# An Identity-Based Mediated Signature Scheme Without Trusted PKG

Xiaofeng Wang and Shangping Wang
School of Science, Xi'an university of technology, Xi'an 710048, P.R.China
E-mail: xfwang66@sina.com.cn

**Keywords:** ID-based signature, ID-based mediated signature, without trusted PKG, immediate revocation, GDH group

**Received:** July 14, 2008

*Mediated Signature Scheme provides an efficient method for fast revocation of a user's identity in identity (ID)-based cryptosystems. The only ID-based mediated signature scheme was proposed by Cheng et al. from bilinear pairing in [8]. Unfortunately, their scheme has an inherent flaw that the PKG is fully capable to generate a valid mediated signature of some message on behalf of its signers by only utilizing the public information of the system. In this paper, an efficient ID-based mediated signature scheme without trusted PKG is proposed. Compared with the scheme [8], the proposed scheme has other property besides achieving immediate revocation of a signer's ID. That is, proposed scheme is ID-based, but without any assumption of pre-fixed trusted relationship between users and PKG, which effectively solves the problem that exists in some existing ID-based public key cryptosystems in which a trusted PKG and key escrow are needed.*

*Povzetek: Predstavljena je metoda elektronskega podpisovanja.*

## 1 Introduction

The ID-based public key cryptosystems allow public keys of a user to be computed easily and publicly from a string to correspond with his (her) identity (such as name, telephone number, email address or an IP address). This characteristic avoids the necessity of using certificates and PKI system. Compared with certificate-based cryptosystems, ID-based cryptosystems have simplified key management since there is no need to maintain a great database containing a list of public keys and their respective owners. Therefore, ID-based public key cryptosystems have a wide application foreground in information security field. However, two inherent limitations of ID-based cryptosystems have hindered its development in implementing.

The first limitation is the necessity of a trusted party, referred to as Private Key Generator (PKG) and key escrow. In ID-based cryptosystems, a user's identity (ID) is used as his/her public key, for this work, users cannot generate their own key-pairs. As alternative, this is done by a PKG. The PKG uses a master key to generate private keys for users. Usually, PKG is supposed to be trusty. However, there is not a fully trusted PKG in practice. Since PKG knows private key of each user, a dishonest PKG can impersonate any user and forge their signatures. Recent research shows that this problem can be mitigated by splitting PKG's master key between a numbers of PKGs[1], but this adds extra complexity to key generation.

The second limitation is that current ID-based cryptosystems cannot provide an efficient solution to immediately revoke a user's identity. The typical way of revoking a user's identity is to concatenate a valid period to the identity string. Revocation is achieved by instructing PKG to stop issuing new private keys for revoked identities. This involves the need to periodically re-issue all private keys in the system, and the PKG must be online most of the time, otherwise, the user's identity cannot be immediately revoked using this method.

Boneh et al. introduced a method for obtaining fast revocation of a user's public key privilege in RSA-based cryptosystems. They call it mediated RSA (mRSA)[2]. The main idea behind mRSA is to introduce a special online entity in standard RSA, called Security Mediator (SEM). To sign or decrypt a message, user must first obtain a message-specific token from the SEM, and he(she) cannot use his (her) private key without this token. To revoke user's ability to sign or decrypt, the administrator instructs the SEM to stop issuing tokens for user's public key. Mediated RSA (mRSA) is a simple and practical method of splitting RSA private keys between the user and the SEM. Neither the user nor the SEM can cheat one another since each signature or decryption must involve both parties. mRSA allows fast revocation of user's security privileges. However, mRSA still relies on public key certificates to derive public keys. Boneh et al.[3] and Ding et al.[4] proposed Identity-based mRSA schemes, respectively. The basic idea behind identity-based mRSA is the use of a single common RSA modulus $n$ among all users of a system. This modulus is assumed to be public and contained in a public key certificate, and the certificate is issued, as usual, by a Certificate Authority (CA). This method cannot essentially avoid the necessity of using certificates and CA.

Boneh et al. first gave a practical ID-based encryption scheme from Weil pairing [5] in 2001. Based on this scheme, Libert et al. [6], Baek et al. [7] proposed an ID-based mediated encryption scheme, respectively, using the

similar method given in mRSA. Both schemes provide efficient methods to immediately revoke a user's identity.

Very recently, Cheng et al. proposed an ID-based mediated signature scheme [8]. Their scheme avoids the using of certificates and CA. The main idea behind it is to introduce a SEM, in a general ID-based signature scheme. A signer's private key is split into two parts. One part is hold by himself(herself), and another is given to the SEM. Therefore, only with the help of the SEM, can a signer generate a valid signature. As a result, an immediate revocation of a signer's ID (i.e. a signer's signing privilege) is possible by instructing the SEM not to help the revoked user anymore. Unfortunately, their scheme has an inherent flaw, it is that the PKG is fully capable to generate a valid mediated signature of some message on behalf of its signers by only utilizing the public information of the signers and the SEM.

In this paper, we propose an ID-based mediated signature scheme from bilinear pairing. Proposed scheme has other properties besides achieving immediate revocation of signer's ID. First, our scheme is ID-based, but without any assumption of pre-fixed trusted relationship between users and PKG, it solves the problem that exists in some existing ID-based public key cryptosystems, in which a trusted PKG and key escrow are needed, in certain extent. Second, our scheme is able to prevent the dishonest PKG from impersonating the signer to generate a valid mediated signature. To construct such a scheme, we first improve Cheng's ID-based signature scheme [8], to make it has the property that the PKG is unable to generate a valid signature on behalf of any signers even if it knows the private keys of the signers, then used it to construct an efficient ID-based mediated signature scheme without trusted PKG.

