Efficient Identity-based Signature Scheme with Message Recovery

Salome James¹, P Vasudeva Reddy²
¹Department of Engineering Mathematics, Andhra University, Visakhapatnam, India; salomecrypto@gmail.com
²Department of Engineering Mathematics, Andhra University, Visakhapatnam, India; vasucrypto@andhrauniversity.edu.in

* Correspondence: vasucrypto@andhrauniversity.edu.in; Tel.: +91-988-500-0274.

Abstract. Digital signature is one of the important primitive of public-key cryptography and has become an essential technique in providing security services in modern communications. Due to the limitations imposed by both the communication bandwidth and computational power of wireless communication devices, signature schemes with less bandwidth and less computational cost are desirable for practical applications. Signature schemes with message recovery provide a feature that the message is recoverable from the signature and hence does not need to be transmitted separately for signature verification. Recently many signature schemes with message recovery have been designed in traditional as well as Identity based settings and most of the schemes are constructed using bilinear pairings over elliptic curves. Nevertheless, the computational cost of a pairing is more expensive and is higher than the scalar multiplication. Thus, signature schemes without pairing would be more appealing in terms of efficiency. In this paper, we propose an efficient identity-based message recovery scheme without pairings. In our scheme the message itself is not required to be transmitted together with the signature and so it turns out to have the least data size of communication cost. Also, we compare our scheme with the existing ID-based signature schemes with message recovery in terms of computational and communicational point of view. With the pairing-free realization, the proposed scheme is efficient and applicable for resource constrained devices.

Keywords: Digital signature; ID-based cryptography; Message Recovery; Elliptic Curve Discrete Logarithm Problem.

1. Introduction
A digital signature scheme with message recovery is a signature scheme in which the original message of the signature is not required to be transmitted together with the signature. In fact, the message is embedded in the signature and can be recovered during the verification / message recovery process. The advantage of these kind of signatures are to minimize the total length of the original message and the appended signature and so they are useful in an organization where bandwidth is one of the main concern or for the applications in which small messages should be signed.

The concept of Identity-Based Cryptography (IBC) was introduced by Shamir [1] in 1984, to simplify the key management problems in traditional cryptography. In IBC a user can directly generate his public key through his unique identity information and the corresponding private key is
generated by a Trusted third party (TTP) called Private key generator (PKG). With the advantage of IBC, many cryptographic schemes have been designed in identity-based setting.

In traditional PKC, Nyberg and Rueppel [2] in 1993 proposed the first message recovery signature scheme based on the DLP. Since 1993, many message recovery schemes have been proposed in the literature [3-9]. In 2005, Zhang et al. [10] designed the first message recovery and partial message recovery signature scheme for arbitrary length messages in the identity-based setting. This idea motivates a new direction to shorten signatures instead of proposing short signature schemes in identity based setting.

In addition to these schemes, Kalkan et al. [11], Tso et al. [12], Wang et al. [13] proposed signature schemes with message recovery in ID-based setting with pairings. Recently Salome et al. [14] proposed an ID-based signature scheme with message recovery on pairings. Also, some variants of message recovery signature schemes for specific applications have been proposed in literature [15, 16, 17]. However, all these ID-based message recovery schemes are based on bilinear pairings and the evaluation of pairing is very expensive.

In recent years, Elliptic Curve Cryptography (ECC) based schemes have become popular, since ECC provides high level security with smaller keys in size, which results less storage and low bandwidth. Hence the schemes without pairings would be more desirable to achieve high efficiency with the same level of security. In this regard, we focus on the design of new ID-based signature scheme with message recovery in pairing free environment.

In this paper, we propose an identity-based message recovery signature scheme without pairings. The proposed scheme does not use bilinear pairings over ECs, so that it improves greatly the computational and communicational efficiency than the existing ID-based message recovery signature schemes. This scheme has low computational cost and thus can be a good choice for computational constrained devices. The security of the proposed scheme is based on elliptic curve discrete logarithm problem (ECDLP) and is proven secure against existential forgery under adaptively chosen identity and message attacks in the random oracle model.

The organization of the rest of the paper is as follows. Section 2, gives a brief review of the background of elliptic curve group and mathematical preliminaries which are useful throughout this paper. In Section 3, we present the syntax and security model of the proposed scheme. In Section 4, we present our pairing-free ID-based signature scheme with message recovery. In Section 5, the security and the efficiency analysis of the proposed scheme are presented. Finally, we conclude the paper in Section 6.

