption scheme) [3]. It consists of the following five phases:

[Setup]

Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q, a generator P of G_1, a bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ and hash functions:

$$H: \{0,1\}^* \to Z_q, H_1: \{0,1\}^* \to G_1,$$
$$H_2: \{0,1\}^* \to Z_q^*, H_3: G_2 \to \{0,1\}^n.$$

It chooses master key $s \in Z_q^*$ and computes $P_{pub} = sP$. It also chooses a secure symmetric cipher (E, D). The PKG publishes system's public parameters

$$\{G_1, G_2, n, k, q, \hat{e}, P, P_{pub}, H, H_1, H_2, H_3, E, D\}$$

and keeps the master key s secret. Let P_0 be the original signer and $QUAL = \{P_1, P_2, ..., P_n\}$ be the proxy group of n proxy signcrypters. Each user P_i owns a secret key $d_i \in G_1$.

[Extraction]

Given an identity, the PKG computes $Q_{ID} = H_1(ID)$, and the private key $d_{ID} = sQ_{ID}$.

[Generation of the proxy share]

Let m_w be the warrant consisting the identity of the original signcrypter and the proxy signcrypters, the threshold parameter t and the valid delegation time. Every proxy signcrypter P_i calculates its own proxy signcrypting key share as follows:

Step1: The original signer P_0 first chooses $x_w \in Z_q^*$ randomly and computes $U_w = x_w P$. Then he computes $V_W = d_0 + x_w H_w$ in which $H_W = H_2(ID_0, m_w, U_w)$ and sends m_w and $w = <U_w, V_w>$ to each $P_i \in QUAL$.

Step2: The proxy signcrypter P_i first takes $Q_0 = H_1(ID_0) \in G_1$ and $H_w = H_2(ID_0, m_w, U_w) \in G_1$.

He accepts the signature if

$$\hat{e}(P, V_w) = \hat{e}(P_{pub}, Q_0)\hat{e}(U_w, H_w)$$

holds and rejects it otherwise.

Finally P_i computes $s_i = d_i + \frac{1}{n} V_w$ as his own proxy signcryption share.

Step3: P_i chooses a $(t-1)$-degree polynomial $g_i(x) = \sum_{l=1}^{t-1} a_{il} x^l + s_i$ with random coefficients $a_{il} \in G_1$ and publishes $A_{il} = \hat{e}(P, a_{il})$ for $l = 1, 2..t-1$.

A_{i0} can be calculated as

$$\hat{e}(P, s_i) = \hat{e}(P_{pub}, H_1(ID_i))\hat{e}(P_{pub}, \frac{1}{n} Q_0)\hat{e}(U_w, \frac{1}{n} H_w)$$

Then P_i sends $g_i(j)$ to P_j via a secure channel for every $j \neq i$.

Step4: On receiving $g_j(i)$, P_i check the equality

$$\hat{e}(P, g_j(i)) = \prod_{k=0}^{t-1} A_{jk}^{i^k}$$

If it holds P_i computes his proxy signcrypting key share $dp_i = \sum_{k=1}^{n} g_k(i)$.

[Proxy Signcryption]

Step1: Each $P_i \in QUAL$ randomly chooses a $(t-1)$-degree polynomial

$$f_i(x) = \sum_{l=1}^{t-1} b_{il} x^l + b_{i0}$$

with random coefficients $b_{il} \in Z_q^*$ and publishes $B_{il} = b_{il} P$. Furthermore, P_i sends $f_i(j)$ to P_j via a secure channel for $j \neq i$. On receiving $f_i(j)$, P_j validates

$$f_i(j)P = \sum_{k=0}^{t-1} j^k \bullet B_{ik}$$

If it holds, each P_i computes his secret share $r_i = \sum_{k=1}^{n} f_k(i)$.

Step2: Let $D = \{P_1, P_2, ..P_t\}$ be the actual proxy signcrypters. Each $P_i \in D$ applies the Lagrange interpolation formula to compute $x_i = \eta_i r_i$, in which

$$\eta_i = \prod_{j \neq i}^{j \in \{1,2,...,t\}} \frac{j}{j-i}$$

Then he computes

$$Q_{ID_B} = H_1(ID_B)$$
$$k_{1i} = \hat{e}(P, P_{pub})^{x_i}$$
$$k_{2i} = \hat{e}(P_{pub}, Q_{ID_B})^{x_i}$$

Finally each $P_i \in D$ sends (k_{1i}, k_{2i}) to a designated trusted third party via a secure channel.

Step3: To signcrypt a message $m \in \{0,1\}^*$, the designated trusted third party computes

$$k_1 = \prod_{i=1}^{t} k_{1i}$$

$$k_2 = H_3(\prod_{i=1}^{t} k_{2i})$$

$$c = E_{k_2}(m)$$

$$r = H_2(c, k_1)$$

Then he sends r to each $P_i \in D$.

Step4: Each $P_i \in D$ calculates $S_i = r_i P_{pub} - r dp_i$ and sends it to the designated trusted third party via a secure channel.

Step5: The third party computes $S = \sum_{i=1}^{t} \eta_i S_i$ in which $\eta_i = \prod_{j \in \{1,2,\ldots,t\}, j \neq i} \frac{j}{j-i}$ and sends (m_w, U_w, c, r, S) to the receiver Bob.

[Unsigncryption]

When receiving (m_w, U, c, r, S), the verifier Bob first takes $Q_i = H_1(ID_i) \in G_1$ and $H_w = H_2(ID_0, m_w, U_w)$.