The remaining sections are organized as follows. In Section 2 we briefly introduce some related mathematical knowledge. In Section 3 we recall the Cheng's ID-based mediated signature scheme. In Section 4 we propose an ID-based signature scheme, based on this scheme, we propose a new ID-based mediated signature scheme without trusted PKG and analysis its security in Section 5, then we conclude this paper in Section 6.

# 2 Preliminaries

## 2.1 Bilinear pairings

Let $q$ be a prime with $l$ bits length. Let $G_1$ be an additive cyclic group generated by $P$, whose order is $q$. Let $G_2$ be a multiplicative cyclic group of the same order $q$. A bilinear pairing is a map $\hat{e}: G_1 \times G_1 \to G_2$ satisfies the following properties:

(1) Bilinear: For any $aP, bP \in G_1$, $\hat{e}(aP, bP) = \hat{e}(P,P)^{ab}$, where $a, b \in Z_q^*$;

(2) Non-degenerate: There exists $P$,$Q \in G_1$ such that $\hat{e}(P,Q) \neq 1_{G_2}$;

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

## 2.2 Gap Diffie-Hellman (GDH) group

We consider the following problems in $G_1$.

(1) Discrete logarithm problem (DLP): Given $Q \in G_1$, to find an integer $x \in Z_q^*$, such that $Q = xP$ (Assuming such an integer exists.).

(2) Computational Diffie-Hellman problem (CDHP): Given $aP, bP \in G_1$, to compute $abP$.

(3) Decisional Diffie-Hellman problem (DDHP): Given $P, aP, bP, cP \in G_1$, to decide whether $c = ab \bmod q$, if so, $(P, aP, bP, cP)$ is called a valid Diffie-Hellman quaternion.

**Definition 2.1** We call $G_1$ a gap Diffie-Hellman (GDH) group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP on $G_1$ with non-negligible probability.

Such a group can be found in super-singular elliptic curve or hyper-elliptic curve over finite fields. For more details, see [9,10,11,12,13,14]. An efficient method to solve DDHP is introduced in [15]: assuming there is a bilinear map $\hat{e}$, then $(P, aP, bP, cP)$ is a valid Diffie-Hellman quaternion $\Leftrightarrow \quad \hat{e}(aP, bP) = \hat{e}(P, cP)$.

Schemes in this paper can work on any GDH group. Throughout this paper, we define the system parameters in all schemes as follows: $G_1$, $G_2$, $P$, $q$ and $\hat{e}$ are as described above. These system parameters can be obtained using a GDH Parameters Generator [5,15]. Define two cryptographic hash functions: $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to Z_q^*$.

# 3 Cheng's ID-based mediated signature scheme and its security analysis

## 3.1 The scheme

Cheng's ID-based mediated signature scheme (for short CMSS) consists of three entities: PKG, SEM and signers. There are four algorithms: Setup, MeExtract, MeSign and Verify. They are described as follows:

(1) Setup: Sharing the same system parameters with above. PKG picks $s \in Z_q^*$ at randomly as a master key and computes the system public key $P_{pub} = sP$. $P_{pub}$ is published but $s$ is kept secretly.

(2) MeExtract: Given an identity $ID$, PKG chooses $s_{ID} \in Z_q^*$ at randomly, computes:

$$\begin{aligned} Q_{ID} &= H_1(ID) \\ D_{ID}^{user} &= s_{ID} \cdot Q_{ID} \\ D_{ID}^{SEM} &= (s - s_{ID}) \cdot Q_{ID} \end{aligned}$$

$D_{ID}^{user}$ is sent secretly to the signer whose identity is $ID$, as the private key of the signer, and $(D_{ID}^{SEM}, ID)$ is sent secretly to the SEM.

(3) MeSign: To sign a message $M$, the signer interacts with the SEM as follows:

The signer chooses $\tilde{r}_1 \in Z_q^*$ at randomly, and computes: $\tilde{R}_1 = \tilde{r}_1 P$. The triple $(M, \tilde{R}_1, ID)$ is sent to the SEM.

After having received $(M, \tilde{R}_1, ID)$, the SEM first checks the $ID$ of the signer is not revoked. It then picks $\tilde{r}_2 \in Z_q^*$ at randomly, and computes:

$$\begin{aligned} \tilde{R}_2 &= \tilde{r}_2 P \\ \tilde{R} &= \tilde{R}_1 + \tilde{R}_2 \\ \tilde{h} &= H_2(M, \tilde{R}) \\ \tilde{S}_{SEM} &= \tilde{r}_2 P_{pub} + \tilde{h} D_{ID}^{SEM} \end{aligned}$$

Then $(\tilde{R}, \tilde{S}_{SEM})$ is sent back to the signer.

After having received $(\tilde{R}, \tilde{S}_{SEM})$, the signer computes:

$$\begin{aligned} \tilde{h} &= H_2(M, \tilde{R}) \\ \tilde{S}_{user} &= \tilde{r}_1 P_{pub} + \tilde{h} D_{ID}^{user} \\ \tilde{S} &= \tilde{S}_{user} + \tilde{S}_{SEM} \end{aligned}$$

He verifies whether $\hat{e}(P, \tilde{S}) = \hat{e}(P_{pub}, \tilde{R} + \tilde{h} Q_{ID})$ holds. If so, the signature on message $M$ under $ID$ is set to be $\tilde{\sigma} = (\tilde{R}, \tilde{S})$.

