A New ID-Based Proxy Blind Signature Scheme

LANG Wei-min1,2, YANG Zong-kai†, CHENG Wen-qing1, TAN Yun-meng†
1. Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China;
2. People’s Liberation Army Institute of Communications Command, Wuhan 430010, Hubei, China

Abstract. An identity-based proxy blind signature scheme from bilinear pairings is introduced, which combines the advantages of proxy signature and blind signature. Furthermore, our scheme can prevent the original signer from generating the proxy blind signature, thus the profits of the proxy signer are guaranteed. We introduce bilinear pairings to minimize computational overhead and to improve the related performance of our scheme. In addition, the proxy blind signature presented is non-repudiable and it fulfills perfectly the security requirements of a proxy blind signature.

Key words: digital signature; proxy signature; blind signature; identity-based cryptography; bilinear pairings

CLC number: TP 309.2

Introduction

In modern society, people always need to consign the signing capability to a trusted proxy who can sign on a message instead of the original signer. The concept of proxy signature was first introduced by Mambo [1,2] in 1996, where the proxy signer can create a valid signature for a message on behalf of the original signer. Although many schemes [3-4] have been proposed, they can not provide true non-repudiation [5-6] that may result in the abuse of signature. Proxy signatures can be combined with other signatures.

The concept of blind signature was firstly introduced by Chaum [7], which plays the central role in cryptographic protocols to provide the anonymity of users in E-cash or E-voting system. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. Such signatures allow user to obtain the signature of a message in a way that the signer learns neither the message nor the resulting signature. Blind signature schemes have been shown to be useful in various applications, such as electronic polling and electronic payment [8, 9].

Recently, the bilinear pairings [10] have been found various applications in cryptography, because they can be used to realize some cryptographic primitives that were previously unknown or impractical. More precisely, they are basic tools for construction of identity-based cryptographic schemes. In 1984, Shamir [11] proposed an identity-based encryption and signature scheme to simplify key management procedures in certificate-based public key setting. Since then, many identity-based encryption schemes [12-13] and signature schemes [14-15] have been put forward. In identity-based public key cryptosystem, everyone’s public keys are predetermined by information
that identifies them, such as name, social security number, email address, rather than an arbitrary string.

In this paper, we propose an identity-based proxy blind signature scheme from bilinear pairings, which combines the advantages of proxy signature and blind signature. In this scheme, each entity consigns his signing power to only one proxy who can use the proxy signature key to sign messages on behalf of the original signer. Our scheme can prevent the original signer form generating the proxy blind signature, so it protects the profits of the proxy signer. We introduce bilinear pairings to minimize computational overhead and to improve the related performance of our scheme. In addition, the proxy blind signature presented in this paper is non-repudiable and it fulfills perfectly the security requirements of a proxy blind signature.

1 Bilinear Pairings

Let $G_1$ be an additive group generated by $P$, whose order is a prime $q$, and $G_2$ be a multiplicative group of the same order $q$. $Y$ denotes an initial system parameter set. $Z_q^*$ denotes a positive integer group whose element is less than $q$, that is to say, $Z_q^* = \{1, 2, \ldots, q-1\}$, $x \in \mathbb{Z}/M$ means that $x$ is selected randomly in $M$, where $M$ is a random group.

Definition 1 A bilinear pairing is a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) Bilinear: For all $P, Q, R \in G_1$ and $a, b \in Z_q^*$, such that
   
   $\hat{e}(P, Q + R) = \hat{e}(P, Q) \hat{e}(P, R)$
   $\hat{e}(P + Q, R) = \hat{e}(P, R) \hat{e}(Q, R)$
   $\hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, abQ) = \hat{e}(P, Q)^{ab}$

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

3) Computable: Given $P, Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P, Q)$.

Now we describe some mathematical problems in relation to bilinear pairings.

1) Discrete logarithm problem (DLP): Given two group elements $P$ and $Q$, finding an integer $n$, such that $Q = nP$ whenever such an integer exists.

2) Decision Diffie-Hellman problem (DDHP): For $a, b, c \in Z_q^*$, $P \in G_1$, given $P, aP, bP, cP$, decide whether $c = ab$.

3) Computational Diffie-Hellman problem (CDHP): For $a, b \in Z_q^*$, $P \in G_1$, given $P, aP, bP$, compute $abP$.

4) Gap Diffie-Hellman problem (GDHP): On the group $G_1$, DDHP is easy, but CDHP is hard. Now we call $G_1$ a gap Diffie-Hellman (GDH) group.

We assume through this paper that CDHP and DLP are intractable in $G_1$ and $G_2$. GDH groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field and bilinear pairings can be derived from the Weil or Tate pairing. Our scheme is based on GDH group.

2 Proxy Blind Signature

A proxy blind signature scheme consists of four entities: key generation center (KGC), original signer, proxy signer and receiver.

Definition 2 A proxy blind signature scheme is a digital signature scheme comprising the following five procedures:

1) Setup: On input a security parameter, KGC creates and publishes system parameters and keeps a master key only known by KGC.

2) Extract: The original signer and the proxy submit their identity information ID to KGC. KGC computes and returns a public/private key pair for them respectively.

3) Generation of the proxy key: The original signer creates a proxy signature key with the original signature key and returns it to the proxy.

4) Signing: A probabilistic polynomial time (PPT) algorithm takes $Y$, a proxy key and a message $m$. The algorithm outputs a signature $\sigma(m)$ for the message.

5) Verification: A probabilistic polynomial time algorithm takes $Y$, a signature $\sigma(m)$ and the identity information of the proxy signer. The algorithm outputs either accept or reject.

A strong proxy blind signature scheme should provide:

1) Verifiability: From the proxy blind signature, the verifier can be convinced of the original signer’s agreement on the signed message.

2) Non-forgeability: A designated proxy signer can create a valid proxy blind signature for the original signer. But the original signer and other third parties who are not authorized as a proxy signer can not create it.

3) Non-deniability: Once a proxy signer creates a valid proxy blind signature on behalf of an original signer, the proxy can not repudiate the signature creation.