Identity Based Proxy-Signcryption Scheme from Pairings *

Xiangxue Li Kefei Chen
Department of Computer Science and Engineering
Shanghai Jiaotong University, Shanghai, China
{ *xxli,chen-kf* }*@cs.sjtu.edu.cn*

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. A signcryption is a primitive that provides private and authenticated delivery of messages between two parties. Proxy signature schemes are variations of ordinary digital signature schemes and have been shown to be useful in many applications. In this paper, We proposed an identity based proxy-signcryption scheme from pairings. Also we analyze the proposed scheme from efficiency and security points of view. Heuristic arguments have been given for those security properties. We have shown that the proxy-signcryption scheme is as efficient as ordinary identity based signcryption schemes under certain circumstances.

1. Introduction

As a variation of ordinary digital signature scheme, a proxy signature scheme enables a proxy signer to sign messages on behalf of the original signer([5], [6], [9], [10]). 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. Proxy signature schemes have been shown to be useful in many 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.

Signcryption is a public key primitive proposed by Zheng ([15]) to achieve the combined functionality of digital signature schemes and encryption in an efficient manner. Many researchers have proposed variations of signcryption schemes([1], [4], [7], [8], [11]). One of them is a proxy-signcryption which efficiently combines a proxy signature scheme with a signcryption([4]). However, none of existing signcryption schemes are identity based proxy-signcryption schemes. In this paper we propose an identity based proxy-signcryption scheme from pairings. We analyze the proposed scheme from efficiency and security points of view. We show that the scheme is as efficient as ordinary identity based signcryption schemes under certain circumstances.

The rest of this paper is organized as follows. Some definitions and preliminary works are given in section 2. Section 3 gives the general identity based signcryption scheme. Section 4 describes our identity based proxy-signcryption scheme. Section 5 analyzes the scheme. Section 6 presents our concluding remarks.

2. Preliminaries

In this section, we will briefly describe the basic definition and properties of the bilinear pairings and some problems.

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a, b be elements of Z_q^*. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairings is a map $\widehat{e} : G_1 \times G_1 \longrightarrow G_2$ with the following properties:

1) Bilinear: $\widehat{e}(aP, bQ) = \widehat{e}(P, Q)^{ab}$;

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

3) Computable: There is an efficient algorithm to computa $\widehat{e}(P, Q)$ for all $P, Q \in G_1$.

Modified Weil Pairing and Tate Pairing are examples of cryptographic bilinear maps. Currently active research is being carried out to obtain efficient algorithms to compute pairings. Our work excludes this area.

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

*This work is partially supported by NSFC (No. 60273049 and 90104005).

Let G_1 be a cyclic additive group generated by *P*, whose order is a prime *q*, and G_2 be a cyclic multiplicative group of the same order *q*, a bilinear pairing $\widehat{e} : G_1 \times G_1 \longrightarrow G_2$:

1) Computation Diffie-Hellman Problem (CDHP): Given P, aP, bP for $a, b \in Z_q^*$, to compute abP.

2) Decision Bilinear Diffie-Hellman Problem (DBDHP): Given P, aP, bP, cP for $a, b, c \in Z_q^*$, and an element $h \in G_2$, to decide whether $h = \widehat{e}(P, P)^{abc}$.

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

3. General Identity Based Signcryption

In 1984, Shamir introduced identity based cryptosystems ([13]) in which the user's public key can be generated from a publicly identifiable information such as his email address. For such a system to work there are Trusted Authorities (or Private Key Generators) that generate users' private key from their identity information. Many identity based signature schemes and identity based signcryption schemes have been devised since 1984 ([2], [3], [7], [8], [11], [12]).

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($\sigma, d_{ID_B}, Q_{ID_A}$) 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

σ=Signcrypt(m, d_{ID_A}, Q_{ID_B})

then

m=Unsigncrypt($\sigma, d_{ID_B}, Q_{ID_A}$).

Malone-Lee defines extended security notions for identity based signcryption schemes([8]). These notions are sematic security(i.e., indistinguishability against adaptive chosen ciphertext attacks, IND-IDSC-CCA) and unforgeability against adaptive chosen messages attacks(EF-IDSC-ACMA).

4. Identity Based Proxy-Signcryption Scheme from Pairings

In this section, we present an identity based proxy-signcryption scheme from pairings. This scheme is publicly verifiable. Other security properties are also discussed in the following section. Some initial settings of the scheme are assumed in identity based systems.

