# An Efficient ID-based Digital Signature with Message Recovery Based on Pairing

Raylin Tso, Chunxiang Gu[♯], Takeshi Okamoto[†], and Eiji Okamoto[‡]

Department of Risk Engineering
Graduate School of Systems and Information Engineering
University of Tsukuba, Japan
{raylin, ken[†], okamoto[‡]}@risk.tsukuba.ac.jp
[♯] Network Engineering Department, Information Engineering University
Zhengzhou P.R. China
gcxiang5209@yahoo.com.cn

**Abstract.** Signature schemes with message recovery have been wildly investigated a decade ago in the literature, but the first ID-based signature with message recovery goes out into the world until 2005. In this paper, we first point out and revise one little but important problem which occurs in the previous ID-based signature with message recovery scheme. Then, by completely different setting, we propose a new ID-based signature scheme with message recovery. Our scheme is much more efficient than the previous scheme. In our scheme (as well as other signature schemes with message recovery), the message itself is not required to be transmitted together with the signature, it turns out to have the least data size of communication cost comparing with generic (not short) signature schemes. Although the communication overhead is still larger than Boneh et al. 's short signature (which is not ID-based), the computational cost of our scheme is more efficient than Boneh et al. 's scheme in the verification phase. We will also prove that the proposed scheme is provably secure in the random oracle model under CDH Assumption.

**Key words**: CDH problem, Identity-based signature, Message recovery, Pairing, Short signature.

## 1 Introduction

A digital signature scheme with message recovery is a signature scheme that the original message of the signature is not required to be transmitted together with the signature since it has been appended to the signature and can be recovered according to the verification/message-recovery process. It is different to an authenticated encryption scheme or signcryption scheme since in this scheme, the embed message can be recovered by anyone without a secret information. The purpose of this kind of signatures are to minimize the total length of the original message and the appended signature so are useful in an organization where bandwidth is one of the main concern or useful for the applications in which small messages should be signed.

It is obvious that an RSA signature [10] can be used with message recovery since it is unique in the sense that the signature and encryption functions are inverse to each other. But, for small size messages, it yields much larger signatures. For example, to sign a 100-bit message, the signature will be the size of 1024-bit. In 1993, Nyberg and Rueppke [7] proposed the first digital signature with message recovery based on the discrete logarithm problem (DL problem). Schemes based on the DL problem produce relatively small signatures if they are implemented over a finite group over elliptic curve. For example, a 320-bit signature is enough for a 100-bit message. Due to this reason, DL problem based signature schemes with message recovery (as well as their variants) are appropriate for signing small messages so have been extensively investigated in the literature (e.g., [1, 6–8, 12]).

On the other hand, the concept of identity-based (ID-based) cryptosystem was firstly introduced by Shamir [11] in 1984 which can simplify key management procedures of traditional certificate-based cryptography. Many ID-based cryptosystems have been proposed since that but no ID-based signature scheme with message recovery goes out into the world until the scheme proposed by Zhang et al. [13] in 2005. Zhang et al. proposed two schemes in the paper: an ID-based message recovery signature scheme for messages of fixed length, and an ID-based partial message recovery signature scheme for messages of arbitrary length. Zhang et al. 's idea gives a new concept to shorten ID-based signatures in contrast to proposing a short signature scheme.

**Our Contribution:** Before the main contribution, we first point out and give a revision to one little but important problem occurs in Zhang et al.'s ID-based signature with message recovery scheme [13]. Our small revision corrects their scheme. The main contribution of this paper is to propose a new ID-based signature scheme with message recovery which is much more efficient than Zhang et al. 's scheme. Our scheme improves the computational cost by *one scalar multiplication* in the signing phase and almost *one pairing computation* in the verify/message-recovery phase comparing to Zhang et al. 's scheme. Our idea is inspired from Barreto et al. 's ID-based signature scheme [2] in the benefits that our scheme inherits the efficiency of their scheme on one side and also reduce the total length of the original message and the appended signature on the other side. In addition, Barreto et al. give the security proof of [2] on a stronger assumption (i.e., the $q$-strong Diffie-Hellman problem) while we will prove that our scheme is secure against existential forgery under adaptively chosen message attack and ID attack in the random oracle model and under only a weaker assumption: the hardness assumption of computational Diffie-Hellman (CDH) problem. The essential idea of the security proofs of our scheme can also be used to prove the security of [2] so as to reduce their security assumption from a stronger one to a weaker one. This is another contribution of this paper.

The rest of this paper is organized as follows. in Section 2, we recall some preliminary works which will be used throughout this paper. Section 3 reviews and revises the first ID-based signature scheme with message recovery. In Section 4, we present our new scheme, its variation and the efficiency comparisons with other schemes. In Section 6, we give a concrete proof of our scheme in the random oracle model. Finally, we conclude this paper in Section 7.

## 2 Preliminaries

### 2.1 Bilinear Pairings and the Related Computational Assumption

Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of the same prime order $q$. $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a map which satisfies the following properties.

