

An ID-based Anonymous Proxy Signature From Bilinear Pairings

Zemao Zhao¹, Xianghong Tang¹, Bin Li², Longhai Zhu³

1. School of Communication Engineering, Hangzhou Dianzi Univ. , Hangzhou China; 2. College of Computer & Info. Engineering, Hohai Univ., Nanjing China; 3. Info. Security Center, Beijing Univ. of Posts & Tele., Beijing, China.

Abstract: A new ID-based anonymous proxy signature scheme from bilinear pairings was proposed in this paper. Anonymous proxy signature is suitable for the situation that the proxy signer's identity needs to be kept secret. The verifier needs to reveal the real identity of the proxy signer with the help of the original signer. The signature is based on Gap Diffie-Hellman group problems and meets the security requirements such as verifiability, unforgeability, undeniability, anonymity and traceability.

Key words: proxy signature, ID-based, anonymous proxy, bilinear pairings

1 Introduction

The concept of proxy signature was first introduced by Mambo, et al. in 1996. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message on behalf of the original signer. If an original signer wants to delegate the signing capability to a proxy signer, he uses the original signature key to create a proxy signature key, which will then be sent to the proxy signer. The proxy signer can use the proxy signature key to sign messages on behalf of the original signer. Proxy signature can be verified using a modified verification equation such that the verifier can be convinced that the signature is generated by the authorized proxy entity of the original signer. After Mambo et al's first scheme was announced, many proxy signature schemes have been proposed such as [1-2]. An anonymous proxy signature is applied in such a special situation, for example, an important document which is related about someone's promote needs to be kept, the proxy signers hope to keep secret of his identity, when disputation is appearing, the verifier can reveal the real identity of the proxy signer with the help of the original signer.

Generally, a good anonymous proxy signature has the properties as the followings:

- (1)Verifiability: The verifier can be convinced of the original signer's agreement on the signed message.
- (2)Unforgeability: A designated proxy signer can create a valid proxy signature. But the original signer and other third parties cannot create a valid proxy signature.
- (3)Undeniability: Once a proxy signer creates a valid proxy signature, he cannot repudiate his signature.
- (4)Anonymity: In the Verification Phase, the identity of the proxy signer is blind to the verifier.
- (5)Traceability: In appearing of disputation, the verifier can reveal the real identity of the proxy signer with the help of the original signer.

Shum and Wei Victor[3] proposed a strong proxy signature scheme with proxy signer privacy protection, but it needs a trusted party. Gu et al.[4,5] proposed an anonymous proxy signature scheme without a trusted party in 2005, but it is based on the discrete logarithm problem.

Identity-based public key cryptosystem(simply IDPKC) can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. In IDPKC, everyone's public keys

are predetermined by information that uniquely identifies them, such as name, email address, etc, rather than an arbitrary string. Other papers referred to [6-7].

We proposed an efficient ID-based anonymous proxy signature scheme from bilinear pairings, then analyze the correctness and the security of the proposed scheme.

2 Basic concepts on bilinear pairings

In this section, we will briefly describe the basic concept and properties of bilinear pairings and gap Diffie-Hellman group. We also present the ID-based public key setting based on pairing.

2.1 Bilinear pairings

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 is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:

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

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

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

2.2 Gap Diffie-Hellman group

Now we describe some mathematical problems in G_1 .

–Discrete Logarithm Problem (DLP): Given two group elements P and Q , to find an integer $n \in \mathbb{Z}_q^*$, such that $Q = nP$ whenever such an integer exists.

–Computational Diffie-Hellman Problem (CDHP): Given $P, aP, bP \in G_1$ for $a, b \in \mathbb{Z}_q^*$, to compute abP .

–Decision Diffie-Hellman Problem (DDHP): Given $P, aP, bP, cP \in G_1$ for $a, b, c \in \mathbb{Z}_q^*$, to decide whether $c = ab \bmod q$.

–Gap Diffie-Hellman Problem (GDHP): DDHP is easy, but CDHP is difficult on the group G_1 , which is called a Gap Diffie-Hellman Group, refer to [6, 10] for more details.

Meanwhile, there exists a difficult problem to solve the inverse algorithm of bilinear pairings, i.e., given $P \in G_1$, $r \in G_2$, to find an element $Q \in G_1$, such that $r = e(P, Q)$ whenever such an element exists.

2.3 ID-based public key setting

In IDPKC, user's private key of the user is calculated by a trusted party, called PKG and send to the user via a secure channel. ID-based public key setting involves a PKG and users. The basic operation consists of Setup and Private Key Extraction (simply Extract). When we use bilinear pairings to construct IDPKC, Setup and Extract can be implemented as follows:

Let H_1 and H_2 are two cryptographic hash functions as $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_2: \{0,1\}^* \rightarrow G_1$.

–Setup: PKG chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. The center publishes system parameters

$params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s as the master key, which is known only by him.

–Extract: Original signer A submits his identity information ID_A to PKG. PKG computes the signer's public key as $Q_{ID_A} = H_2(ID_A)$, and returns $S_{ID_A} = sQ_{ID_A}$ to A as his private key and sends it via a secure channel. Same to proxy signer, proxy signer's public and private key is (Q_{ID_B}, S_{ID_B}) .

3 An ID-based anonymous proxy signature

In this section, we present an ID-based anonymous proxy signature scheme from bilinear pairings. Suppose the original signer is A, the proxy signer is B, the verifier is C. Our scheme consists of five phases. The Setup and Extract are same like in Section 2.3, and other phases are as below.