He then computes

$$k_1' = \hat{e}(P, S)\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r$$

$$k_2' = H_3(\hat{e}(S, Q_{ID_B})\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(H_w, U_w)^r)$$

$$m = D_{k_2'}(c)$$

If $r \neq H_2(c, k_1')$ return $\perp$ else accepts m.

5. Security Analysis

Consistency: The consistency can be easily verified by the following equations:

$$\begin{aligned}
k_1' &= \hat{e}(P, S)\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r \\
&= \hat{e}(P, \sum_{i=1}^{t} \eta_i S_i)\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r \\
&= \hat{e}(P, \sum_{i=1}^{t} \eta_i r_i P_{pub})\, \hat{e}(P, \sum_{i=1}^{t} \eta_i dp_i)^{-r}\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r \\
&= \hat{e}(P, \sum_{i=1}^{t} \eta_i r_i P_{pub})\, \hat{e}(P, \sum_{k=1}^{n} \sum_{i=1}^{t} \eta_i g_k(i))^{-r}\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r \\
&= \hat{e}(P, \sum_{i=1}^{t} \eta_i r_i P_{pub})\, \hat{e}(P, V_w + \sum_{k=1}^{n} d_k)^{-r}\, \hat{e}(P_{pub}, \sum_{i=0}^{n} Q_i)^r\, \hat{e}(U_w, H_w)^r \\
&= \hat{e}(P, \sum_{i=1}^{t} \eta_i r_i P_{pub})\, \hat{e}(V_w + \sum_{k=1}^{n} d_k, Q_{ID_B})^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r \\
&= H_3(\hat{e}(\sum_{i=1}^{t} \eta_i r_i P_{pub}, Q_{ID_B})\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^{-r}\, \hat{e}(U_w, H_w)^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r) \\
&= H_3(\hat{e}(\sum_{i=1}^{t} \eta_i r_i P_{pub}, Q_{ID_B})\, \hat{e}(\sum_{i=1}^{t} \eta_i dp_i, Q_{ID_B})^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r) \\
&= H_3(\hat{e}(\sum_{i=1}^{t} \eta_i r_i P_{pub}, Q_{ID_B})\, \hat{e}(\sum_{k=1}^{n} \sum_{i=1}^{t} \eta_i g_k(i), Q_{ID_B})^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r) \\
&= H_3(\hat{e}(\sum_{i=1}^{t} \eta_i r_i P_{pub}, Q_{ID_B})\, \hat{e}(V_w + \sum_{k=1}^{n} d_k, Q_{ID_B})^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r) \\
&= H_3(\hat{e}(\sum_{i=1}^{t} \eta_i r_i P_{pub}, Q_{ID_B})\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^{-r}\, \hat{e}(U_w, H_w)^{-r}\, \hat{e}(\sum_{i=0}^{n} Q_i, d_{ID_B})^r\, \hat{e}(U_w, H_w)^r) \\
&= H_3(\hat{e}(P_{pub}, Q_{ID_B})^{\sum_{i=1}^{t} x_i}) = H_3(\prod_{i=1}^{t} k_{2i}) = k_2
\end{aligned}$$

Strong unforgeability: Because $s_i = d_i + \frac{1}{n} V_w$ contains private key d_i of the proxy agent P_i in the identity based threshold signcryption phase, without private key information of the proxy agents the original proxy signcrypter cannot generate a valid ID-based threshold signcryption scheme by himself.

Strong identifiability: Because the verifier has to compute $Q_i = H_1(ID_i)$ in the unsigncryption phase, any verifier can determine which proxy agents participate in the identity based threshold proxy signcryption.

Strong nonrepudiation: The valid signcryption contains the warrant m_w, which must be verified in the process of the unsigncryption. It cannot be modified by the proxy signcrypters. Thus once the proxy agents creates a valid proxy signcryption for the original, they cannot repudiate the signcryption creation.

Prevention of misuse: Obviously, our proposed scheme satisfies the properties of verifiability and prevention of misuse.

6. Conclusions

In this paper we proposed an identity based threshold proxy signcryption scheme from bilinear pairings. Completeness security analysis of the scheme

is presented. To the best of authors' knowledge, our scheme is the first identity based threshold proxy signcryption scheme. Future research involves proposing more efficient schemes than the current one.

References

[1] Shamir, A., "Identity-base Cryptosystems and Signature Schemes". Proc. of Crypto'84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, (1984) pp.47-53.

[2] Y.Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost(Encryption)". CRYPTO 1997, vol.1294 of LNCS, Springer-Verlag, 1997, pp.165-179.

[3] B.Libert and J-J.Quisquater, "New Identity Based Signcryption Schemes from Pairings". In IEEE Information Theory Workshop, pages 155-158, 2003.

[4] X.Li, K.Chen, "Identity Based Proxy-Signcryption Scheme from Pairings". In Proceedings of the 2004 IEEE International Conference on Services Computing (SCC'04).

[5] X.Boyen, "Multipurpose ID-Based Signcryption : A Swiss Army Knife for Identity-Based Cryptography". CRYPTO 2003, volume 2729 of LNCS, Springer Verlag, 2003, pp.382-398.

[6] J.Xu, Z.F.Zhang, and D.G.Feng, "Identity Based Threshold Proxy Signature". Cryptology ePrint Archive, Report 2004/250, 2004. Available at http://eprint.iacr.org.

[7] B.Lee, H.Kim, K.Kim, "Strong Proxy Signature and its Applications", SCIS2001, Jan.23 26, 2001, vol 2/2 pp 603-608.

[8] Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow, "Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity". ICISC 2003, November 27-28, 2003, Revised Papers, vol.2971 of LNCS, Springer, 2003, pp.352–369.