1. Bilinear: $\forall P, Q \in G_1, \forall \alpha, \beta \in Z_q, \hat{e}(\alpha P, \beta Q) = \hat{e}(P, Q)^{\alpha\beta}$;
2. Non-degenerate: If $P$ is a generator of $G_1$, then $\hat{e}(P, P)$ is a generator of $G_2$;
3. Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

Such an bilinear map is called an *admissible bilinear pairing* [3]. The Weil pairings and the Tate pairings of elliptic curves can be used to construct efficient admissible bilinear pairings.

**Definition 1 (CDH Assumption).** Let $(G_1, +)$, $(G_2, \cdot)$ and $\hat{e}$ be the same as those defined at Section 2.1. Let also $P$ be a generator of $G_1$, the challenger chooses $a, b \in Z_p$ at random and outputs $(P, A = aP, B = bP)$. The adversary then attempts to output $abP \in G_1$. An adversary, $\mathcal{B}$, has at least an $\epsilon$ advantage if

$$Pr[\mathcal{B}(P, aP, bP) = abP] \geq \epsilon$$

where the probability is over the randomly chosen $a, b$ and the random bits consumed by $\mathcal{B}$.

**Definition 2.** We say the CDH assumption is $(t, \epsilon)$-secure if there is no $t$-time adversary with at least $\epsilon$ advantage in solving the above game.

### 2.2 Scheme Model

An ID-based message recovery signature scheme is defined by four algorithms:

- **Setup:** A deterministic algorithm which takes as input a security parameter $\lambda$, outputs the Key generation Center $KGC$'s private key, $S_{KGC}$, and public key, $P_{pub}$, together with the system parameters, $para$.
- **Extract:** A deterministic algorithm which takes as input an identity, $ID_i$, of a user $U_i$, outputs the user's private key, $S_{ID_i}$.
- **Sign:** A probabilistic algorithm which takes as inputs a signer's private key $S_{ID}$ and a message $m$, outputs a signature $\sigma$.
- **Verify:** A deterministic algorithm which takes as input the sender's identity, $ID$, and the signature, $\sigma$, outputs 1 if $\sigma$ is a valid signature. In this case, the original message can be recovered successfully. Otherwise, outputs 0.

### 2.3 Security Definition

For digital signatures, the widely accepted notion of security was defined by Goldwasser et. al. in [5] as *existential forgery against adaptive chosen-message attack* (EF-ACMA). It's ID-based variation is described as the following form.

**Definition 3.** An ID-based digital signature scheme is said to be secure against EF-ACMA, if for any polynomial-time adversary $\mathcal{F}$, the advantage defined by

$$Adv_{\mathcal{F}}^{EF-ACMA} \triangleq Pr \left[ \begin{array}{l} Verify((m,\sigma), ID) = 1, \\ (ID, m, \sigma) \notin S_{list}, \\ (ID, .) \notin E_{list} \end{array} \middle| \begin{array}{l} para \leftarrow Setup(1^{\lambda}), \\ (ID, m, \sigma) \leftarrow \mathcal{F}^{S(.),E(.)}(para) \end{array} \right]$$

is negligible, where $S_{list}$ and $E_{list}$ are the query/answer lists coming from *Sign* oracle $S(.)$ and *Extract* oracle $E(.)$ respectively during the attack. In the random oracle model, the attackers can also access to the random oracle. The probability is taken over the coin tosses of the algorithms, of the oracles, and of the forger.

### 2.4 Notations

The following notations will be used throughout this paper.

- $a||b$**:** a concatenation of two strings $a$ and $b$.
- $\oplus$**:** X-OR computation in the binary system.
- $[x]_{10}$ **:** the decimal notation of $x \in \{0,1\}^*$.
- $[y]_2$ **:** the binary notation of $y \in Z$.
- $_{l_2}|\beta|$ **:** the first $l_2$ bits of $\beta$ from the left side.
- $|\beta|_{l_1}$ **:** the first $l_1$ bits of $\beta$ from the right side.

## 3 Zhang et al.'s Scheme Revisit

In this section, we review Zhang et al.'s ID-based message recovery signature scheme [13] and show one problem of their scheme.

- **Setup:** $PKG$ chooses a random number $s \in {Z_q}^*$ and sets $P_{pub} = sP$. $PKG$ also publishes system parameters $\{G_1, G_2, \hat{e}, q, \lambda, P, H_0, H_1, F_1, F_2, k_1, k_2\}$, and keeps $s$ as the master-key, which is known only by itself. Here
  - $|q| = k_1 + k_2$,

  and $H_0, H_1, F_1, F_2$ are for cryptographic hash functions such that
  - $H_0 : \{0,1\}^* \to {G_1}^*$,
  - $H_1 : \{0,1\}^* \to {Z_q}^*$,
  - $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$
  - $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$.
- **Extract:** A user submits his/her identity information $ID$ to $PKG$. $PKG$ computes the user's public key as $Q_{ID} = H_0(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his /her private key.
- **Sign:** Let the message be $m \in \{0,1\}^{k_2}$.

