International Journal of Pure and Applied Mathematics
Volume 120 No. 5 2018, 1405-1422
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

New and Efficient ID-based Signature Scheme with Message Recovery using Bilinear Pairings over Elliptic Curves

Salome James, N.B.Gayathri, P. Vasudeva Reddy*

Department of Engineering Mathematics, Andhra University, Visakhapatnam, INDIA

*Corresponding Author: vasucrypto@andhrauniversity.edu.in.

Abstract:

Digital signature is one of the most important cryptographic primitive and has many practical applications in the real world. In many signature schemes, messages are to be transmitted together with signature and thus these schemes requires a large communicational cost for which they may be cannot efficiently used in some resource constrained devices such as WSNs, Mobile phones etc., where the less computation and low band width for communication are of great concern. In this paper, we design and analyze a new signature scheme with message recovery in the Identity based setting using bilinear pairings over elliptic curves. We discuss the proof of correctness and the security of the proposed scheme. Finally, we compare our scheme with the related schemes in terms of computational and communicational point of view.

***Keywords*:** digital signature, Id-based cryptography, message recovery, bilinear pairings, CDH problem.

1. Introduction

Digital signature is one of the most important cryptographic primitive, which can provide the data integrity, authentication and non-repudiation to digital communications and has many practical applications in the real world such as e-commerce, e-governance, e-voting etc,. Many signature schemes have been proposed in traditional and ID-based settings [18]. In many existing signature schemes, message is to be transmitted together with signature and thus these schemes requires a large communicational cost for which they may be cannot efficiently used in some special environments where low-communication and low-computation cost usually required. To solve this problem, signature scheme with message recovery technique is presented. In this these schemes, the original message of the signature is not required to be transmitted together with the signature. The message is embed in a

signature and can be recovered according to the verification/message recovery process. Hence, it results more bandwidth savings and has the advantage of small data size of communication.

Signatures with message recovery are useful for an organization where bandwidth is one of the main concerns. For e.g., in wireless devices such as cell phones, RFID chips and sensors, battery life is the main limitation. Communicating even one bit of data uses significantly more power than one 32-bit instruction. Reducing the number of bits to communicate saves power and is important to increase the battery life.

2. Related Work

The first signature scheme with message recovery was proposed by Nyberg and Rueppel [13] in 1993 based on the DLP. Since then several message recovery signature schemes have been proposed in the literature [17, 36, 35, 19, 1, 13, 14, 2]. The first ID-based signature scheme with message recovery was proposed by Zhang et al. in 2005 [7]. They also presented ID-based partial message recovery signature scheme for arbitrary length messages. Zhang et al. [7] idea gives a new direction to shorten ID-based signatures in contrast to proposing short signature schemes.

In additions to these schemes, Kalkan et al. [28, 29] proposed a generalized ID-based El Gamal signatures with message recovery. They also obtained new ID-based signatures with message recovery from this generalized scheme. Tso et al. [26] proposed two efficient ID-based digital signatures with message recovery based on Barreto et al. [24]. The first one deal with messages of fixed length and the second one deal with messages of arbitrary length. Wang et al. [33] proposed a Novel ID-based signature scheme with message recovery from RSA problem. Their scheme satisfies the existential unforgeability against adaptive chosen message and identity attacks in the random oracle model. Many variants of signature schemes with message recovery have been proposed to meet the various requirements for different applications [3, 10, 16, 20, 31, 8, 9]. These schemes can be implemented in resource constrained devices such as wireless sensor networks and vehicular ad-hoc networks to improve the communication efficiency [21, 22, 23, 25].

In order to improve the computational efficiency in ID-based signature with message recovery schemes, in this paper, a new and efficient ID-based Signature Scheme with Message Recovery (IBSSMR) is presented. The scheme is based on the bilinear pairings over elliptic curves and is designed for the messages of fixed length. The scheme is useful where the bandwidth is one of the crucial

concerns. The proposed scheme has existential unforgeability under an adaptive chosen-message and an adaptive chosen ID-attack with the assumption that the CDH problem is hard.

The organization of the rest of the paper is as follows. In section 2, mathematical preliminaries which are useful throughout the paper are provided. Section 3 presents the syntax and security model of the proposed scheme. In Section 4, our identity-based signature scheme with message recovery is proposed. In Section 5, the proof of correctness, security analysis and the efficiency analysis of the proposed scheme are presented. Finally, Section 6 concludes the paper.