[**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 $\widehat{e}$: $G_1 \times G_1 \longrightarrow G_2$ and hash functions $H : \{0,1\}^* \longrightarrow Z_q, H_1 : \{0,1\}^* \longrightarrow G_1, H_2 : \{0,1\}^* \longrightarrow Z_q^*, H_3 : G_2 \longrightarrow \{0,1\}^n$. It chooses a 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, $\widehat{e}$, P, P_{pub}, H, H_1, H_2, H_3, E, $D\}$ and keeps the master-key *s* secret.

[**Extraction**]

Given an identity ID, the PKG computes

$$Q_{ID} = H_1(ID)$$

and the private key

$$d_{ID} = sQ_{ID}.$$

[**Generation of the Proxy Key**]

To delegate the signcrypting capacity to a proxy signcrypter, the original signcrypter Alice does the following to make the signed warrant m_w. There is an explicit description of the relative rights and information of the original signcrypter and proxy signcrypter in the warrant m_w such that a verifier can use it as a part of verification information. If the following process is finished successfully, the proxy signcrypter gets a proxy key d_{ap}.

–Alice chooses $x \longleftarrow_R Z_q^*$

computes $U = xP$

$$d_{ap} = H(m_w||U)d_{ID_A} + xP_{pub}$$

sends (m_w, U, d_{ap}) as the delegation to the proxy signcrypter securely. Actually, (m_w, U) can be delivered in a public channel, and only d_{ap} should be sent in a secure channel.

–The proxy signcrypter accepts d_{ap} as a valid proxy signcryption key only if the following equation is satisfied:

$$\widehat{e}(P, d_{ap}) = \widehat{e}(P_{pub}, Q_{ID_A})^{H(m_w||U)}\widehat{e}(U, P_{pub}).$$

This step is done only once between the original signcrypter and the proxy signcrypter. Thus the proxy signcrypter needs to compute three pairings only once. If it is finished successfully, the proxy signcrypter can signcrypt any message which conforms to the warrant on behalf of the original signcrypter.

[**Proxy Signcryption**]

To signcrypt a message $m \in \{0,1\}^*$, a proxy signcrypter chooses $x' \longleftarrow_R Z_q^*$

computes $Q_{ID_B} = H_1(ID_B)$

$$k_1 = \widehat{e}(P, P_{pub})^{x'}$$

$$k_2 = H_3(\widehat{e}(P_{pub}, Q_{ID_B})^{x'})$$

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

$$r = H_2(c, k_1)$$
$$S = x'P_{pub} - (rd_{ID_P} + d_{ap})$$

sends (m_w, U, c, r, S) to Bob.

[Unsigncryption]

When receiving (m_w, U, c, r, S), Bob performs the following tasks:

computes
$Q_{ID_A} = H_1(ID_A)$
$Q_{ID_P} = H_1(ID_P)$
$k'_1 = \widehat{e}(P, S)\widehat{e}(P_{pub}, Q_{ID_P})^r$
$\quad \cdot\widehat{e}(P_{pub}, Q_{ID_A})^{H(m_w||U)}\widehat{e}(U, P_{pub})$
$k'_2 = H_3(\widehat{e}(S, Q_{ID_B})\widehat{e}(Q_{ID_P}, d_{ID_B})^r$
$\quad \cdot\widehat{e}(Q_{ID_A}, d_{ID_B})^{H(m_w||U)}\widehat{e}(U, d_{ID_B}))$
$m = D_{k'_2}(c)$
if $r \neq H_2(c, k'_1)$ return $\perp$
accepts m.

Remarks:

1. Since the knowledge of the plaintext m is not required for the public verification of a message's origin, any third party can be convinced of the message's origin by recovering k'_1 as above and checking if the equality $r = H_2(c, k'_1)$ holds. Thus, this proxy signcryption scheme is public verifiable.

2. Notice that if we compute $r = H_2(m, k_1)$ instead of $r = H_2(c, k_1)$, then any adversary can verify the signature on two plaintexts m_0 and m_1 during the game IND-IDSC-CCA([8]), and find out which one matches to the challenge ciphertext, that is, replacing $r = H_2(c, k_1)$ by $r = H_2(m, k_1)$ would induce an obstacle to the sematic security.

3. Since the secret key d_{ID_P} of the proxy signcrypter is required in the proxy signcryption process of the scheme, only the proxy signcrypter can create a valid ciphertext of message m. Thus, this proxy signcryption scheme protects the proxy signcrypter.