  S1: Compute $v = e(P,P)^k$, where $k \in_R {Z_q}^*$.

  S2: $f = F_1(m)||(F_2(F_1(m)) \oplus m)$.

  S3: $r = H_1(v) + f \bmod q$.

  S4: $U = kP - rS_{ID_A}$

  The signature is $(r, U)$
- **Verification:** Given $ID_A$, a message $m$, and a signature $(r, U)$, compute

$$r - H_1(\hat{e}(U,P)\hat{e}(Q_{ID_A}, P_{pub})^r) = f, \quad \text{and} \quad m = {}_{k_2}|f| \oplus F_2(|f|_{k_1}).$$

  Accept the signature if $|f|_{k_1} = F_1(m)$. Otherwise, reject the signature.

### 3.1 Discussion

We found that in some undesirable cases, a correctly generated signature may be misjudged and rejected. Accordingly, in such cases, the message cannot be recovered correctly.

Since we have $|q| = k_1 + k_2$ and we know that any element $a \in {Z_q}^*$ of course has the size $|a| \leq |q|$. On the contrary, any value $b$ with size $|b| = |q|$ cannot be concluded that $b \in {Z_q}^*$. An toy example is that elements $16, 17, 18 \in {Z_{19}}^*$ all have the same size equal to $|19| = 5$, but elements $20, 21, \cdots, 31 \notin {Z_{19}}^*$ also have the same size 5. These cases come more often when $q$ is large.

In S2 of the signing phase, $f = F_1(m)||(F_2(F_1(m)) \oplus m)$. $|f| = k_1 + k_2 = |q|$, but it is very likely that $f > q$ even though they have the same size. If $f > q$, say $f = f' + q$, then, in the verification phase,

$$r - H_1(\hat{e}(U, P)\hat{e}(Q_{ID_A}, P_{pub})^r) = f', \quad \text{and} \quad m = {}_{k_2}|f'| \oplus F_2(|f'|_{k_1}).$$

With a large probability $|f'|_{k_1} \neq F_1(m)$, so the signature will be reject although it is generated correctly.

Their second scheme for partial message recovery also suffers this problem. To prevent this problem of misjudgement, we suggest $r$ be $H_1(v) + f$ instead of $H_1(v) + f \bmod q$. This small revision is very important in order to make the verification correct.

## 4 New ID-based Message Recovery Scheme

In this section, we present our efficient ID-based message recovery signature scheme with the restriction (for any message recovery scheme) that it can deal with only messages of some fixed length (ie., $m \in \{0, 1\}^{l_1}$ for some fixed integer $l_1$).

- **Setup:** Takes as input a security parameter $\lambda \in N$, outputs a random number $s \in Z_q^*$ as $KGC$'s private key and sets $P_{pub} = sP$. The system parameters made public are

$$para = \{G_1, G_2, \hat{e}, q, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2\}, where$$

  - $G_1, G_2$ are cyclic groups of the same order $q$, $|q| = l_1 + l_2$,
  - $\hat{e} : G_1 \times G_1 \leftarrow G_2$ is the admissible bilinear pairing,
  - $\mu = \hat{e}(P, P)$,
  - $H : \{0, 1\}^* \rightarrow {Z_q}^*$, a collision resistent one-way function,
  - $H_1 : G_2 \rightarrow \{0, 1\}^{|q|}$, a collision resistent one-way function,

- $F_1 : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$, a collision resistent one-way function,
- $F_2 : \{0,1\}^{l_2} \to \{0,1\}^{l_1}$ a collision resistent one-way function,.

- **Extract:** Takes as input a user's identity $ID_i \in \{0,1\}^*$, $KGC$ computes the user's private key $S_{ID_i} \leftarrow (H(ID_i) + s)^{-1}P$. The user's ID-based public key $P_{ID_i}$ is $(H(ID_i) + s)P$, which can be computed as $H(ID_i)P + P_{pub}$.
- **Sign:** For input a user $A$'s private key $S_{ID_A}$ and a message $m \in \{0,1\}^{l_1}$:
  (1) Pick a random number $r_1 \in Z_q{}^*$, compute $\mu^{r_1}$ and $\alpha \leftarrow H_1(\mu^{r_1}) \in \{0,1\}^{|q|}$
  (2) Compute $\beta \leftarrow F_1(m)||(F_2(F_1(m)) \oplus m)$ and $r_2 \leftarrow [\alpha \oplus \beta]_{10}$.
  (3) Compute $U \leftarrow (r_1 + r_2)S_{ID_A}$.

  The signature $\sigma$ on $m$ is $(r_2, U)$.
- **Verify:** Given the signature $\sigma$ and $ID_A$:
  (1) Compute $\tilde{\alpha} \leftarrow H_1(\hat{e}(U, P_{ID_A})\mu^{-r_2})$.
  (2) Compute $\tilde{\beta} \leftarrow [r_2]_2 \oplus \tilde{\alpha}$.
  (3) Recover the message $\tilde{m} \leftarrow |\tilde{\beta}|_{l_1} \oplus F_2({}_{l_2}|\tilde{\beta}|)$.
  (4) Output 1 and accept $\sigma$ as a valid signature of the message $m \leftarrow \tilde{m}$ if and only if $|_{l_2}\tilde{\beta}| = F_1(\tilde{m})$.