2. Preliminaries

This section presents the descriptions of some preliminaries needed in our signature scheme.

2.1. Elliptic Curve Cryptography

Due to the computation, communication and security strength of ECC, plays a very important role in modern PKC [18, 19].

Let \( E_q(a,b) \) be a set of elliptic curve points over the prime field \( F_q \), defined by the non-singular elliptic curve equation: \( y^2 \equiv x^3 + ax + b \pmod{p} \) with \( a, b \in F_q \) and \( 4a^3 + 27b^2 \equiv 0 \pmod{p} \).

The additive elliptic curve group is defined as \( G_q = \{(x,y) : x, y \in F_q \} \cup \{ O \} \), where the point \( O \) is known as “point at infinity”. The order of the elliptic curve over \( F_q \) is \( o\left(E\left(F_q\right)\right) \) satisfies the relation \( 1-2\sqrt{q} \leq o\left(E\left(F_q\right)\right) \leq q+1 \). The scalar multiplication on the cyclic group \( G_q \) defined as \( kP = P + P + \cdots + P \) (\( k \) times). Here \( P \in G_q \) is the generator of order \( n \).
2.2. Computational Problems

- Given a random instance $P$, the generator of $G$ and $Q = aP$, where $a \in \mathbb{Z}_q^*$, the ECDLP is to find $a$ from $P$ and $Q$.
- The probability that any polynomial-time bounded algorithm $Adv_{ECDLP}$ can solve the ECDLP is defined as $Adv_{ECDLP}[G, q] = \text{Prob}\{ Adv(P, Q) = a \mid P, Q \in G_q \text{ and } Q = aP, a \in \mathbb{Z}_q^* \}$.

2.3. Notations

The following notations will be used throughout this paper.

| Notations | Meanings |
|-----------|----------|
| $E(F_q)$ | Group of points elliptic curve over $F_q$ |
| $k$ | Security parameter |
| $H_0, H_1, H_2, F_1, F_2$ | Cryptographic hash functions |
| $a \| b$ | Concatenation of two strings $a$ and $b$ |
| $\oplus$ | X-OR computation in the binary system |
| $[x]_{10}$ | Decimal representation of $x \in \{0, 1\}^*$ |
| $[y]_2$ | Binary representation of $y \in \mathbb{Z}$ |
| $l_2[\beta]$ | The first $l_2$ bits of $\beta$ from the left side |
| $l_1[\beta]$ | The first $l_1$ bits of $\beta$ from the right side |
| $\Omega$ | Signature on the message $m$ |

3. Syntax and security model of the proposed IBS-MR

In this section, we present the syntax and security model of the proposed scheme.

3.1. Syntax of IBS-MR

An ID-based signature scheme with message recovery, in short we denote it by IBS-MR, consists of the following four polynomial time algorithms:

- **System Setup.** For a given security parameter $k \in \mathbb{Z}^+$, the Private Key Generator (PKG) runs this algorithm and outputs the system parameters $\text{Params}$ and the master key $s$. $\text{Params}$ are made public and $s$ is kept secret. $\text{Params}$ are implicit input to all the following algorithms.
- **Key Extract.** For a given user’s identity $ID$, the PKG runs this algorithm to generate the public key and private key. PKG sends the private key to the corresponding user over a secure channel.
- **Signature Generation.** For a given signer’s identity $ID$ and a message $m \in \{0, 1\}^{l_1}$, the signer runs this algorithm and outputs a signature $\Omega$.
- **Message Recovery and Signature Verification.** For a given signer’s identity $ID$ and a signature $\Omega$, a verifier runs this algorithm to recover the message and check the validity of the signature $\Omega$, more precisely, the algorithm $\text{Verify}(ID, \Omega)$ and outputs “accept” if the signature is valid; or “reject”, otherwise.
3.2. Security model of IBS-MR

This section describes the security notion of IBS-MR namely, existential Unforgeability in the ROM under an adaptive chosen-message and an adaptive chosen-ID attack. To prove the security, we follow the security modal presented in [20]. We adopt the following game between a challenger $\xi$ and a forger $Adv$. A forger’s advantage $Adv_{IBS-MR, Adv}$ is defined as its probability of success in the game.

**Setup.** The challenger $\xi$ takes a security parameter $k$ and executes the setup algorithm of the IBS-MR to get the system Param. $\xi$ then gives params to $Adv$ and keeps the master secret key securely.