3. Preliminaries

In this section, we will briefly discuss the basic concepts on bilinear pairings and some related mathematical problems.

3.1 Bilinear Pairings

It is an important cryptographic primitive and is widely adopted in many positive applications of cryptography. Let G_1 and G_2 are additive and multiplicative cyclic groups respectively of same prime order q with P as a generator of G_1. An admissible bilinear pairing is a map $\hat{e}$ defined by $\hat{e}: G_1 \times G_1 \to G_2$ satisfying the following properties:

1. Bilinearity: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-Degeneracy: There exists $P \in G_1$, such that $\hat{e}(P, P) \neq 1$.
3. Computability: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

For efficient implementation of pairing based schemes, Weil or Tate pairings on elliptic curves over finite fields have been considered [24].

3.2 Bilinear Pairings over Elliptic Curves

The modified Weil pairing and Tate pairing are admissible instantiations of bilinear pairings. The modified Weil pairing settings are briefly discussed below.

Let p be a sufficiently large prime that satisfies (1) $p \equiv 2 \bmod 3$; (2) $p = lq - 1$, where q is also a large prime. Let E be an elliptic curve defined by the equation $y^2 = x^3 + 1$ over F_p. Define $E(F_p)$ to be the group of points on E defined over F_p. Let $P \in E(F_p)$ be a point of order q and let G_1 be the subgroup of points generated by P. Set G_2 to be the subgroup of $F^*_{p^2}$ of order q. The

modified Weil pairing is thus defined by $\hat{e}: G_1 \times G_1 \to G_2$ satisfying the conditions of a bilinear pairing.

3.3 Map-to-Point Hash Function

Consider a hash function $H_1: \{0,1\}^* \to G_1^*$. It is sufficient to have a hash function $H_1: \{0,1\}^* \to A$ for some set A and an encoding function $L: A \to G_1^*$. In case of using modified Weil pairings, we have the set A is F_p, and the encoding function L is called Map-to-Point.

Again, let p be a prime satisfying $p \equiv 2 \bmod 3$ and $p = lq - 1$, where q is also prime. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$ over F_p.

Let G_1 be the subgroup of points on E of order q. Suppose we already have a hash function $H_1: \{0,1\}^* \to F_p$. Algorithm Map-to-Point works as follows on input $y_0 \in F_p$.

1. Compute $x_0 = \left(y_0^2 - 1\right)^{1/3} = \left(y_0^2 - 1\right)^{(2p-1)/3} \in F_p$.
2. Let $Q = (x_0, y_0) \in E(F_p)$ and set $Q_{ID} = lQ \in G_1$.
3. Output Map-to-Point $(y_0) = Q_{ID}$.

3.4 Computational Problems

Now, we give some computational problems which will form the basis of security for our scheme [6,12].

1. Discrete Logarithm Problem (DLP) : Given two group elements P and Q, find an integer n such that $Q = nP$ whenever such an integer exists.
2. Decisional Diffie-Hellman Problem (DDHP) : For $a,b,c \in_R Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.
3. Computational Diffie-Hellman Problem (CDHP) **:** For $a,b \in_R Z_q^*$, given P, aP, bP compute abP.

Throughout this paper, we assume that CDHP and DLP are intractable. When the DDHP is easy but the CDHP is hard on the group G, we call G, a *Gap Diffie-Hellman (GDH)* group. Such groups can be found on super singular elliptic curves or hyper elliptic curves over finite field and the bilinear pairings can be derived from the Weil or Tate pairing.

4. Syntax and Security Model of the Proposed IBBSSMR

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

4.1 Syntax of IBSSMR

An ID-based signature scheme with message recovery IBSSMR consists of four polynomial time algorithms: System Setup, Key Extract, Signature Generation, Signature Verification with Message Recovery. Here we present the detailed functionalities of these algorithms.

- System Setup: For a given security parameter $k \in Z^+$, the Key Generation Centre/Private Key Generator (KGC/PKG) runs this algorithm and generates the system parameters *Params* and the master key *s*. *Params* are made public and *s* is kept secret. *Params* are implicit input to all the following algorithms.
- Key Extract: For a given user's identity *ID*, the KGC runs this algorithm to generate the public key Q_{ID} and the private key d_{ID}. KGC sends d_{ID} to the corresponding user over a secure channel.
- Signature Generation: On input signer's identity *ID* and a message $M \in \{0, 1\}^{l_1}$, this algorithm outputs a signature σ.
- Signature Verification with Message Recovery: For a signer's identity *ID* and a signature σ, a verifier runs this algorithm to recover the message and check the validity of the signature σ, more precisely, the algorithm *Verify* (ID, σ) and outputs 1 if accepted, or 0 if rejected.