**Correctness** The correctness of this scheme can be proved as follows:

$$\begin{aligned}
\hat{e}(U, P_{ID_A})\mu^{-r_2} &= \hat{e}((r_1 + r_2)S_{ID_A}, P_{ID_A})\hat{e}(P, P)^{-r_2} \\
&= \hat{e}((H(ID_A) + s)^{-1}P, (H(ID_A) + s)P)^{r_1+r_2}\hat{e}(P, P)^{-r_2} \\
&= \hat{e}(P, P)^{r_1+r_2}\hat{e}(P, P)^{-r_2} \\
&= \hat{e}(P, P)^{r_1} = \mu^{r_1}
\end{aligned}$$

If $\sigma$ is a valid signature, then $H_1(\mu^{r_1}) = \alpha$ and

$$F_1(m)||(F_2(F_1(m)) \oplus m) = \beta = [r_2]_2 \oplus \alpha.$$

Hence, we obtain

$$\begin{aligned}
&|\beta|_{l_1} \oplus F_2({}_{l_2}|\beta|) \\
&= (F_2(F_1(m)) \oplus m) \oplus F_2(F_1(m)) \\
&= m.
\end{aligned}$$

Finally, the integrity of $m$ is justified if ${}_{l_2}|\beta| = F_1(m)$. $\square$

### 4.1 Variation (A Partial Message Recovery Scheme for Long Messages)

In this section, we simply modify the previous scheme so that the modified scheme can be used for messages of arbitrarily length (i.e., $m \in \{0,1\}^*$).

- **Setup:** The system setting is the same as the previous scheme with the only modification of $F_1$. In this scheme, $F_1 : \{0,1\}^* \rightarrow \{0,1\}^{l_2}$.
- **Extract:** The same as the previous scheme.
- **Sign:** For input a user $A's$ private key $S_{ID_A}$ and a message $m \in \{0,1\}^*$:
  (1) Pick a random number $r_1 \in {Z_q}^*$, compute $\mu^{r_1}$ and $\alpha \leftarrow H_1(\mu^{r_1})$
  (2) Divide $m$ into $m_2||m_1$ with $m_1 \in \{0,1\}^{l_1}$
  (3) Compute $\beta \leftarrow F_1(m)||(F_2(F_1(m)) \oplus m_1)$ and $r_2 \leftarrow [\alpha \oplus \beta]_{10}$.
  (4) Compute $U \leftarrow (r_1 + r_2)S_{ID_A}$.

  The signature $\sigma$ on $m$ is $(m_2, r_2, U)$.
- **Verify:** Given the signature $\sigma$ and $ID_A$:
  (1) Compute $\tilde{\alpha} \leftarrow H_1(\hat{e}(U, P_{ID_A})\mu^{-r_2})$
  (2) Compute $\tilde{\beta} \leftarrow [r_2]_2 \oplus \tilde{\alpha}$ where $[x]_2$ is the binary representation of $x$
  (3) Recover $\tilde{m}_1 \leftarrow |\tilde{\beta}|_{l_1} \oplus F_2({}_{l_2}|\tilde{\beta}|)$.
  (4) Output 1 and accept $\sigma$ if and only if ${}_{l_2}|\tilde{\beta}| = F_1(m_2||\tilde{m}_1)$. Otherwise, output 0 and abort the next step.
  (5) Recover $m \leftarrow m_2||\tilde{m}_1$.

**Correctness:** The correctness of the scheme is straightforward according to that of the previous scheme.

## 5 Efficiency Comparison

Denote our scheme and the modified scheme as Scheme 1 and Scheme 2, respectively. In this section, we compare our schemes with Boneh et al. 's short signature scheme [4], Barreto et al. 's efficient ID-based signature scheme [2] , and Zhang et al. 's ID-based message recovery signature schemes [13] in total length and computation cost. In Table 1, we denote by $\hat{e}$ a computation of the pairing, $EC$ an ordinary scalar multiplication in $G_1$, and $Exp.$ an exponential operation in $G_2$. In addition, the hash functions used by our schemes and the scheme of BLMQ[2] are generic and efficient so the computation cost can be neglected. On the contrary, Boneh et al. [4] and Zhang et al. [13] 's schemes depend on a special hash function called "MaptoPoint", which is still probabilistic and usually not efficient enough to be neglected. The computation of a "MaptoPoint" hash is denoted by $\mathcal{H}$ in Table 1.

To compare at approximately the same security as a standard 1024-bit RSA signature, $q$ should be a 170-bit prime and $G_1$ be a group where each element of $G_1$ is 171-bit if we use any of the families of curves described in [4]. In addition, $l_1 = k_2 = 91$ according to [13] in order to obtain a $2^{-80}$ probability of the verification condition holding for an attempted forgery generated by an adversary.