**Queries.** The forger $Adv$ asks the following queries to the challenger $\xi$.

- **Hash Queries.** When $Adv$ performs queries to the hash functions, the Challenger $\xi$ answers these queries with consistent and totally random values.

- **Extract Queries.** When $Adv$ requests the this query ID of its choice, the challenger $\xi$ runs the key extraction algorithm on ID and gives the output $d_{ID}$ to $Adv$.

- **Sign Queries:** When $Adv$ requests adaptively a signature on a given message $m$ with an identity ID, $\xi$ returns a signature $\Omega$.

**Output.** $Adv$ outputs $\left( m^*, ID^*, \Omega^* \right)$ as a forgery and succeeds the game if:

(i) $ID^*$ never asks the private key for ID with extraction oracle

(ii) $\Omega^*$ never gets as an answer from a sign query $(m, ID)$

(iii) $\Omega^*$ is a valid signature.

The advantage to win the above game by a PPT-bounded adversary $Adv$ with the help of $\xi$ is defined as $Adv_{Adv} = Pr[Adv succeeds]$.

**Definition 1.** An IBS-MR is secure against existential forgery under the adaptive chosen message attack (EF-ACMA) and identity attacks if there exists no probabilistic polynomial time adversary which has a non-negligible advantage in the above game.

4. Proposed pairing free IBS-MR scheme

This section presents our pairing free ID-based signature scheme with message recovery. This scheme deals with messages of fixed length. In the following we present the detailed functionalities of our proposed scheme.

**System Setup.** For a given $k \in \mathbb{Z}_q^+$, the PKG performs the following.

1. Choose a cyclic additive group $G$ of prime order $q$ with the points on an elliptic curve $E$ and $P$ as the generator of $G$.

2. Chooses $s \in \mathbb{Z}_q^*$ randomly and computes the system public key $P_{pub} = sP$.

3. Choose $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $F_1 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, $F_2 : \{0,1\}^{l_2} \rightarrow \{0,1\}^{l_1}$ as hash functions. $l_1$ and $l_2$ are positive integers such that $q = l_1 + l_2$.

4. KGC returns the system parameters as $Params = \{ E, G, q, P, P_{pub}, H_0, H_1, H_2, F_1, F_2, l_1, l_2 \}$.

5. KGC keeps params as public and the master key $<s>$ as secret.

**Key Extract.** For a given ID, the KGC runs this algorithm by choosing $r \in \mathbb{Z}_q^*$ and computes

$$R = rP;$$

$$h_0 = H_0 \left( ID, R, P_{pub} \right);$$
$$d = (r + sh_0) \mod q.$$ 

KGC returns $D = (d, R)$ to the user ID securely as private key.

**Signature Generation.** To sign a message $m \in \{0, 1\}^l$, this algorithm takes signer’s identity $ID$ and private key $D = (d, R)$ as input and performs the following.

1. Choose $t \in \mathbb{Z}_q^*$ and compute $U = tP, \ h_1 = H_1(ID, U), \ h_2 = H_2(ID, m, R)$. If gcd of $\left(\left(\left(t + h_1\right)^{-1} \cdot q\right)\right) = 1$ proceed, else choose another $t$.

2. Compute $\alpha = (t + h_1)^{-1} d \mod q$;
   $$\alpha = \left[\sigma(U + h_1P)\right]_X \in \{0, 1\}^{|d|},$$ where $(\cdot)_X$ denotes the X-coordinate of a point on the elliptic curve.

3. Compute $\beta = \left[F_1(m) \parallel F_2(F_1(m)) \oplus m\right]$; $v = [\alpha \oplus \beta]_0$ and $w = (h_2d + \beta)$.

4. Output the signature on the message $'m'$ as $\Omega = (R, v, w)$.

**Message Recovery and Signature Verification.** Given an identity ID and the corresponding signature $(R, v, w)$, in this algorithm, the verifier performs the following.

1. Compute $h_0 = H_0(ID, R, P_{pub})$;
   $$\tilde{\alpha} = \left[R + h_0P_{pub}\right]_X$$
   $$\tilde{\beta} = [v]_2 \oplus \tilde{\alpha}$$

2. Recover the message $\tilde{m} = \left[\tilde{\beta}\right]_1 \oplus F_2\left[l_2 \left[\tilde{\beta}\right]\right] = (m)$.