(4) Verification: Given a signature $\tilde{\sigma} = (\tilde{R}, \tilde{S})$ on message $M$ under $ID$, the verifier computes:

$$\begin{aligned} \tilde{h} &= H_2(M, \tilde{R}) \\ Q_{ID} &= H_1(ID) \end{aligned}$$

He accepts the signature if $\hat{e}(P, \tilde{S}) = \hat{e}(P_{pub}, \tilde{R} + \tilde{h} Q_{ID})$.

### 3.2 Security analysis

The signature on message $M$ under $ID$ is:

$$\begin{aligned} \tilde{S} &= \tilde{S}_{user} + \tilde{S}_{SEM} \\ &= \tilde{r}_1 P_{pub} + \tilde{h} D_{ID}^{user} + \tilde{r}_2 P_{pub} + \tilde{h} D_{ID}^{SEM} \\ &= s(\tilde{R}_1 + \tilde{R}_2) + \tilde{h} s Q_{ID} \\ &= s\tilde{R} + \tilde{h} s Q_{ID} \end{aligned}$$

It is obvious that not only can the dishonest PKG generate every user's private key and impersonate any user to forge their signatures, but also generate a valid mediated signature on message $M$ under $ID$ by only utilizing the public information $(M, \tilde{R}, ID)$.

## 4 Improved ID-based signature scheme and its security

### 4.1 Improved ID-based signature scheme

Our ID-based signature scheme is based on GDH groups. It is a variant of the ID-based signature scheme given by Yi [16]. Similar variants can be seen in [8,23,24]. The security analysis of the scheme can be found in [17]. In some ID-based signature scheme such as [12,16,18], the PKG can directly forge signature by using of the signature's public information. Our construction avoids this flaw. Our ID-based signature scheme consists of four algorithms: Setup, Extract, Signing and Verification, which is described as follows.

(1) Setup: Given a security parameter $l$, PKG runs the GDH Parameters Generator to obtain Params = $\{G_1, G_2, P, q, \hat{e}, H_1, H_2\}$. Then it picks a random number $s \in Z_q^*$ as a master key and computes the system public key $P_{pub} = sP$. $P_{pub}$ is published but $s$ is kept secretly.

(2) Extract: It is a key extraction algorithm engaged by PKG and a user. A user submits and authenticates his/her identity $ID \in \{0,1\}^*$ to PKG, PKG inputs system parameters, master key and the user's identity $ID$; and outputs the user's public key and private key.

The signer randomly chooses an integer $r_u \in Z_q^*$, sets $R_u = r_u P$, submits $(ID, R_u)$ to PKG, and authenticates his(her) identity to PKG by out-band mechanism. PKG generates signer's public key and private key: $Q_u = H_1(ID, R_u)$, $D_u = sQ_u$, and sends $D_u$ to the signer via a secure channel.

(3) Signing: Given a message $M$, the signer picks a random number $r_v \in Z_q^*$ such that $r_v r_u \bmod q \neq 1$, and computes:

$$\begin{aligned} R_v &= r_v P \\ h &= H_2(M, ID, R_u, R_v) \\ X &= r_u r_v P + h D_u \end{aligned}$$

The signature on message $M$ is set to be $\delta = (X, R_u, R_v)$.

(4) Verification: Given a signature $\delta = (X, R_u, R_v)$ on message $M$ under $ID$, the verifier computes:

$$\begin{aligned} h &= H_2(M, ID, R_u, R_v) \\ Q_u &= H_1(ID, R_u) \end{aligned}$$

He accepts the signature if $\hat{e}(X, P) = \hat{e}(R_u, R_v)\hat{e}(hQ_u, P_{pub})$.

### 4.2 Security analysis

**Theorem 4.1** The improved ID-based signature scheme is secure against existential forgery under adaptively chosen message and ID attack in the random oracle model.

Analysis: Generally, an ID-based signature scheme involving two security models[10]. The first is adaptively chosen message and ID attack, the second is adaptively chosen message and given ID attack. The latter is in fact the security notion of a general signature scheme. Using the same methodology as Lemma 1 in [10], we can prove that, if there exists a forger $\mathscr{A}$ who performs an existential forgery under an adaptively chosen message and ID attack against our scheme, then, making use of $\mathscr{A}$, we can construct an algorithm $\mathscr{B}$, with the same advantage as $\mathscr{A}$, against our scheme under adaptively chosen message and given ID attack.

Following certification process shows, if there exists a adversary $\mathscr{B}$ which performs an existential forgery against our scheme under adaptively chosen message and given ID

attack, then we can construct an algorithm $\mathscr{F}$ that solves the CDHP by running the adversary $\mathscr{B}$ as a subroutine.

Proof: We cannot directly reduce the security of our ID-based signature scheme to the hardness of the CDHP because our scheme contains a random value in its signature [13]. We reduce the security of our ID-based signature scheme to the hardness of the CDHP by making use of the oracle replay technology and the forking lemma [20,21].