Except Boneh et al. 's short signature scheme [4], we see from these results that our schemes surpass other schemes in at least one aspect and be second to none in every aspect. Our schemes are faster than all known pairing-based IBS methods according to [2] since our schemes inherit the efficiency of [2] but surpass [2] in the aspect of total-length (i.e., $|message|+|signature|$). Also note that our schemes happens to be faster than [4] at verification and exceed [4] in the aspect of ID-based propoerty.

**Table 1.** Efficiency comparison

| | ID-based | Total Length | Sign | Verify |
|---|---|---|---|---|
| Scheme 1* | Y | $\|q\| + \|G_1\|$ | $1Exp. + 1EC$ | $1\hat{e} + 1Exp. + 1EC$ |
| Scheme 2 | Y | $\|m\| - l_1 + \|q\| + \|G_1\|$ | $1Exp. + 1EC$ | $1\hat{e} + 1Exp. + 1EC$ |
| BLMQ[2] | Y | $\|m\| + \|q\| + \|G_1\|$ | $1Exp. + 1EC$ | $1\hat{e} + 1Exp. + 1EC$ |
| BLS[4] | No | $\|m\| + \|G_1\|$ | $1EC + 1\mathcal{H}$ | $2\hat{e} + 1EC + 1\mathcal{H}$ |
| ZSM[13] 1* | Y | $\|q\| + \|G_1\|$ | $1Exp. + 2EC$ | $2\hat{e} + 1Exp + 1\mathcal{H}.$ |
| ZSM[13] 2 | Y | $\|m\| - k_2 + \|q\| + \|G_1\|$ | $1Exp. + 2EC$ | $2\hat{e} + 1Exp. + 1\mathcal{H}$ |

* Available for messages of fixed length only.

## 6 Security Proof

Since the two schemes are essentially the same and can be proved in a similar way, we give a concrete security proof of the basic scheme in this section only. We will show that the proposed scheme is secure against EF-ACMA and ID-attack in the random oracle model assuming the hardness of CDH problem (see Definition 1). In addition, although we will not discuss in detail, we emphasize that the proofs we used here are also useful to prove the security of Barreto et al.'s ID-based signature scheme [2]. The advantage of using our security proofs is that we need only a weaker hardness assumption while the scheme in [2] is proved under a stronger hardness assumption (i.e., the $q$-strong Diffie-Hellman problem).

The following definition will be used as a core of the proof.

**Definition 4 (Forking Lemma [9]).** Let $(\mathcal{G}, \Sigma, V)$ be a generic digital signature scheme with security parameter $k$. Let $\mathcal{A}$ be a probabilistic polynomial time Turing machine whose input only consists of public data. Assume that, within a time bound $T$, $\mathcal{A}$ can produce a valid signature $(m, \sigma_1, h, \sigma_2)$ with probability $\epsilon \geq 10(q_s + 1)(q_s + q_h)/2^k$ by making $q_s$ signing queries and $q_h$ random oracle queries. If the triple $(\sigma_1, h, \sigma_2)$ can be simulated without knowing the private key, with an indistinguishable distribution probability, then there exists another Turing machine $\mathcal{A}'$ that uses $\mathcal{A}$ to produce two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$ in expected time $T' \leq 120686 q_h T/\epsilon$.

For short, denote our scheme of Section 4 by $IDMR$, we first define a related (non-ID-based) public key signature scheme with message recovery $PKMR = (KGen, Sign', Verify')$ as following:

- **KGen:** Takes as input a security parameter $\lambda \in N$,
  - runs $Setup(1^\lambda)$ of $IDMR$ to generate a master key $s$ and system parameters $para = \{G_1, G_2, \hat{e}, q, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2\}$,
  - selects randomly $ID \in \{0,1\}^*$, computes $P_{ID} = H_1(ID)P + P_{pub}$, $S_{ID} = (H_1(ID) + s)^{-1}P$,
  - returns $S_{ID}$ as private key and $(para, P_{ID})$ as public key.
- **Sign':** Given a secret key $S_{ID}$ and a message $m \in \{0,1\}^{l_1}$, do the same as that of $IDMR$.
- **Verify'**: Given the signature $\sigma$ and the public key $(para, P_{ID})$, do the same as that of $IDMR$

It is obviously that the $PKMR$ is a *generic signature scheme*. Also, if we assume $H : \{0,1\}^* \to Z_q^*$ to be a random function, then the function $H'$ defined by

$$\begin{aligned} H' : \{0,1\}^* &\to G_1 \\ ID_i &\to H(ID_i)P + P_{pub} \end{aligned}$$

is a random function. In the following proof, we take $H'(.)$ instead of $H(.)$ as a random oracle.

**Lemma 1.** In the random oracle mode, if there is an adversary $\mathcal{A}$ whose input only consists of public data, and can succeed in existential forgery on $IDMR$ within a time bound $T$ by un-negligible probability $\varepsilon$, then there is another adversary $\mathcal{A}'$ who can succeed in existential forgery on $PKMR$, within expected time $T$ with un-negligible probability $\varepsilon/q_h$, where $q_h$ is the number of queries that $\mathcal{A}$ can ask to the random oracle $H'(.)$.