4.2 Security Model of IBSSMR

The most general security notion of a signature scheme is existential unforgeability under an adaptive chosen message attack (EUACMA). It is extended to an IBSSMR scheme, namely, existential unforgeability under an adaptive chosen-message and an adaptive chosen-ID attack.

4.2.1 Unforgeability of IBSSMR against an adaptive chosen message attack and an adaptive chosen-ID attack

In this model/game a forger can choose its messages and its identities adaptively. We give the forger the power to request private keys on identities of its choice. The forger is also given access to the signing oracle for any messages for desired identities. A forger's advantage $Adv_{IBSSMR, A}$ is defined as its probability of success in the following game between a challenger C and a forger A.

– Setup: The challenger C takes a security parameter *k* and runs the setup algorithm of the IBSSMR. It gives the *Params* to A and keeps the master secret with itself.
– Queries: The forger A adaptively makes different queries to the challenger C. Each query can be one of the following. All these queries can be made in an adaptive way; i.e. each query may depend on the answers obtained to the previous queries.

- Hash Queries: When the involved hash functions are modeled by random oracles. A also performs adaptive queries to the hash functions. The Challenger C answers these queries of the forger of this oracle, providing it with consistent and totally random values.
- Extract Queries: When A requests the private key of an identity *ID* of its choice, the challenger C runs the key extraction algorithm on ID and forwards the output d_{ID} to A.
- Sign Queries: When A requests adaptively a signature on a given message *M* with an identity ID, C returns a signature σ.

Output/Forgery:

Finally, A outputs a forged signature σ^* on M^* with identity ID^* as (M^*, ID^*, σ^*). The adversary wins the game if the following holds:

1. A did not make any extraction query on ID^*.
2. A did not make any sign query with
3. σ^* is a valid signature.

The advantage of A in the above game is defined as $Adv_{\mathrm{A}} = \Pr[\text{A succeeds}]$, where the probability is taken overall coin tosses made by C and A. We note that the above game captures the notion of strong unforgeability, introduced by An et al. [11].

Definition 1: An IBSSMR is said to be secure against existential forgery against adaptive chosen message attack (EF-ACMA) and identity attacks if no probabilistic polynomial time adversary has a non-negligible advantage in the above game.

5. Proposed ID-based Signature Scheme with Message Recovery

In this section, we present the concrete description of our ID-based signature scheme with message recovery (IBSSMR) using bilinear pairings. This scheme deals with messages of fixed length. As discussed in section 3.1, we present the detailed functionalities of our scheme in the following.

- **System Setup:** For a given security parameter $(1^k) \in Z^+$, the KGC runs this algorithm as follows.

1. Chooses two groups G_1, G_2 of same prime order $q \geq 2^k$ with a bilinear pairing $\hat{e}: G_1 \times G_1 \to G_2$; G_1 is an additive cyclic group with $P \in G_1$ as a generator and G_2 is a multiplicative cyclic group.
2. Selects $s \in Z_q^*$ randomly and computes the system public key $P_{pub} = sP$.

3. Chooses a map-to-point hash function $H_1 : \{0, 1\}^* \rightarrow G_1$ and three cryptographic hash functions $H_2 : \{0, 1\}^* \times G_2 \rightarrow \{0, 1\}^{l_1+l_2}$, $F_1 : \{0, 1\}^{l_1} \rightarrow \{0, 1\}^{l_2}$, $F_2 : \{0, 1\}^{l_2} \rightarrow \{0, 1\}^{l_1}$.
4. KGC publishes the system parameters as $Params = \{G_1, G_2, \hat{e}, q, P, P_{pub}, H_1, H_2, F_1, F_2\}$ as public and keeps the master key $< s >$ as secret.

- **Key Extract :**Given an user's identity *ID*, the KGC computes the corresponding private key $d_{ID} = sQ_{ID}$, where $Q_{ID} = H_1(ID)$ is the public key of the user. The private key should be sent to the user over a secure channel.
- **Signature Generation :** To sign on a message $M \in \{0, 1\}^{l_1}$, the signer with identity *ID* does the following:

1. Picks a random integer $r \in Z_q^*$ and computes $U = \hat{e}(P_{pub}, rQ_{ID})$.
2. Compute $\alpha = H_2(ID, U)$.
3. $\beta = F_1(M) \parallel (F_2(F_1(M)) \oplus M)$.
4. $h = [\alpha \oplus \beta]_{10}$.
5. $V = (r + h)\, d_{ID}$.