Given an identity $ID$, the corresponding public/private key pair is $(Q_u, D_u)$. If there exists an efficient algorithm $\mathscr{B}$ against our scheme under adaptively chosen message and given ID attack, then an algorithm $\mathscr{F}$ can be constructed as follows: inputs $P$, $P_{pub} = sP$ and $Q_u = tP$ for some $t \in Z_q^*$, if $\mathscr{B}$ chooses a message $M$, uses the oracle replay method and the forking lemma [20,21], $\mathscr{F}$ can obtain two valid signatures $(M, R_u, R_v, h_1, X_1)$ and $(M, R_u, R_v, h_2, X_2)$ such that $h_1 \neq h_2$, and satisfying equations $\hat{e}(X_1, P) = \hat{e}(R_u, R_v)\hat{e}(h_1 Q_u, P_{pub})$ and $\hat{e}(X_2, P) = \hat{e}(R_u, R_v)\hat{e}(h_2 Q_u, P_{pub})$. That is, $\hat{e}(X_1 - X_2, P) = \hat{e}((h_1 - h_2)D_u, P)$. We have $\hat{e}((X_1 - X_2) - (h_1 - h_2)D_u, P) = 1_{G_2}$. Since $\hat{e}$ has the property of non-degeneracy, we have $(X_1 - X_2) - (h_1 - h_2)D_u = O$ (here $O$ is an ideally defined point, namely the point at infinity, and is also recognized as a point on elliptic curve.), and $D_u = (h_1 - h_2)^{-1}(X_1 - X_2)$ (see [8]). It means that $\mathscr{F}$ can solve an instance of CDHP in $G_1$ since $D_u = sQ_u = stP = (h_1 - h_2)^{-1}(X_1 - X_2)$.

# 5 Proposed scheme and its security analysis

The idea behind ID-based mediated signature is to introduce a trusted online party SEM in a general ID-based signature scheme. A private key of the signer is split into two parts. One part is given to the signer, and another is given to the SEM. Therefore, only with the help of the SEM, can a signer generate a valid mediated signature. As a result, an immediate revocation of a signer's signing privilege is possible by instructing the SEM not to help the revoked user anymore.

## 5.1 Our scheme

Now we give the mediated version of the improved ID-based signature scheme in Section 4.1, and show how can avoid forging signature by dishonesty PKG in our scheme. Our scheme consists of three entities: PKG, SEM and signer, and four algorithms: Setup, MeExtract, MeSign and Verification, they are described as follows:

(1) Setup: Given a security parameter $l$, PKG runs the GDH Parameters Generator to obtain Params= $\{G_1, G_2, P, q, \hat{e}, H_1, H_2\}$. PKG picks two different random numbers $s_1 \in Z_q^*$ and $s_2 \in Z_q^*$, lets $s = s_1 + s_2$ as the master key, and generates system public key $P_{pub} = sP$. $P_{pub}$ is published but $s_1, s_2$ are kept secretly.

(2) MeExtract: the signer randomly chooses an integer $r_s \in Z_q^*$, sets $R_s = r_s P$, submits ($ID$,$R_s$) to PKG and authenticates his/her identity $ID$ to PKG by out-band mechanism. PKG generates the public key and private key of the signer: $Q_s = H_1(ID, R_s)$, $D_s = s_1 Q_s$. PKG generates the private key of the SEM: $D_{SEM} = s_2 Q_s$. Then sent $D_s$ to the signer, sent $(D_{SEM}, ID)$ to the SEM, respectively, over a confidential and authentic channel.

(3) MeSign: To sign a message $M$, the signer must present a service requisition to SEM. He interacts with the SEM as follows:

The signer chooses a random number $r_1 \in Z_q^*$ such that $r_1 r_s \bmod q \neq 1$ and $r_1^2 \bmod q \neq 1$, computes:

$$\begin{aligned} R_1 &= r_1 P \\ Z_s &= r_s r_1 P + H_2(M, ID, R_s, R_1) D_s \end{aligned}$$

Signer sends $(M, ID, R_s, R_1, Z_s)$ to the SEM.

After having received $(M, ID, R_s, R_1, Z_s)$, the SEM checks that the $ID$ of the signer is not revoked, then computes:

$$\begin{aligned} v_s &= H_2(M, ID, R_s, R_1) \\ Z &= Z_s + v_s D_{SEM} \end{aligned}$$

and verifies:

$\hat{e}(Z, P) = \hat{e}(R_s, R_1)\hat{e}(v_s H_1(ID, R_s), P_{pub})$

If so, the signer is a legitimate participant, and the SEM provides service for him/her.

SEM then picks a random number $r_2 \in Z_q^*$ such that $r_2^2 \bmod q \neq 1$, and computes:

$$\begin{aligned} R_2 &= r_2 P \\ S_{SEM} &= r_2^2 P + H_2(M, ID, R_s, R_1, R_2) D_{SEM} \end{aligned}$$

The pair $(R_2, S_{SEM})$ is sent to signer.

After having received $(R_2, S_{SEM})$, the signer computes:

$$\begin{aligned} v &= H_2(M, ID, R_s, R_1, R_2) \\ S_s &= r_1^2 P + v D_s \\ S &= S_s + S_{SEM} \end{aligned}$$

and verifies:

$\hat{e}(S, P) = \hat{e}(R_1, R_1)\hat{e}(R_2, R_2)\hat{e}(vQ_s, P_{pub})$

If so, the mediated signature on message $M$ under $ID$ is set to be $\sigma = (R_s, R_1, R_2, S)$.

(4) Verification: Given a signature $\sigma = (R_s, R_1, R_2, S)$ on message $M$ under $ID$, the verifier computes:

$$\begin{aligned} v &= H_2(M, ID, R_s, R_1, R_2) \\ Q_s &= H_1(ID, R_s) \end{aligned}$$

He accepts the signature if and only if $\hat{e}(S, P) = \hat{e}(R_1, R_1)\hat{e}(R_2, R_2)\hat{e}(vQ_s, P_{pub})$.