3. Accept the signature $\Omega$ as a valid signature on the message $\tilde{m} = m$ if the following conditions hold.
   (i) $l_2 \left[\tilde{\beta}\right] = F_1(\tilde{m})$;
   (ii) $wP = h_2 \left(R + h_0P_{pub}\right) + \tilde{\beta}P$, where $h_2 = H_2(ID, \tilde{m}, R)$ i.e., $wP = h_2 \left(R + h_0P_{pub}\right) + \beta P$.

5. Analysis of the proposed pairing free IBS-MR scheme

This section provides the proof of correctness, security analysis and efficiency analysis of the proposed IBS-MR scheme.

**5.1. Proof of correctness**

The correctness of the above scheme is as follows.

We can prove $\alpha = \tilde{\alpha}, \ \beta = \tilde{\beta}$ and $m = \tilde{m}$.

Consider
$$\tilde{\alpha} = \left[R + h_0P_{pub}\right]_X$$
$$= [rP + h_0sP]_X$$
$$= \left[(t + h_1)(t + h_1)^{-1}(r + h_0s)P\right]_X$$
$$= \left[(t + h_1)^{-1}(t + h_1)dP\right]_X$$
\[
\left( t + h_1 \right)^{-1} d \left( U + h_1 P \right) \]_X \\
= \left[ \sigma \left( U + h_1 P \right) \right]_X \\
= \alpha.
\]

Consider \( \tilde{\beta} = v \oplus \tilde{\alpha} \)
\[
= \left[ \alpha \oplus \beta \right] \oplus \tilde{\alpha} \\
= \beta \quad (\because \alpha = \tilde{\alpha}).
\]

Hence \( m = \left[ \tilde{\beta} \right]_{l_2} \oplus F_2 \left[ \tilde{\beta} \right]_{l_2} \)
\[
= \left[ \beta \right]_{l_2} \oplus F_2 \left[ \beta \right]_{l_2} \\
= F_2 \left( F_1 (m) \right) \oplus m \oplus F_2 \left( F_1 (m) \right) \\
= m \quad \text{and this holds iff} \quad F_1 (m) = \left[ \beta \right]_{l_2}.
\]

Also, it is clear that \( \omega = (h_2 d + \beta) P = \left[ h_2 \left( r + h_0 s \right) + \beta \right] P = h_2 \left( R + h_0 P_{\text{pub}} \right) + \beta P. \)

5.2. Security analysis

The security of a signature scheme is basically defined by the unforgeability against the adversary, as defined in Section 3.2, in the random oracle model. In the following theorem we discuss unforgeability of the proposed IBS-MR scheme.

**Theorem 1.** The proposed IBS-MR scheme is existentially unforgeable against the adaptive chosen message and identity attacks based on the infeasibility assumption of the ECDLP.

**Proof.** Let \( \xi \) be an ECDLP challenger and is given a random instance \( Q = sP \) of the ECDL problem in \( G \) for a randomly chosen \( s \in \mathbb{Z}_q^* \). Its goal is to compute \( s \). Let \( \text{Adv} \) is an adversary who interacts with \( \xi \) as described in 3.2. Now, we prove that \( \xi \) can solve the ECDLP using \( \text{Adv} \). During simulation process \( \xi \) needs to guess the target identity of \( \text{Adv} \). Without loss of generality, \( \xi \) takes \( ID^* \) as target identity of \( \text{Adv} \) on a message \( m \).

**Initialization Phase.** \( \xi \) runs the Setup algorithm and sets \( P_{\text{pub}} = Q = sP \) as public key and generates system parameters \( \text{params} \) and sends \( \text{params}, P_{\text{pub}} \) to \( \text{Adv} \).

**Queries Phase.** \( \text{Adv} \) can access the following oracle in an adaptive manner and the algorithm \( \xi \) responds to these oracles as follows.