**Proof**: We show how to build an $\mathcal{A}'$ to forge a signature on $PKMR$ if there is an adversary $\mathcal{A}$ who can forge a valid signature on $IDMR$ via EF-ACMA.

Without loss of generality, we may assume that for any $ID$, $\mathcal{A}$ queries $H'(.)$ with $ID$ before $ID$ is used as (part of) an input of any query to $Extract(.)$ and $Sign(.)$.

From $\mathcal{A}$, we can construct adversary $\mathcal{A}'$ against $PKMR$ as follows:

1. A challenger $\mathcal{C}$ runs $(S_{ID}, (para, P_{ID} = Q)) \leftarrow KGen(1^\lambda)$, where $para = \{G_1, G_2, \hat{e}, q, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2\}$, and gives $(para, Q)$ to $\mathcal{A}'$.
2. $\mathcal{A}'$ sets $z = 1$, picks randomly $t, 1 \le t \le q_h$ and $x_i \in {Z_q}^*, i = 1, 2, ...q_h$.
3. $\mathcal{A}'$ runs $\mathcal{A}$ with input $para$. During the execution, $\mathcal{A}'$ simulates the following oracles which can be accessed by $\mathcal{A}$:
   - $H'(.)$: For input $ID$, $\mathcal{A}'$ checks if $H'(ID)$ is defined. If not, he defines $H'(ID) = \begin{cases} Q & z = t \\ x_i P & z \ne t \end{cases}$, and set $ID_z \leftarrow ID, z \leftarrow z + 1$. $\mathcal{A}'$ returns $H'(ID)$ to $\mathcal{A}$. $\mathcal{A}'$ records and keeps the tuples $(ID, H'(ID))$ in the $H' - list$.
   - $H_1(.)$: If $\mathcal{A}$ makes a query $\mu^r$ to random oracle $H_1(.)$, $\mathcal{A}'$ checks if $H_1(\mu^r)$ is defined. If not, it picks a random $\alpha \in \{0,1\}^{|q|}$, and sets $H_1(\mu^r) \leftarrow \alpha$. $\mathcal{A}'$ returns $\alpha$ to $\mathcal{A}$ and records $(\mu^r, \alpha)$ to the $H_1 - list$.
   - $F_1(.)$ and $F_2(.)$ queries: $\mathcal{A}$ can also query the random oracle $F_1(.)$ and $F_2(.)$ at any time. $\mathcal{A}'$ simulates the oracles $F_1(.)$ and $F_2(.)$ in the same way as the $H_1(.)$ oracle, keeping an $F_1 - list$ and $F_2 - list$ of tuples, respectively.
   - $Extract(.)$: For input $ID_i$, if $i = t$, then abort. Otherwise, $\mathcal{A}'$ computes $S_{ID_i} = x_i^{-1} \cdot P$ and lets $S_{ID_i}$ be the reply to $\mathcal{A}$.
   - $Sign(.)$: For input $ID_i$ and message $m$, if $i \ne t$, $\mathcal{A}'$ uses $S_{ID_i} = x_i^{-1} P$ as the private key to sign on $m$. Otherwise, $\mathcal{A}'$ simulates $ID_t$'s signing oracle with his own signing oracle $Sign'(.)$.

4. If $\mathcal{A}$ outputs $(ID_i, m, r_2, U)$ which satisfies $Verify(ID_i, m, (r_2, U)) = 1$, in addition, if $i = t$, then $\mathcal{A}'$ can get a forgery $(m, (r_2, U))$ on $PKMR$ corresponding to $(para, Q)$.

If $\mathcal{A}$ succeed in his attack, then $\mathcal{A}$ has not query to $Extract(.)$ with input $ID_t$. Hence the responses of $\mathcal{A}'$'s emulations are indistinguishable from $\mathcal{A}$'s real oracles. Because $t$ is chosen randomly, $\mathcal{A}'$ can output a forgery corresponding to $(para, Q)$ of $PKMS$ within expected time $T$ and with probability $\varepsilon/q_h$.

Let $\delta = \mu^{r_1}$, in the following lemma, we prove that the signature triples $(\delta, r_2, U)$ on $PKMR$ can be simulated without the knowledge of the signer's secret key, with an indistinguishable distribution probability.