The signature on message *M* is $(h, V) \in Z_q^* \times G_1$ and is of length $|q| + |G_1|$.

- **Message Recovery and Signature Verification :** Given an identity *ID* and the signature (h, V), the signature can be verified by anyone and the message can be recovered as follows:

1. Compute $\alpha' = H_2(ID, \hat{e}(P, V)\, \hat{e}(P_{pub}, -hQ_{ID}))$.
2. Compute $\beta' = [h]_2 \oplus \alpha'$.
3. Recover the message $M' = |\beta'|_{l_1} \oplus F_2(_{l_2}|\beta'|)$.
4. Accept (h, V) as a valid signature and message $M'(= M)$ if and only if $F_1(M') = _{l_2}|\beta'|$.

6. Analysis of the Proposed IBSSMR

In this section, we provide the proof of correctness, security analysis and efficiency analysis of the proposed scheme.

6.1 Proof of Correctness

The correctness of the above scheme may be easily validated according to the following equation.

Consider

$$\begin{aligned}
&\hat{e}(P,\ V)\ \hat{e}(P_{pub},\ -hQ_{ID})\\
&=\hat{e}(P,\ (r+h)\ d_{ID})\ \hat{e}(P_{pub},\ -hQ_{ID})\\
&=\hat{e}(P,\ rd_{ID})\ \hat{e}(P,\ hd_{ID})\ \hat{e}(P_{pub},\ Q_{ID})^{-h}\\
&=\hat{e}(P_{pub},\ Q_{ID})^{r}\ \hat{e}(P_{pub},\ Q_{ID})^{h}\ \hat{e}(P_{pub},\ Q_{ID})^{-h}\\
&=\hat{e}(P_{pub},\ rQ_{ID})\\
&=U.
\end{aligned}$$

If $(h,\ V)$ is a valid signature, then $H_2(ID,\ U)=\alpha$ and $F_1(M)\ \|\ \left(F_2(F_1(M))\oplus M\right)=\beta=[h]_2\oplus\alpha.$

Hence we obtain,

$$|\beta|_{l_1}\oplus F_2({}_{l_2}|\beta|)=\ (F_2(F_1(M))\oplus M)\ \oplus\ F_2(F_1(M))=M.$$

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

6.2 Security Analysis

In the following, we prove that the proposed IBSSMR is secure against existential forgery on an adaptive chosen-message and ID attack in the random oracle model with the assumption that the CDH problem is intractable.

Theorem 1 **:** If the CDH problem is $(T',\ \varepsilon')$- hard, the scheme IBSSMR is $(T,\ q_{H_1},\ q_{H_2},\ q_{F_1},\ q_{F_2},\ q_E,\ q_S,\ \varepsilon)$- secure against existential forgery under adaptive chosen-message and ID attacks for any T and ε satisfying $\varepsilon\geq e(q_E+1)\ \varepsilon',\ T\leq T'-T_{EM}\ (q_{H_1}+q_E+2q_S),$ where e is the base of the natural logarithm, T_{EM} is the time for computing a scalar multiplication in $G_1.$ Also $q_{H_1},\ q_{H_2},\ q_{F_1},\ q_{F_2}$ denote the number of queries made to the hash oracle, q_E denotes the number of queries made to the key extract oracle and is q_S denotes the number of queries made to the sign oracle.

Proof: Suppose A is a forger who breaks the proposed IBSSMR. By using the forgery algorithm A , we will construct an algorithm B which outputs the CDH solution abP for a given CDH instance $(P,\ aP,\ bP)$ in $G_1.$ Algorithm B performs the following simulation by interacting with the forger A . Algorithm B simulates a real signer to get a valid signature from the forger A . If B does not fail this simulation, he/she gets a valid signature, and can solve the CDH problem.

Setup : Algorithm sets $P_{pub} = aP$ and starts by giving A the system parameters *Params* including P and P_{pub}.