- **Extraction oracle.** \( \xi \) maintains an initial-empty \( H_0 \)-oracle list \( L_0 \), which includes the tuples like \( \left( ID_i, R_i, P_{\text{pub}}, d_i, h_{0i} \right) \). When \( \text{Adv} \) makes this query on identity \( ID_i \), \( \xi \) looks for \( ID_i \) in the list \( L_0 \) and returns the output to \( \text{Adv} \) as follows.
  1. If \( ID_i = ID^* \), \( \xi \) aborts
  2. If \( ID_i \neq ID^* \), \( \xi \) selects \( a_i, b_i \in \mathbb{Z}_q^* \) and sets \( d_i = b_i, R_i = a_i P_{\text{pub}} + b_i P \) and \( h_{0i} = -a_i \). It is clear that \( \left( d_i, R_i \right) \) satisfies the equation \( d_i P = R_i + h_{0i} P_{\text{pub}} \). Then \( \xi \) outputs \( d_i \) as secret key of the user \( ID_i \) and incorporates the tuple \( \left( ID_i, R_i, P_{\text{pub}}, d_i, h_{0i} \right) \) to \( L_0 \) list and returns \( d_i \) to \( \text{Adv} \).
• Queries on oracle \( H_1 : H_1(ID_i, U_i) \). When \( Adv \) asks a \( H_1 \) query with the input \((ID_i, U_i)\), \( \xi \) then replies with previous value \( h_{i \xi} \in \mathbb{Z}_q^* \) if the tuple \((ID_i, U_i, h_{i \xi})\) is in \( L_1 \). Otherwise, \( \xi \) picks a random \( h_{i \xi} \in \mathbb{Z}_q^* \) and returns \( h_{i \xi} \) to \( Adv \) and adds \((ID_i, U_i, h_{i \xi})\) to the list \( L_1 \).

• Queries on oracle \( H_2 : H_2(ID_i, m_i, R_i) \). \( \xi \) maintains an initially empty list \( L_2 \) with tuples of the form \((ID_i, m_i, R_i, h_{2i})\). After receiving the query on \((ID_i, m_i, R_i)\), if a tuple \((ID_i, m_i, R_i, h_{2i})\) exists on \( L_2 \), \( \xi \) returns \( h_{2i} \in \mathbb{Z}_q^* \). Otherwise, \( \xi \) picks a random \( h_{2i} \in \mathbb{Z}_q^* \) and returns \( h_{2i} \). \( \xi \) adds \((ID_i, m_i, R_i, h_{2i})\) to \( L_2 \).

• Queries on \( F_1, F_2 \). \( \xi \) maintains two separate lists \( F_1\)-list, \( F_2\)-list, which are initially empty. If the queries are made earlier, then it returns the same answer. Otherwise, \( \xi \) picks random numbers from \( \{0,1\}^l \) and \( \{0,1\}^l \) respectively and returns to adversary. \( \xi \) stores these values in \( F_1, F_2 \) lists respectively.

• Signing oracle: When \( Adv \) makes this query on \((ID_i, m_i)\), \( \xi \) first makes queries on \( H_1, H_2, F_1, F_2 \) oracles and recovers the tuples \((ID_i, U_i, h_{i \xi}), (ID_i, m_i, R_i, h_{2i})\) from lists respectively. Then \( \xi \) generates the signature as follows.

Choose \( t_i \in \mathbb{Z}_q^* \) and sets \( U_i = t_i P \) and
\[
\hat{\alpha}_i = \left( (t_i + h_{i \xi})^{-1} d_i [U_i + h_{i \xi} P] \right)_X
\]
\[
\hat{\beta}_i = F_1(m_i) \left| F_2(F_1(m_i)) \right| m_i
\]
and \( w_i = h_{2i} d_i + \hat{\beta}_i \)

Finally, \( \xi \) responds to \( Adv \) with signature \( \Omega_i = (R_i, v_i, w_i) \).

Forgery. After forging a valid signature \( \Omega_i^* = (R_i^*, v_i^*, w_i^*) \) on the message \( m_i^* \) under the identity \( ID_i^* \) by \( Adv \), \( \xi \) recovers the corresponding tuples \((ID_i^*, U_i^*, h_{i \xi}^*)\), \((ID_i^*, m_i^*, R_i^*, h_{2i}^*)\) from \( L_1, L_2 \) lists. From the tuples, if \( ID_i^* \neq ID_i \) then \( \xi \) halts and fails. Otherwise, if \( ID_i^* = ID_i \), \( \xi \) computes the value of \( s \) as follows. From Forking Lemma [21], if we have a replay of \( \xi \) with same random tape but different choice of \( H_1, H_2, Adv \) will out put another signature \( \Omega_{i^*} = (R_{i^*}, v_{i^*}, w_{i^*}) \). This signature satisfies the verification equation.

By \( r_{i^*} \), \( s \), we now denote discrete logarithms of \( R_{i^*}, P_{Pub} \) respectively, that is \( R_{i^*} = r_{i^*} P, P_{Pub} = s P \).