## 5.2 Security analysis

**Theorem 5.1** In our scheme, the dishonest PKG can not impersonate its signer to generate a valid mediated signature.

Analysis: We discuss the Theorem 5.1 from the following two aspects:

First, dishonest PKG can not generate a valid mediated signature by only utilizing the public information of a signer and the SEM.

For the valid mediated signature on message $M$ under signer $U$'s identity $ID$ :

$$S = S_s + S_{SEM} = r_1^2 P + r_2^2 P + vsQ_s$$

Consider following impersonation attack[19]: PKG wants to impersonate the signer $U$ to forge a mediated signature, it can do as follows:

Chooses $r'_s$, $r'_1$, $r'_2 \in Z_q^*$ at randomly, computes:

$$\begin{aligned} R'_s &= r'_s P \\ R'_1 &= r'_1 P \\ R'_2 &= r'_2 P \end{aligned}$$

Lets $Q'_s = H_1(ID, R'_s)$ as the $U$'s public key, then PKG computes:

$$\begin{aligned} v' &= H_2(M, ID, R'_s, R'_1, R'_2) \\ S' &= {r'_1}^2 P + {r'_2}^2 P + v' s Q'_s \end{aligned}$$

Mediated signature is $\sigma' = (R'_s, R'_1, R'_2, S')$. Because $\hat{e}(S', P) = \hat{e}(R'_1, R'_1)\hat{e}(R'_2, R'_2)\hat{e}(v'Q'_s, P_{pub})$, PKG forged a *valid* mediated signature.

However, signer $U$ can provide a proof to convince that the mediated signature is forged by PKG. To do so, he firstly sends $R_s = r_s P$ to an arbiter, and provides a *knowledge proof* that he knows $Q_s = H_1(ID, R_s)$ and private key $D_s = s_1 Q_s$; the arbiter randomly chooses a secret integer $a \in_R Z_q^*$ and sends $aP$ to $U$; $U$ then computes $B = \hat{e}(D_s, aP)$ and sends $B$ to arbiter. If the equation $B = \hat{e}(H_1(ID, R_s), P_{pub})^a$ holds, i.e., identity $ID$ corresponds to both $R_s = r_s P$ and $R'_s = r'_s P$. The arbiter deduces PKG dishonest because the master-key $s$ is only known to PKG.

Second, dishonest PKG can not generate a valid mediated signature by replacing signer's secret value $r_1$ and SEM's secret value $r_2$.

Consider the following impersonation attack: PKG wants to impersonate a signer with identity $ID$. To do so, PKG chooses $r'_s \in Z_p^*$ at randomly, lets $R'_s = r'_s P$, $Q'_s = H_1(ID, R'_s)$, lets $D'_s = s_1 Q'_s$ as signer's private key. To sign a message $M$, PKG must firstly present the service requisition to SEM. It interacts with the SEM as follows:

PKG chooses $r'_1 \in Z_q^*$ at randomly, computes:

$$\begin{aligned} R'_1 &= r'_1 P \\ v'_s &= H_2(M, ID, R'_s, R'_1) \\ Z'_s &= r'_s r'_1 P + v'_s D'_s \end{aligned}$$

Then he sends $(M, ID, R'_s, R'_1, Z'_s)$ to the SEM.

The SEM checks that the signer's $ID$ is not revoked, then computes:

$$\begin{aligned} v'_s &= H_2(M, ID, R'_s, R'_1) \\ Q'_s &= H_1(ID, R'_s) \\ Z' &= Z'_s + v'_s D_{SEM} \end{aligned}$$

It is able to find immediately $\hat{e}(Z', P) \neq \hat{e}(R'_s, R'_1)\hat{e}(v'_s H_1(ID, R'_s), P_{pub})$. Therefore, the SEM refuses to provide service for it.

**Theorem 5.2** In our scheme, the only functionality of the SEM is to revoke signer's signing privilege. It cannot generate valid mediated signatures of some message on behalf of its signers.

Supposing that an attacker is able to compromise the SEM and expose the secret key $D_{SEM}$, it enables the SEM to *un-revoke* previously revoked, or blocks possible future revocation of current valid identities. However, the knowledge of $D_{SEM}$ does not enable the attacker to sign messages on behalf of its signers, since the generation of a valid mediated signature needs a cooperation of the SEM and the signer. Let us consider an attacker trying to forge a signer's mediated signature on some message. Recall that the token sent to the signer by the SEM, it is a pair $(R_2, S_{SEM})$, where $R_2 = r_2 P$ and $S_{SEM} = r_2^2 P + vD_{SEM}$, respectively. We notice that they are all random elements in $G_1$, which is useless to the attacker.

**Theorem 5.3** The proposed ID-based mediated signature scheme is unforgeable under the random oracle model with the assumption that $G_1$ is a GDH group.

According to the analysis of Theorem 4.1, if we want to proof that our scheme is secure against adaptively chosen message and ID attack, we only need to proof that our scheme is secure against adaptively chosen message and given ID attack [10]. Now we proof the latter under the random oracle model.