**Lemma 2.** Give $para = \{G_1, G_2, \hat{e}, q, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2\}$ and an identity $ID$, $Q = P_{ID} = H(ID)P + P_{pub}$, $S_{ID} = (H(ID) + s)^{-1}P$, the following distributions are the same.

$$\sigma = \left\{ (\delta, r_2, U) \,\middle|\, \begin{array}{c} r_1 \in_R Z_q^* \\ r_2 \in_R Z, |r_2| \leq |q| \\ \delta = \mu^{r_1} \\ U = (r_1 + r_2) \cdot S_{ID} \end{array} \right\}, \quad \sigma' = \left\{ (\delta, r_2, U) \,\middle|\, \begin{array}{c} U \in_R G_1 \\ r_2 \in_R Z, |r_2| \leq |q| \\ \delta = \mu^{-r_2} \cdot \hat{e}(U, Q) \\ \delta \neq 1 \end{array} \right\}$$

**Proof:** First we choose a triple $(a, b, c)$ from the set of the signatures: $a \in G_2^*$, $b \in Z$ with $|b| \leq |q|$, $c \in G_1$ such that $a = \mu^{-b} \cdot \hat{e}(c, Q) \neq 1$. We then compute the probability of appearance of this triple following each distribution of probabilities:

$$\Pr_\sigma \left[ (\delta, r_2, U) = (a, b, c) \right] = \Pr_{r \neq 0} \begin{bmatrix} \mu_1^r = a \\ r_2 = b \\ (r_1 + r_2) \cdot S_{ID} = c \end{bmatrix} = \frac{1}{(q-1)2^{|q|}}.$$

$$\Pr_{\sigma'} \left[ (\delta, r_2, U) = (a, b, c) \right] = \Pr_{\alpha \neq 1} \begin{bmatrix} a = \alpha = \mu^{-r_2} \cdot \hat{e}(U, Q) \\ r_2 = b \\ U = c \end{bmatrix} = \frac{1}{(q-1)2^{|q|}}.$$

That is, we can construct a simulator $\mathcal{M}$, which produces triples $(\delta, r_2, U)$ with an identical distribution from those produced by the signer, as follows.

- **Simulator** $\mathcal{M}$: For input $\{G_1, G_2, \hat{e}, q, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2\}$ and $Q = H(ID)P + P_{pub}$ and a message $m \in \{0,1\}^{l_1}$,
  1. randomly chooses $U \in G_1$, $r_2 \in Z$ with $|r_2| \leq |q|$ , and computes

$\delta = \mu^{-r_2} \cdot \hat{e}(U, Q)$. In the (unlikely) situation where $\delta = 1$, we discard the results and restart the simulation.

2. returns the triple $(\delta, r_2, U)$.

**Theorem 1.** In the random oracle model, if there is an adversary $\mathcal{A}$ who performs, within a time bound $T$, an existential forgery on $IDMR$ with probability $\varepsilon \geq 10q_h(q_s+1)(q_{h_1}+q_s)/q$, where $q_h$, $q_{h_1}$ and $q_s$ are the number of queries that $\mathcal{A}$ can ask to the oracles $H(.)$, $H_1(.)$ and $Sign(.)$ respectively. Then there is a Turing machine $\mathcal{M}_1$ that can output $a^{-1}P$ on input of any given $P, aP \in G_1^*$ within expected time less than $120686 \cdot q_h \cdot q_{h_2} \cdot T/\varepsilon$.

**Proof**: With the Lemma 1, using adversary $\mathcal{A}$, we can construct another adversary $\mathcal{A}'$, given $(para, Q)$, who can produce a valid signature of $PKMR$, within expected time $T$ and with un-negligible probability $\varepsilon' = \varepsilon/q_h$. $PKMR$ is a generic signature scheme and the signature triples $(\delta, r_2, U)$ can be simulated without the knowledge of the signer's secret key and with an indistinguishable distribution probability (proved in Lemma 2). $\varepsilon' = \varepsilon/q_h \geq 10(q_s+1)(q_{h_2}+q_s)/q$. Hence, with the Forking Lemma, there is another machine $\mathcal{B}$ which has control over the machine obtained from $\mathcal{A}'$ replacing the signing oracle by simulation and produces two valid signatures $(m, \delta, r_2, U)$ and $(m, \delta, r_2', U')$ such that $r_2 \neq r_2'$ in expected time less than $120686 \cdot q_{h_2} \cdot T/\varepsilon' = 120686 \cdot q_h \cdot q_{h_2} \cdot T/\varepsilon$.

From the adversary $\mathcal{B}$, we can construct a Turing machine $\mathcal{M}_1$ such that $\mathcal{M}_1$ can output $a^{-1}P$ on input of any given $P, aP \in G_1^*$ as follows:

1. A challenger $\mathcal{C}$ generates $(G_1, G_2, q, \hat{e})$ and selects randomly $P, aP \in G_1$. $\mathcal{C}$ gives $(G_1, G_2, q, \hat{e}, P, aP)$ to $\mathcal{M}_1$ as inputs.
2. $\mathcal{M}_1$ selects randomly a $s \in Z_q{}^*$, sets $P_{pub} = sP$ and selects four hash functions $H, H_1, F_1, F_2$.
3. $\mathcal{M}_1$ runs $\mathcal{F}_2$ with input $(para = (G_1, G_2, q, \hat{e}, P, P_{pub}, \mu, H, H_1, F_1, F_2, l_1, l_2), aP)$ until $\mathcal{F}_2$ outputs two valid signatures $(m, \delta, r_2, U)$ and $(m, \delta, r_2', U')$ such that $r_2 \neq r_2'$.
4. $\mathcal{M}_1$ can computes and outputs $a^{-1}P$ as follows:

$$a^{-1}P = (r_2 - r_2')^{-1}(U - U')$$

**Theorem 2.** Suppose there is a Turing machine $\mathcal{M}_1$ that can output $a^{-1}P$ on input of any given $P, aP \in G_1^*$ with probability $\varepsilon$, in expected time bound $T$. Then there is a Turing machine $\mathcal{M}_2$ which outputs $abP$ on input of any given $P, aP, bP \in G_1^*$ with probability $\varepsilon^3$ in expected time $3T$.