As the signatures \( \Omega_i^* = (R_i^*, v_i^*, w_i^*) \), \( \Omega_{i^*}^* = (R_{i^*}, v_{i^*}, w_{i^*}) \) satisfy the verification equations, we get two linearly independent equations as below.
\[
w_{i^*}^{(j)} = h_{2i^*}^{(j)} (r_{i^*} + h_{2i^*}^{(j)} s) + \beta_{i^*}^{(j)} \text{ for } j = 1,2.
\]
\( \xi \) solves the unknown values \( r_{i^*}, s \) from the above two linear independent equations and outputs \( s \) as the solution of ECDLP. But, the ECDLP is computationally infeasible by any polynomial-time bounded algorithm. Therefore, based on the intractability assumption of ECDLP, our IBS-MR scheme is provable secure in the ROM against the adaptive chosen message and identity attacks.
5.3. Efficiency analysis of the proposed IBS-MR scheme

In this section, we analyze the performance of our IBS-MR scheme and then we compare our scheme with the related schemes in terms of computational cost point of view.

We consider the experimental results [22, 23, 24] to achieve the comparable security with 1024-bit RSA key, where the bilinear pairing (Tate pairing) is defined over the super singular elliptic curve 

\[ E_q : y^2 = x^3 + x \]

with embedding degree 2 and the 160-bit Solinas prime number \( q = 2^{159} + 2^{17} + 1 \) with 512-bit prime number \( p \) satisfying \( p + 1 = 12q \).

We consider the running time calculated for different cryptographic operations in [22, 23, 24] using MIRACL (Shamus software) [25], and implemented on a hardware platform PIV (Pentium-4) 3GHZ processor with 512-MB memory and a windows XP operating system. Furthermore, Chung et al. [26], indicated that the time to evaluate one elliptic curve scalar multiplication \( (T_{EM}) \) is approximately \( 29T_{ML} \) and the time needed for modular exponentiation \( (T_{EX}) \) is approximately \( 240T_{ML} \). It was also mentioned in [23] that the time needed to execute one pairing based scalar multiplication \( (T_{EM}) \) is approximately \( 6.38ms \), i.e. \( T_{EM} \approx 6.38ms \), the time needed for one bilinear pairing (Tate pairing) operation \( (T_{BP}) \) is approximately \( 20.01ms \) i.e. \( T_{BP} \approx 20.01ms \) and the time needed to execute one pairing-based exponentiation \( T_{PX} \) is approximately \( 11.20ms \) i.e. \( T_{PX} \approx 11.20ms \). Now from the works proposed in [24, 27] \( T_{BP} \approx 3T_{EM} \) and \( T_{PX} \approx (1/2)T_{BP} \). We summarize these computational results in Table 2.

### Table 2. Cryptographic operations and their conversions.

| Notations | Descriptions |
|-----------|--------------|
| \( T_{ML} \) | Modular multiplication |
| \( T_{EM} \) | Elliptic curve point multiplication (Scalar multiplication in \( G_1 \)) \( : T_{EM} \approx 29T_{ML} \) |
| \( T_{BP} \) | Bilinear pairing operation in \( G_2 \) \( : T_{BP} \approx 87T_{ML} \) |
| \( T_{PX} \) | Pairing-based exponentiation operation in \( G_2 \) \( : T_{PX} \approx 43.5T_{ML} \) |
| \( T_{EX} \) | Modular exponentiation in \( Z_q^* \) \( : T_{EX} \approx 240T_{ML} \) |
| \( T_{IN} \) | Modular inversion in \( Z_q^* \) \( : T_{IN} \approx 11.6T_{ML} \) |
| \( T_{MTP} \) | Map-to-point (hash function) \( : T_{MTP} \approx T_{EM} \approx 29T_{ML} \) |
| \( T_{PA} \) | Point addition of 2 elliptic curve points. (point addition in \( G_1 \)) \( : T_{PA} \approx 0.12T_{ML} \) |
We analyze the efficiency of our proposed Pairing-free IBS-MR scheme by comparing it with the existing schemes [10, 12, 13]. The comparison is summarized in Table 3. In Zhang et al. [10] scheme, for the signature generation, the signer needs to compute two scalar multiplications in $G_1$, one bilinear pairing operation in $G_2$, one pairing-based exponentiation operation in $G_2$ and one point addition in $G_1$. For the message recovery and verification, the verifier needs to compute two bilinear pairing operations in $G_2$ and one pairing-based exponentiation operation in $G_2$. So, the total computation cost for signing and verification of Zhang et al.’s [10] scheme is $406.12T_{ML}$. In Tso et al. [12] scheme, for the signature generation, the signer needs to compute one pairing-based exponentiation operation in $G_2$ and one scalar multiplication in $G_1$. For the message recovery and verification, the verifier needs to compute one bilinear pairing operation in $G_2$ and one pairing-based exponentiation operation in $G_2$ and one scalar multiplication in $G_1$. Therefore, the total computation cost for signing and verification of Tso et al.’s [12] scheme is $625T_{ML}$. In Wang et al. [13] scheme, for the signature generation, the signer needs to compute two pairing-based exponentiation operations in $G_2$. For the message recovery and verification, the verifier needs to compute two pairing-based exponentiation operations in $G_2$. Hence, the total computation cost for signing and verification of Wang et al.’s [13] scheme is $960T_{ML}$.