**Lemma 5.1** If there is a forger $\mathscr{F}$ for an adaptively chosen message and *given* ID attack against our ID-based mediated signature scheme, $\mathscr{F}$ can ask queries to the oracle $H_1$, $H_2$, MeExtract, and MeSign, at most $q_{H_1}, q_{H_2}, q_E, q_S$ times, and has running time $T_0$ and advantage $\varepsilon_0 \geq 10(q_S + 1)(q_S + q_{H_2})/l$, then CDHP can be solved with probability $\varepsilon \geq 1/9$ within running time $T \leq (23 q_{H_2} T_0)/\varepsilon_0$.

*Proof*: Let $G_1$ be a cyclic additive group defined in Section 2. We show how to construct an algorithm $\mathscr{B}$ that compute $abP$ for a randomly given instance $P, aP, bP \in G_1$ (where $a, b \in Z_q^*$) by running $\mathscr{F}$ as a subroutine.

During the game, $\mathscr{F}$ will consult $\mathscr{B}$ for answers to the random oracles $H_1$, $H_2$. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collision, $\mathscr{B}$ keeps two lists $L_1$ and $L_2$ to store the answers. We assume that $\mathscr{F}$ will ask for $H_1(ID, \cdot)$ before $ID$ is used as an input of any other queries.

**Initialization:** Fix an identity $ID$, lets $P_{pub} = aP$ as system public key.

**ID-Hash Queries ($H_1$):** When $ID_i$ is submitted to $H_1$ oracle, $\mathscr{B}$ first scans $L_1$ of sorted elements $(ID_i, Q_{s_i})$ (where

$1 \le i \le q_{H_1}$) to check whether $H_1$ was already defined for that input. If it was, the previously defined value $Q_{s_i}$ is returned. Otherwise, $\mathscr{B}$ picks $r_i \in Z_q^*$ at randomly, defines $Q_{s_i} = \begin{cases} bP, & if \quad ID_i = ID \\ r_iP, & otherwise \end{cases}$, and stores $(D_i, Q_{s_i})$ in $L_1$.

**Private Key Extraction Queries (MeExtract):** When $\mathscr{F}$ requests the private key associated with an identity $ID_k$ (where $1 \le k \le q_E$ ), $\mathscr{B}$ recovers the corresponding $(ID_k, Q_{s_k})$ from $L_1$. Then $\mathscr{B}$ picks $u_k \in Z_q^*$ at randomly, lets $D_k = u_k Q_{s_k}$ as the private key corresponding to $ID_k$. Note that $\mathscr{F}$ must not ask the private key corresponding to the $ID_k = ID$.

**Message-Hash Queries ($H_2$):** When a message $(M_j, ID_j)$ is submitted to the $H_2$ oracle, $\mathscr{B}$ first scans $L_2$ of sorted elements $(M_j, ID_j, R_{s_j}, R_{1_j}, R_{2_j}, v_j)$ (where $1 \le j \le q_{H_2}$) to check whether $H_2$ was already defined for that input. If it was, the previously defined value $v_j$ is returned. Otherwise, $\mathscr{B}$ picks $r_{1_j}, r_{2_j}, v_j \in_R Z_q^*$ at randomly, returns $v_j$ as the answer to $\mathscr{F}$, lets $R_{s_j} = r_j P$, $R_{1_j} = r_{1_j} P$, $R_{2_j} = r_{2_j} P$, and stores $(M_j, ID_j, R_{s_j}, R_{1_j}, R_{2_j}, v_j)$ in $L_2$.

**Signing Queries (MeSign):** If $\mathscr{F}$ asks the signature on $M_t$ of $ID_t$, $\mathscr{B}$ first scans $L_1$ to recover the previously defined value $(ID_t, Q_{s_t})$, then scans $L_2$ to recover the previously defined value $(M_t, ID_t, R_{s_t}, R_{1_t}, R_{2_t}, v_t)$. Then $\mathscr{B}$ lets $S_t = r_{1_t}^2 P + r_{1_t}^2 P + r_t v_t (aP)$, and returns $\sigma_t = Sign(M_t, ID_t) = (M_t, ID_t, R_{s_t}, R_{1_t}, R_{2_t}, v_t, S_t)$ to $\mathscr{F}$ as the answer. Obvious, $\sigma_t$ is a valid ID-based mediated signature, i.e. it satisfies the verify equation $\hat{e}(S_t, P) = \hat{e}(R_{1_t}, R_{1_t})\hat{e}(R_{2_t}, R_{2_t})\hat{e}(v_t Q_{s_t}, P_{pub})$.

**Output:** We need to take care of a nasty problem of collisions of the query result of **MeSign** and $\boldsymbol{H}_2$, as mentioned in [20] (Proof of Lemma 4). This may cause some "collision"; a query result of **MeSign** may produce a value that is inconsistent with other query results of **MeSign** or $\boldsymbol{H}_2$. In this case, $\mathscr{B}$ just outputs fail and exits. If no collisions have appeared, $\mathscr{B}$ outputs a valid signature $\sigma = (M, ID, R_s, R_1, R_2, v, S)$ with probability $\varepsilon_0$, which is expected to be valid for the fixed ID, without accessing any oracles except $H_1$, $H_2$. i.e. it satisfies the verification equation $\hat{e}(S, P) = \hat{e}(R_1, R_1)\hat{e}(R_2, R_2)\hat{e}(vQ_s, P_{pub})$. Considering $P_{pub} = aP$, $Q_s = bP$, we have $\hat{e}(S, P) = \hat{e}(R_1, R_1)\hat{e}(R_2, R_2)\hat{e}(vabP, P)$ ..... (1).