At any time, A can query the random oracles H_1, H_2, F_1, F_2, Key Extract and Sign Queries. Without loss of generality, we assume that for any Extract Query, Sign Query involving an identity, a H_1 Query has previously been made on that identity. To respond these Queries, B does the following:

H_1- ***Queries*:** Algorithm B maintains a list of tuples (ID, x, y, w) referred as H_1 which is initially empty. When A queries the oracle that a point $ID \in \{0,1\}^*$, B responds as follows:

1. If the query *ID* already appears on the H_1-list in a tuple (ID, x, y, w) then B responds with $H_1(ID) = w \in G_1$.
2. Otherwise, B picks a random coin $y \in \{0, 1\}$, such that $pr[y = 0] = 1/(q_E + 1)$.
3. Algorithm B picks a random $x \in Z_q^*$,

   If y=0, B computes $w = x(bP) \in G_1$.

   If y=1, B computes $w = xP \in G_1$.
4. B adds the tuple (ID, x, y, w) to the H_1- list and responds to A with $H_1(ID) = w \in G_1$.

H_2- ***Queries* :** At any time A queries the oracle H_2 at (ID, U). To respond the query made by A to (ID, U), B maintains a list referred as H_2-list of tuples (ID, U, γ), which is initially empty and proceed as follows.

1. If the queried tuple (ID, U) already appears on the H_2-list in a tuple (ID, U, γ) then B responds with $H_2(ID, U) = \gamma \in Z_q^*$.
2. Otherwise, B picks a random $\gamma \in Z_q^*$, and adds the tuple (ID, U, γ) in the H_2-list and responds to A with $H_2(ID, U) = \gamma \in Z_q^*$.

$F_1(\cdot)$ and $F_2(\cdot)-$

Queries: A queries the random oracles $F_1(\cdot)$ and $F_2(\cdot)$ at any time. To respond the queries made by A to the oracles $F_1(\cdot)$ and $F_2(\cdot)$, B simulates the oracles $F_1(\cdot)$ and $F_2(\cdot)$ in the same manner as that of the $H_2(\cdot)$ oracle, by maintaining F_1- list and F_2- list of tuples respectively.

Key Extract Queries: When A queries the private key associated to *ID*, B first recovers the corresponding tuple (ID, x, y, w) from the H_1-list.

1. If y=0, then B output failure and halts.

2. Otherwise, B computes $d_{ID} = xP_{pub} = x(aP) \in G_1$ by using the tuple (ID, x, y, w) in the H_1- list and returns d_{ID} to A..

Sign Queries: When A queries a signature on a message *M* for an identity *ID*, B proceeds as follows:

1. Chooses a random integer $t \in Z_q^*$ and computes $U = \hat{e}(P_{pub}, t(xP))$.
2. Retrieves the H_2-list and sets $\gamma = H_2(ID, U)$.
3. Computes $\delta = F_1(M) \parallel F_2(F_1(M)) \oplus M)$ and $= [\gamma + \delta]_{10} \in Z_q^*$.
4. Also computes $V = (t + h')\, xP_{pub} \in G_1$.

Outputs the signature $\sigma = (h, V)$ as a signature on the message M.

All responses to sign queries are valid; indeed, the output σ of sign query is a valid signature on M under ID . To see this

$\hat{e}(P, V)\, \hat{e}(P_{pub}, -hQ_{ID})$
$= \hat{e}(P, (t+h)xP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID})$
$= \hat{e}(P, txP_{pub})\, \hat{e}(P, hxP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID})$

$= \hat{e}(P, x(aP))^t\, \hat{e}(P, x(aP))^h\, \hat{e}(P_{pub}, -hQ_{ID}$
$= \hat{e}(aP, t(xP))\hat{e}(P_{pub}, Q_{ID})^h\, \hat{e}(P_{pub}, Q_{ID})^{-h}$
$= \hat{e}(P_{pub}, t(xP))$
$= U$.

Output / Forgery: Finally, A outputs a tuple (h^*, V^*) as the forged signature on the message M^* for ID^* with non-negligible probability. If (h^*, V^*) is a valid signature, B recovers the tuple (ID^*, U^*, V^*) from the H_2-list, and then replaces A with the same random tape but with different choices of the hash function $H_2-$by exploiting the Forking technique [5]. On the message M^*, B gets another valid signature (h', V') such that $h' \neq h^*$ and $V' \neq V^*$.