4.This scheme does not only protect the proxy signcrypter but also guarantee the forward secrecy. Even if d_{ap} is revealed, a person without knowledge of d_{ID_P} can not compute k_2 since $k_2 = H_2(\widehat{e}(S, Q_{ID_B})\widehat{e}(d_{ID_P}, Q_{ID_B})^r\widehat{e}(d_{ap}, Q_{ID_B}))$. If both d_{ID_P} and d_{ap} are revealed, a third party can compute k_2=$H_2(\widehat{e}(S, Q_{ID_B})\widehat{e}\ (d_{ID_P}, Q_{ID_B})^r\widehat{e}(d_{ap}, Q_{ID_B}))$ without the knowledge of d_{ID_B}. But the case that both of them are disclosed is very rare.

5. Analysis of the Proxy-Signcryption Scheme

5.1. Correctness

The consistency of this scheme is easy to verify by the bilinearity of the map since

$k_1 = \widehat{e}(P, P_{pub})^{x'}$
$\quad = \widehat{e}(P, x'P_{pub})$
$\quad = \widehat{e}(P, S + rd_{ID_P} + d_{ap})$
$\quad = \widehat{e}(P, S)\widehat{e}(P, d_{ID_P})^r\widehat{e}(P, d_{ap})$
$\quad = \widehat{e}(P, S)\widehat{e}(P_{pub}, Q_{ID_P})^r$
$\qquad \cdot\widehat{e}(P, d_{ID_A})^{H(m_w||U)}\widehat{e}(P, xP_{pub})$
$\quad = \widehat{e}(P, S)\widehat{e}(P_{pub}, Q_{ID_P})^r$
$\qquad \cdot\widehat{e}(P_{pub}, Q_{ID_A})^{H(m_w||U)}\widehat{e}(U, P_{pub})$
$\quad = k'_1$

and

$k_2 = H_2(\widehat{e}(P_{pub}, Q_{ID_B})^{x'})$
$\quad = H_2(\widehat{e}(x'P_{pub}, Q_{ID_B}))$
$\quad = H_2(\widehat{e}(S + rd_{ID_P} + d_{ap}, Q_{ID_B}))$
$\quad = H_2(\widehat{e}(S, Q_{ID_B})\widehat{e}(d_{ID_P}, Q_{ID_B})^r\widehat{e}(d_{ap}, Q_{ID_B}))$
$\quad = H_2(\widehat{e}(S, Q_{ID_B})\widehat{e}(Q_{ID_P}, d_{ID_B})^r$
$\qquad \cdot\widehat{e}(d_{ID_A}, Q_{ID_B})^{H(m_w||U)}\widehat{e}(xP_{pub}, Q_{ID_B}))$
$\quad = H_2(\widehat{e}(S, Q_{ID_B})\widehat{e}(Q_{ID_P}, d_{ID_B})^r$
$\qquad \cdot\widehat{e}(Q_{ID_A}, d_{ID_B})^{H(m_w||U)}\widehat{e}(U, d_{ID_B}))$
$\quad = k'_2.$

5.2. Computation Costs

In the comparison of computation costs, we assume that computation of pairings is the most time consuming.

Under this assumption, checking for the number of computations, it can be observed that the pairing $\widehat{e}(P, P_{pub})$ can be pre-computed since it does not depend on users or messages. When users often have to communicate between each other, all those pairings $\widehat{e}(P_{pub}, Q_{ID_P}), \widehat{e}(P_{pub}, Q_{ID_A}), \widehat{e}(U, P_{pub}), \widehat{e}(Q_{ID_P}, d_{ID_B})$, $\widehat{e}(Q_{ID_A}, d_{ID_B})$, and $\widehat{e}(U, d_{ID_B})$ can be pre-computed too. In this case, the most expensive operations of the proxy signcryption algorithm are two exponentiations in G_2 and one computation of the type $aP + bQ \in G_1$. The unsigncryption operation only requires two pairing evaluations and two exponentiations in G_2(the other two exponentiations in G_2 can be pre-computed too).

Since the pairing evaluation is the most time consuming, the proposed proxy-signcryption scheme is as efficient as ordinary identity based identity based signcryption schemes([7]).

5.3. Security concerns

Similar to ([7]), it is straightforward to show that our scheme satisfies the semantic security notion IND-IDSC-CCA under the Decision Bilinear Diffie-Hellman (DBDHP) assumption.