**Proof.** From $\mathcal{M}_1$, we can construct a Turing machine $\mathcal{M}_2^*$ as follows:

1. $\mathcal{M}_2$'s input is $P, aP, bP \in G_1^*$.
2. $\mathcal{M}_2$ runs $\mathcal{M}_1$ with input $aP, P$ ($P$ can be used as $a^{-1}aP$). If $\mathcal{M}_1$ outputs $Y_1 = aaP = a^2P$, then goto the next step.
3. $\mathcal{M}_2$ runs $\mathcal{M}_1$ with input $bP, P = b^{-1}bP$. If $\mathcal{M}_1$ outputs $Y_2 = bbP = b^2P$, then goto the next step.
4. $\mathcal{M}_2$ runs $\mathcal{M}_1$ with input $(a+b)P, P = (a+b)^{-1}(a+b)P$. If $\mathcal{M}_1$ outputs $Y_3 = (a+b)^2P$, then goto the next step.
5. $\mathcal{M}_2$ computes and outputs $Y = 2^{-1}(Y_3 - Y_1 - Y_2)$.

Obviously, $Y = 2^{-1}(Y_3 - Y_1 - Y_2) = 2^{-1}(2abP) = abP$. Hence, in expected time $3T$, $\mathcal{M}_2$ can output $abP$ with success probability $\varepsilon^3$.

With Theorem 1 and Theorem 2, we can get the conclusion that the new ID-based signature scheme with message recovery is secure against EF-ACMA and ID-attack under the hardness assumption of CDH Problem in the random oracle model.

## 7 conclusion

This paper first shows a little revision to Zhang et al.'s scheme [13] in order to make their scheme correct and then presents an efficient ID-based signature scheme with message recovery. Our scheme is much more efficient than the previous scheme proposed by Zhang et al.. Our scheme can be regarded as an improvement of Barreto el al. 's signature scheme [2] since our scheme not only inherits the efficiency of their scheme but also reduce the total length of a message and the corresponding signature comparing to [2]. In addition, we prove that our scheme is secure against EF-ACMA and ID-attack in the random oracle under the CDH Assumption while [2] is proved secure under a stronger assumption.

## References


1. M. Abe and T. Okamoto, *A signature scheme with message recovery as secure as discrete logarithm*, Advances in cryptology –ASIACRYPT'99, Lecture Notes in Computer Science **1716**, pp.378–389, 1999.
2. P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. Quisquater, *Efficient and provably-secure identity-based signatures and signcryption from bilinear maps*, Advances in cryptology –ASIACRYPT'05, Lecture Notes in Computer Science **3778**, pp.515–532, 2005.
3. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology –CRYPTO'01, Lecture Notes in Computer Science **2139**, pp. 213–229, 2001.

4. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the weil pairing*, Advances in cryptology –ASIACRYPT'01, Lecture Notes in Computer Science **2248**, pp.514–533, 2001.
5. S. Goldwasser, S. Micali and R. L. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM Journal of Computing **17(2)**, pp.281–308, 1988.
6. A. Miyaji, *A message recovery signature scheme equivalent to DSA over elliptic curves*, Advances in cryptology –ASIACRYPT'96, Lecture Notes in Computer Science **1163**, pp.1–14, 1996.
7. K. Nyberg and R. A. Tuepple, *A new signature scheme based on the DSA giving message recovery*, Proceedings of the 1st ACM conference on communication and Computer security, pp.58–61, 1993
8. K. Nyberg and R. A. Ruepple, *Message recovery for signature schemes based on the discrete logarithm problem*, Advances in cryptology –EUROCRYPT'94, Lecture Notes in Computer Science **950**, pp.182–193, 1995.
9. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, **13(3)**, pp.361–396, 2000.
10. R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of the ACM, **21**, pp.120–126, 1978.
11. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in cryptology –CRYPTO'84, Lecture Notes in Computer Science **0196**, pp.47–53, 1984.
12. C. Y. Yeun, *Digital signature with message recovery and authenticated encryption (signcryption)- a comparison*, IMA - Crypto & Coding'99, Lecture Notes in Computer Science **1746**, pp.307–312, 1999.
13. F. Zhang, W. Susilo, and Y. Mu, *Identity-based partial message recovery signatures (or How to shorten ID-based signatures)*, FC'05, Lecture Notes in Computer Science **3570**, pp.45–56, 2005.