[Generation of proxy key]

To delegate the signing capacity to proxy singer, the original signer A do the following operations:

Step1: The original signer A randomly chooses $k_A \in Z_q^*$, computes $r_A = e(P, P_{pub})^{k_A}$, $c_A = H_1(m_w \| r_A)$,

$U_A = c_A S_{ID_A} + k_A P_{pub}$, and $U_P = c_A (Q_{ID_A} + Q_{ID_B}) + k_A P$, where m_w denotes the delegation description

include limit of usages and efficient time, and makes U_P public in the system as public key of proxy signature.

Step2: A sends (m_w, c_A, U_A) to proxy signer B in a secure way.

Step3: After receiving (m_w, c_A, U_A) , the proxy signer B first computes $r_A = e(U_A, P)e(Q_{ID_A}, P_{pub})^{-c_A}$, accepts it if and only if $c_A = H_1(m_w \| r_A)$. If it is right, he accepts it as a valid proxy, and uses the privilege of signature on behalf of A, then computes $s_P = c_A S_{ID_B} + U_A$ and takes s_P as a private key of proxy signature, and stores (U_P, ID_B) in the database. Otherwise he rejects it.

[Signature phase]

Proxy signer B randomly chooses $k_B \in Z_q^*$, $k_B \neq 1$, and computes $r_B = e(P, P_{pub})^{k_B}$, $c_B = H_1(m \| r_B)$,

$U_B = c_B s_P + k_B P_{pub}$, hence the final proxy signature is (m, c_B, U_B, U_P, m_w) .

[Verification Phase]

After receiving the proxy blind signature (m, c_B, U_B, U_P, m_w) , the verifier V computes

$\tilde{r}_B = e(U_B, P)e(U_P, P_{pub})^{-c_B}$, then computes $\tilde{c}_B = H_1(m \| \tilde{r}_B)$, the signature holds true if and only if $c_B = \tilde{c}_B$.

4 Analysis of the Proposed Scheme

4.1 Correctness

The verification of the signature is justified by the following equations:

$$\begin{aligned} \tilde{r}_B &= e(U_B, P)e(U_P, P_{pub})^{-c_B} = e(c_B s_P + k_B P_{pub}, P)e(U_P, P_{pub})^{-c_B} = e(c_B s U_P + k_B P_{pub}, P)e(U_P, P_{pub})^{-c_B} \\ &= e(c_B U_P, P_{pub})e(k_B P_{pub}, P)e(U_P, P_{pub})^{-c_B} = e(P, P_{pub})^{k_B} = r_B. \text{ So, we have } \tilde{c}_B = H_1(m \| \tilde{r}_B) = H_1(m \| r_B) = c_B. \end{aligned}$$

4.2 Security Analysis

(1)Verifiability. From the signature (m, c_B, U_B, U_P, m_w) , the verifier can calculate the verification equation, if it is right, he can be convinced that the proxy signer has the original signer's signature on the warrant m_w . In general the warrant contains the identity information and the limit of the delegated signing capacity and so satisfies the verifiability.

(2)Unforgeability. Unforgeability means that any illegal entity cannot create a valid signature. Any an adversary who wants to forge the proxy signature of the message m must have the original signer's signature on a warrant m_w , but cannot forge this signature, since the original signer uses his private key to sign based on Schnorr's signature scheme. On the other hand, the original signer cannot create a valid proxy signature. Since the proxy signature scheme is obtained by using Schnorr's signature scheme and the proxy key includes the private key of the proxy signer.

(3)Undeniability. Since the proxy signer uses his private key to sign on message m , and the valid proxy signature contains the warrant m_w , which must be verified in the verification phase, it cannot be modified by the proxy signer. Thus once a proxy signer creates a valid proxy signature of an original signer, he cannot repudiate the signature creation.

(4)Anonymity. From the verification of the signature, any one cannot judge the information about the signer. So it satisfies anonymity requirement.

(5)Traceability. When the verifier proposes the disputation for the signature, since the original signer stores the proxy signer's the proxy signature public key and identity, so he can reveal the real identity of the proxy signer with the help of the original signer.

5 Conclusions

Proxy signature have plenty of applications, however, most of the previous schemes are under the traditional CA-based public infrastructure. In this paper, we proposed an anonymous proxy signature scheme from bilinear pairings, which is under the ID-based public key cryptosystem. The proposed signature scheme is suitable for the situation that the proxy signer's identity needs to be secret. Finally, we analyze the security. The proposed scheme satisfies the required secure properties of anonymous proxy signature: verifiability, unforgeability, undeniability, anonymity and traceability.

References

- [1] S. Kim, S. Park, and D. Won, Proxy signatures, revisited, In Pro. of ICICS 97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.
- [2] B. Lee, H. Kim and K. Kim, Secure mobile agent using strong non-designated proxy signature, Proc. of ACISP2001, LNCS 2119, pp.474-486, Springer Verlag, 2001.
- [3] Shum K, Wei Victor K. A strong proxy signature scheme with proxy signer privacy protection [EB/OL].<http://www.computer.org/proceedings/wetice/1748/17480055.pdf>,2002.
- [4] Gu Li-ze, Li Zhong-xian and Yang Yi-xian. A Anonymous Proxy Signature Scheme without a Trusted Party[J]. Journal of Beijing university of posts and telecommunications,2005,28(1):48-50(In Chinese).
- [5] Gu Li-ze, Zhang Sheng and Yang Yi-xian. A new proxy signature scheme[J]. Journal of Electronics & Information Technology,2005,27(9):1463-1466(In Chinese).
- [6] J.C. Cha and J.H. Cheon, An identity-based signature from gap Diffie-Hellman groups, Public Key Cryptography - PKC 2003, LNCS 2139, pp.18-30, Springer-Verlag, 2003.
- [7] F. Zhang and K. Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings [A]. In: Advances in Cryptology-Crypto' 2003[C], LNCS2727,pp.312~323, Springer-Verlag, 2003.