The unforgeability against adaptive chosen messages attacks derives from the security of Hess's identity based signature scheme under the Computation Diffie-Hellman (CDHP) assumption([2]). Any attacker that is able to forge a signcrypted message for the proxy signcrypter and the original signcrypter must be able to forge a signature for the following scheme which is a variant of Hess's identity based signature scheme: Hess's scheme is proven to be secure against existential forgery on adaptive chosen message attacks under the random oracle assumption.

Setup and Extract are the same as above.
Sign: to sign a message *m*
choose $x \longleftarrow_R Z_q^*$
compute $U = xP$
$r = H(m, U)$
$V = xP_{pub} + rd_{ID_A}$
The signature on *m* is (*U*, *V*).
Verify: when receiving (*U*, *V*) and *m*, compute
$Q_{ID_A} = H_1(ID_A)$
$r' = H(m, U)$
if $\widehat{e}(P, V) \neq \widehat{e}(U, P_{pub})\widehat{e}(P_{pub}, Q_{ID_A})^{r'}$ return $\perp$
accept the signature (*U*, *V*).

6. Conclusions and Open Issues

The identity based public key setting can be an alternative for certificate-based public key setting. Signcryption is a novel paradigm in public key cryptography, in which message encryption and digital signature are simultaneously fulfilled in a logically single step. Proxy signature schemes are variations of ordinary digital signature schemes and have been shown to be useful in many applications. In this paper, We proposed an identity based proxy-signcryption scheme from pairings. Also we analyzed the proposed scheme from security and efficiency points of view. Heuristic arguments have been given for those security properties. We have shown that the proxy-signcryption scheme is as efficient as ordinary identity based signcryption schemes under certain circumstances.

Future research involves proposing more efficient schemes than the current one. More interesting aspect would be to find identity based proxy-signcryption schemes with both forward secrecy and public verifiability.

References

[1] F.Bao and R.H.Deng. A signcryption scheme with signature directly verifiable by public key. In *PKC*'98, pages 55-59. Springer-Verlag, LNCS 1431, 1998.

[2] F.Hess. Efficient identity based signature schemes based on pairings. *Proceedings of 9th workshop on selected areas in cryptography-SAC*2002. Lecture Notes in Computer Science. Springer-Verlag.

[3] F. Hess. Exponent group signature schems and efficient identity based signature schemes based on pairings. Cryptology ePrint Archive,Report 2002/012,2002.http://eprint.iacr.org/

[4] H.Y.Jung,D.H.Lee,et al. Signcryption schemes with forward secrecy. *WISA* 2001,vol.2, pages 403-475, 2001.

[5] S.Kim,S.Park,D.Won. Proxy signatures,revisited. *Proc.of ICICS*'97, *International Conference on Information and Communications Security*, LNCS 1334, pages 223-232, 1997.

[6] B.Lee,H.Kim,K.Kim. Strong proxy signature and its applications. *Proc.of SCIS*. pages 603-608, 2001.

[7] B.Libert,J-J.Quisquater. New identity based signcryption scheme from pairings. Full version available at http://eprint.iacr.org/2003/023/

[8] J.Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive,Report 2002/098,http:// eprint.iacr.org/

[9] M.Mambo,K.Usuda,E.okamoto. Proxy signature: delegation of the power to sign messages. I*EICE Trans.Fundamentals*. E79-A:9, pages 1338-1353, 1996.

[10] M.Mambo,K.Usuda,E.okamoto. Proxy signature for delegating signing opertion. *Proc. of 3rd ACM Conference on Computer and Communications Security, ACM Press New York*, pages 48-57, 1996.

[11] D.Nalla,K.C.Reddy. Signcryption scheme for identity based cryptosystems. Cryptology ePrint Archive,Report 2003/066,http://eprint.iacr.org/

[12] K.G. Paterson. ID-based signatures from pairings on elliptic curves. *Electronics Letters*. 38487, 1025-1020, January, 1999.

[13] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology- CRYPTO*'84, volume 196 of Lecture Notes in Computer Science, pages 47-53, Springer-Verjag, 1984.

[14] F.Zhang,K.Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings. *ACISP* 2003, LNCS 2727, pages 312-323, 2003.

[15] Y.Zheng. Digital signcryption or how to achieve cost(signature & encryption)<< cost(signature) + cost(encryption). In *Advances in Cryptology- CRYPTO*'97, volume 1294 of Lecture Notes in Computer Science, pages 165-179,Springer-Verlag, 1997.