| Scheme               | Signing cost          | Verification cost       | Total cost       |
|----------------------|-----------------------|-------------------------|------------------|
| Zhang et.al. Scheme  | $2T_{EM} + T_{BP} + T_{PX} + T_{PA}$ | $2T_{BP} + T_{PX}$       | $406.12T_{ML}$   |
| Tso et.al. Scheme    | $1T_{EX} + T_{EM}$    | $1T_{BP} + T_{EX} + T_{EM}$ | $625T_{ML}$     |
| Wang et.al. Scheme   | $2T_{EX}$             | $2T_{EX}$               | $960T_{ML}$      |
| Our Proposed Scheme  | $3T_{EM} + T_{IN} + T_{PA}$ | $4T_{EM} + 2T_{PA}$     | $214.96T_{ML}$   |

Clearly from Table 3, in the signature generation of our proposed IBS-MR scheme, the signer needs to compute three scalar multiplications in $G_1$, one modular inversion operation in $Z_q^*$ and one point addition in $G_1$. In the message recovery and verification, the verifier needs to compute four scalar multiplications in $G_1$ and two point additions in $G_1$. Hence, the total computation cost for signing and verification of our proposed scheme is $214.96T_{ML}$, which is 52.54% of the Zhang et al. [10] scheme, 34.39% of Tso et al. [12] scheme, 22.39% of Wang et al. [13] scheme. Thus when compared to the existing message recovery schemes with pairings, the proposed scheme requires less computational cost.

6. Conclusion
In this paper, an identity-based message recovery scheme without pairings has been proposed. This scheme is capable of message recovery, so that the message does not need to be sent along with the signature, which saves storage and communication bandwidth. So, the proposed scheme doesn’t use bilinear pairing operations and hence requires less computational cost. With the running time being greatly saved, the proposed scheme is more practical than the pairing-based schemes for practical application. The proposed scheme is useful in communications, which require smaller bandwidth for signed messages, when compared with the same constructions except the message-recovery. Since the proposed scheme is identity-based, the user’s public key is easily extracted from his identification.
information. The correctness of the proposed scheme has been validated. The security of the proposed scheme is based on elliptic curve discrete logarithm problem (ECDLP) and is proven secure against existential forgery under adaptively chosen identity and message attack in the random oracle model. Finally, the proposed scheme is computationally efficient compared to the related schemes.