We apply the oracle replay technique which was invented by Pointcheval and Stern in [20,21], in which, $\mathscr{B}$ replays the same random tape but different choices of $H_2$, as done in the forking lemma [20], we obtain signature $(M, ID, R_s, R_1, R_2, v', S')$ with $v \ne v'$, which are expected to be valid with respect to hash function $H_2'$ on $(M, ID, R_s, R_1, R_2)$. So we have $\hat{e}(S', P) = \hat{e}(R_1, R_1)\hat{e}(R_2, R_2)\hat{e}(v'abP, P)$ .....(2).

From (1) and (2), we have:

$\hat{e}(S - S', P) = \hat{e}((v - v')abP, P)$

Then we obtain $abP = \frac{S - S'}{v - v'}$.

Since the oracle $\boldsymbol{H}_1$, $\boldsymbol{H}_2$, **MeExtract**, and **MeSign** generate random distribution and are indistinguishable from the original scheme, $\mathscr{F}$ learns nothing from query results. Therefore, $\mathscr{B}$ works as expected if no collisions appear in **Output**. Intuitively, since $v$ is random, the possibility of collisions is negligible; in [20] (Proof of Theorem 3), this probability was computed explicitly, and furthermore, it was proved that the oracle replay in **Output** produces valid signatures $(M, ID, R_s, R_1, R_2, v, S)$ and $(M, ID, R_s, R_1, R_2, v', S')$ with the expected properties such that $v \ne v'$ with probability $\varepsilon \ge 1/9$ within the time $T \le (23 q_{H_2} T_0)/\varepsilon_0$.

## 5.3 Discussion

There are two types of possible attacks against the proposed scheme. The first comes from the choice of the random numbers used in our scheme; the second comes from the attacks on the discrete logarithm of elliptic curves. We show the details as following:

(1) Choosing appropriate random numbers

In our ID-based signature scheme (see the Section 4.1(3)), if $r_v r_u \bmod q = 1$, then $X = r_u r_v P + hD_u$ can be represented as $X = P + hD_u$, thus the signer's private key can be computed from $D_u = h^{-1}(X - P)$.

In our ID-based mediated signature scheme (see the Section 5.1(3)), if $r_1 r_s \bmod q = 1$, then $Z_s = r_s r_1 P + v_s D_s$ can be represented as $Z_s = P + v_s D_s$, thus the signer's private key can be computed by SEM from $D_s = v_s^{-1}(Z_s - P)$. If $r_1^2 \bmod q = 1$, then $S_s = r_1^2 P + vD_s$ can be represented as $S_s = P + vD_s$, thus the signer's private key can be computed by the verifier from $D_s = v^{-1}(S_s - P)$. If $r_2^2 \bmod q = 1$, then $S_{SEM} = r_2^2 P + vD_{SEM}$ can be represented as $S_{SEM} = P + vD_{SEM}$, thus the SEM's private key can be computed by the signer from $D_{SEM} = v^{-1}(S_{SEM} - P)$.

The probability of both $r_v r_u \bmod q = 1$ and $r_1 r_s \bmod q = 1$ are all $1/(q-1)$, and the probability both $r_1^2 \bmod q = 1$ and $r_2^2 \bmod q = 1$ are all $1/(q-1)$. It is neglectable when $q$ is large enough. (e.g., The bit length of $q$ exceed the length that defined in the international standards for elliptic curve cryptography, such as ANSIX9.62, ANSIX9.63, IEEE-P1363, ISO/IEC14888,etc..)

In our scheme, we restrict that $r_v r_u \bmod q \ne 1$, $r_1 r_s \bmod q \ne 1$, $r_1^2 \bmod q \ne 1$, and $r_2^2 \bmod q \ne 1$ to avoid these events taking place. Though similar ID-based signature scheme[16] and its variants [8,23,24] have not any restriction for choosing random numbers, and do not discuss this security flaw, but we especially emphasize such a restriction in order to make our scheme more perfect.

(2) The attacks on the discrete logarithm of elliptic curves

Our scheme is based on elliptic curve cryptography whose security relies on the difficulty to solve the discrete logarithm problem of the elliptic curve abelian group (The Elliptic Curve Discrete Logarithm Problem, ECDLP). The results show, the time complexity is exponential to break the ECDLP using the Pollard rho algorithm that is acknowledged most effective attack method for ECDLP [25,26]. However, not all the elliptic curves are suitable for cryptography. In order to guarantee the security, we must choose

secure elliptic curves whose orders are large prime numbers (e.g. Its bit length exceeds 234[26]) or include large prime factors. The result [27] provided four efficient methods to select secure elliptic curves. As long as select appropriate secure elliptic curves, as far as we know, there are not efficient methods to break ECDLP.

# 6 Conclusions

We improved an ID-based signature scheme and constructed an efficient ID-based mediated signature scheme from the bilinear pairing. Our ID-based mediated signature scheme has a character that the dishonest PKG can not impersonate signer to generate a valid mediated signature. Our scheme not only provides an efficient method for immediate revocation of a user's identity in ID-based public key cryptosystems, but also solves the problem that exists in some existing ID-based signatures scheme, in certain extent, in which, a trusted PKG and key escrow are needed.

## Acknowledgement

This work was supported by the National Natural Science Foundation of China (60873268); the China Postdoctoral Science Foundation (No.20080431238 and No.200902596); the Natural Science Foundation Research Plan of Shaanxi province of China (No.08JK382 and No.2009JM8004-5).