7. References

[1] Shamir A 1985 Identity-based cryptosystems and signature schemes Crypto ’84: Advances in Cryptology LNCS 196 (Santa Barbara CA USA) pp 47-53
[2] Nyberg K and Rueppel R A 1993 A new signature scheme based on the DSA giving message recovery CCS ’93: Proceedings of 1st ACM conference on communication and computer security (Fairfax Virginia USA) pp 58-61
[3] Abe M and Okamoto T 1999 A signature scheme with message recovery as secure as discrete logarithm ASIACRYPT’99: International Conference on the Theory and Application of Cryptology and Information Security LNCS (Singapore) pp 378-389
[4] Miyaji A 1996 A message recovery signature scheme equivalent to DSA over elliptic curves ASIACRYPT’96: International Conference on the Theory and Application of Cryptology and Information Security LNCS (Kyongju South Korea) pp 1-14
[5] Nyberg K and Rueppel R A 1995 A message recovery for signature schemes based on the discrete logarithm problem EUROCRYPT’94: Advances in Cryptology LNCS (Saint-Malo France) pp 182-193
[6] Yeun C Y 1999 Digital signature with message recovery and authenticated encryption (signcryption)- a comparison Cryptography and Coding ’99: Proceedings of IMA International Conference on Cryptography and Coding LNCS (Cirencester UK) pp 307-312
[7] Chen Y G and Jia C F 2008 Signature scheme with arbitrary length message recovery in CPK Proceedings of The 4th International Conference on Mobile Ad-hoc and Sensor Networks (Wuhan China) pp 55-58
[8] Li M and Fang T 2014 Provably secure and efficient ID-based strong designated verifier signature scheme with message recovery Proceeding of International Conference on Network-Based Information System (NBiS) (Salerno Italy) pp 287-293
[9] Kalkan S Kaya K and Selcuk A A 2008 Generalized ID-based blind signatures from bilinear pairings Proceedings of International Symposium on Computer and Information Sciences (Istanbul Turkey) pp 1-6
[10] Zhang F Susilo W and Mu Y 2005 Identity-based partial message recovery signaturen FC 2005: Proceedings of International Conference on Financial Cryptography LNCS (Roseau, Dominica) pp 45-56
[11] Kalkan S Kaya K and Selcuk A A 2007 Generalized ID-based ElGamal signatures Proceedings of International Symposium on Computer and Information Sciences (Ankara Turkey) pp 1-6
[12] Tso R Gu C Okamoto T and Okamoto E 2007 Efficient ID-based digital signatures with message recovery CANS 2007: Proceedings of International Conference on Cryptology and Network Security LNCS 4856 (Singapore) pp 47-59
[13] Wang X and Qian H 2011 A Novel ID-based Signature with Message Recovery from RSA Proceedings of International Conference on Electronic & Mechanical Engineering and Information Technology (Harbin Heilongjiang China) pp 4827-4831
[14] Salome J Gowri T Ramesh Babu G V and Vasudeva Reddy P 2017 Identity-based blind signature scheme with message recovery International Journal of Electrical and Computer Engineering vol 7(5) pp 2674-2682
[15] Hwang M S Chen S M Liu C Y 2016 Digital signature schemes with message recovery based on a discrete logarithm problem IETE Journal vol 62(3) pp 415-423
[16] Verma G K and Singh B B 2017 Efficient message recovery proxy blind signature scheme from pairings Trans Emerging Tel Tech (Wiley) vol 3167 pp 1-9
[17] Verma G K and Singh B B 2018 Efficient identity-based blind message recovery signature scheme from pairings IET Information Security vol 12(3) pp 150-156
[18] Miller V S 1985 Use of elliptic curves in cryptography *CRYPTO’85: Proceedings of Conference on the Theory and Application of Cryptographic Techniques* (Santa Barbara CA USA) pp 417-426
[19] Koblitz N 1987 Elliptic curve cryptosystem *Journal of Mathematics of Computation* vol 48(177) pp 203-209
[20] An J H Dodis Y and Rabin T 2002 On the security of joint signature and encryption *EUROCRYPT’02: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques* LNCS 2332 (Prague Czech Republic) pp 83-107
[21] Pointcheval D and Stern J 2000 Security arguments for digital signatures and blind signatures *Journal of Cryptology* vol 13(3) pp 361-396
[22] Ren K Lou W Zeng K and Moran P J 2007 On broadcast authentication in wireless sensor networks *IEEE Transaction on Wireless Communication* vol 6(11) pp 4136–4144
[23] Cao X Kou W and Du X 2010 A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges *Information Sciences* vol 180(15) pp 2895-2903
[24] Tan S H Heng S H and Goi B M 2010 Java implementation for Pairing-Based Cryptosystems *ICCSA’10: Proceedings of the International Conference on Computational Science and Its Applications* LNCS (Fukuoka Japan) pp 188-198
[25] Shamus Software Ltd. Miracl Library. Available: http://certivox.org/display/EXT/MIRACL
[26] Chung Y F Huang K H Lai F and Chen T S 2007 ID-based digital signature scheme on the elliptic curve cryptosystem *Computer Standards and Interfaces* vol 29(6) pp 601-604
[27] Barreto P S L M Libert B Mc Cullagh N Quisquater J 2005 Efficient and provably secure identity-based signatures and signcryption from bilinear maps *ASIACRYPT’05: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security* LNCS (Chennai India) pp 515-532