# References

[1] T.Candebat, C.R.Dunne and D.Gray. (2005) Pseudonym Management using Mediated Identity-Based Cryptography, *In Advances in 2005 ACM Workshop on Digital Identity Management (DIM'05)*, Fairfax, Virginia, USA, pp.1-10.

[2] D.Boneh, X.Ding, G.Tsudik and C.Wong. (2001) A method for fast revocation of public key certificates and security capabilities, *In Advances in the 10th USENIX Security Symposium*, Washington D.C., pp.297-308.

[3] D.Boneh, X.Ding, G.Tsudik, Identity-based Mediated RSA.(2002) *In Advances in 3rd. International Workshop on Information and Security Applications*, Jeju Island, Korea, pp.192-209.

[4] X.Ding,G.Tsudik.(2003) Simple Identity-Based Cryptography with Mediated RSA. *volume 2612 of LNCS*, Springer-Verlag, pp.192-209.

[5] D.Boneh, M.Franklin.(2001) Identity-based encryption from the Weil pairings, *In Advances in Cryptology-Crypto2001,volume 2139 of LNCS*, Springer-Verlag, pp.213-229.

[6] B.Libert,J.Quisquater.(2003) Efficient revocation and threshold pairing based cryptosystems. *In Advances in 22nd Symposium on Principles of Distributed Computing*, ACM Press, pp.163-171.

[7] J.Baek and Y.Zheng.(2004) Identity-based threshold decryption. *In Advances in PKC'04, volume 2947 of LNCS*. Springer-Verlag, PP.248-261.

[8] X.Cheng, L.Guo, X.Wang.(2006) An Identity-based Mediated Signature Scheme from Bilinear Pairing. International Journal of Network Security, Vol.2, No.1, pp.29-33.

[9] Q.Wu, W.Susilo, Y.Mu, F.Zhang.(2006) Efficient Partially Blind Signatures with Provable Security. *In Advances in ICCSA 2006, volume 3982 of LNCS*,Springer-Verlag, pp.345-354.

[10] J.C.Cha and J.H.Cheon, An identity-based signature from gap Diffie-Hellman groups, *In Advances in PKC 2003, volume 2567 of LNCS*, Springer-Verlag, pp.18-30.

[11] S.D.Galbraith, K.Harrison and D.Soldera.(2002) Implementing the Tate pairings. *In Advances in ANTS 2002, volume 2369 of LNCS*, Springer-Verlag, pp.324-337.

[12] F.Hess.(2003) Efficient identity based signature schemes based on pairings. *In Advances in Select Areas in Cryptography, SAC 2002, volume 2595 of LNCS*, Springer-Verlag, pp.310-324.

[13] J.H.Cheon, Y.Kim, H.J.Yoon.(2004) A New ID-based Signature with Batch Verification, Cryptology ePrint Archive, Report 2004/131.

[14] X.Huang,Y.Mu,W.Susilo,F.Zhang.(2005) Short Designated Verifier Proxy Signature from Pairings. *In Advances in EUC Workshops 2005, volume 3823 of LNCS*. Springer-Verlag, pp.835-844.

[15] D.Boneh, B. Lynn and H. Shacham.(2001) Short signatures from the Weil-pairing. *In Advances in Asiacrypt'01, volume 2248 of LNCS*, Springer-Verlag, pp.514-532.

[16] X.Yi.(2003) An identity-based signature scheme from the Weil pairing, IEEE Communications Letters, vol.7, no.2, pp.76-78.

[17] X.Cheng,J.Liu,X.Wang.(2005) Identity-based aggregate and verifiably encrypted signatures from bilinear pairing. *In Advances in ICCSA 2005, volume 3483 of LNCS*, Springer-Verlag, pp.1046-1054.

[18] K.Paterson.(2002) ID-based signatures from pairings on elliptic curves. Electronics Letters, vol.38, no.18, pp.1025-1026.

[19] X.Chen, F.Zhang, K.Kim.(2002) A new ID-based group signature scheme from bilinear pairings. Cryptology ePrint Archive, Report2002/184, http://eprint.iacr.org/

[20] D.Pointcheval and J.Stern.(2000) Security arguments for digital signatures and blind signatures, Journal of Cryptology, vol.13, no.3, pp.361-396.

[21] D.Pointcheval and J.Stern.(1998) Security proofs for signature schemes. *In Advances in Cryptology-Eurocrypt 96, volume 1163 of LNCS*, Springer-Verlag, pp.387-405.

[22] R.Gennaro, S.Jarecki, H.Krawczyk and T. Rabin.(1996) Robust threshold DDS signatures. *In Advances in Cryptology-Eurocrypt'96, volume 1070 of LNCS*, New York,Springer-Verlag, pp.354-371.

[23] J.Malone-Lee.(2002) Identity-Based Signcryption. Cryptology ePrint Archive, http://eprint.iacr.org /2002/098/.

[24] B.Libert, J.Quisquater.(2003) New identity based signcryption schemes from pairings. IEEE Information Theory Workshop 2003. Paris, France, Available from http://eprint.iacr.org/2003/023.

[25] Ma DaPeng, Huang JianHua.(2007) The elliptic curve cryptosystem and its security analysis. http://www.paper.edu.cn/ downloadpaper.php/serialnumber=200707-432.

[26] Huang BaoQing. The elliptic curve cryptosystem(ECC). http://www.hids.com.cn/ data.asp.

[27] J.H. Silverman.(1986) The Arithmetic of Elliptic Curves. Graduate Texts in Math., vol.106, Springer-Verlag, Berlin, Heidelberg, New York, pp.130-136.