We have

$$e\left(P, V^*\right) e\left(P_{pub}, Q_{ID^*}\right)^{-h^*} = U \qquad (1)$$

$$e\left(P, V'\right) e\left(P_{pub}, Q_{ID^*}\right)^{-h'} = U \qquad (2)$$

$$\Rightarrow e\left(P, V^* - V'\right) e\left(P_{pub}, Q_{ID^*}\right)^{-h^* + h'} = 1 \quad \Rightarrow e\left(P, V^* - V'\right) = e\left(P_{pub}, Q_{ID^*}\right)^{h^* - h'}$$

$$\Rightarrow e\left(P, V^* - V'\right) = e\left(P, xabP\right)^{h^* - h'}$$

$$\therefore V^* - V' = \left(h^* - h'\right) xabP \Rightarrow abP = \left(V^* - V'\right)\left[\left(h^* - h'\right)x\right]^{-1}.$$

This computes the description of B .

Hence B solves the given instance of the CDH problem as $abP = \left(V^* - V'\right)\left[\left(h^* - h'\right)x\right]^{-1}$ with probability at least ε' . For this, we analyze the following three events needed for B to succeed.

E_1 : B does not abort as a result of any of A′ssextract query.

E_2 : A generates a valid and non-trivial signature forgery σ on M^* .

E_3 : Event E_2 occurs and B does not quit the forgery phase.

The probability that B succeeds to solves the CDH problem is $\Pr[E_1 \wedge E_2 \wedge E_3]$.

The probability $\Pr[E_1 \wedge E_2 \wedge E_3]$ is decomposed as $\Pr[E_1 \wedge E_2 \wedge E_3] = \Pr[E_1].\Pr[E_2/E_1].\Pr[E_3/E_1 \wedge E_2]$ (3)

***Claim 1*:** The probability that algorithm B does not abort as a result of A′ssextract query is at least $\left[1-\left(1/(q_E+1)\right)\right]^{q_E}$. Since A makes at most q_E queries to the extract oracle and $\Pr[y=1]=\left[1-\left(1/(q_E+1)\right)\right]$,

we have $\Pr[E_1]=\left[1-\left(1/(q_E+1)\right)\right]^{q_E}$.

***Claim 2*:** If B does not abort as a result of A′ss extract query, then A′ss view is identical to its view in the real attack. Hence $\Pr[E_2/E_1] \geq \varepsilon$.

***Claim 3*:** The probability that B does not abort after A outputs a valid and non-trivial forgery is at least $1/(q_E+1)$. Algorithm B will abort only if A generates a forgery such that $y=1$. Hence, $\Pr[E_3/E_1 \wedge E_2] \geq 1/(q_E+1)$.

From equation (3), using the bounds of the claims, B produces the correct answer with probability at least $\left[1-\left(1/(q_E+1)\right)\right]^{q_E+1} . \varepsilon . \frac{1}{q_E+1} \geq \frac{1}{e}\frac{\varepsilon}{(q_E+1)} \geq \varepsilon'$

$\Rightarrow \varepsilon \geq e(q_E+1)\varepsilon'$.

Algorithm B′s running time is same as A′s running time plus the time it takes to respond to hash queries, q_E key extract queries and q_S sign queries, and the time to transform A′s final forgery into the CDH solution. From the above simulation we notice that there exists: $1T_{EM}$ operations in each H_1 query, $1T_{EM}$ operations in each key extraction query, $2T_{EM}$ operations in each signature query.

Hence, the total running time is at most $T \leq T' - T_{EM}(q_{H_1}+q_E+2q_S)$ as required. This completes the proof of Theorem 1.

6.3 Efficiency of the Proposed IBSSMR

In this section we analyze the performance of our scheme and then we compare it with the related schemes in terms of computational and communicational (signature length) cost point of view.

We consider the experimental results [32, 4, 15], to achieve the comparable security with 1024-bit RSA key, where the bilinear pairing (Tate pairing) is defined over the super singular elliptic curve $E/F_p : y^2 = x^3 + x$ with embedding degree 2 and the 160-bit Solinas prime number $q = 2^{159} + 2^{17} + 1$ with 512-bit prime number p satisfying $p+1 = 12qr$. In addition, we consider the running time calculated for different cryptographic operations in [32, 4, 15] using MIRACL [30], a standard cryptographic library 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. [34], indicate that the time needed to execute the elliptic curve scalar multiplication (T_{EM}) is approximately $29T_{ML}$, and the time needed to execute the modular exponentiation (T_{EX}) is approximately $240T_{ML}$. It was also mentioned in [4, 32] 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 to execute 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], $1T_{BP} \approx 3T_{EM}$ and $1T_{PX} \approx (1/2)T_{BP}$. We summarize these computational results in Table 1.

Table 1: Notations and descriptions of various cryptographic operations and their conversions

Notations	Descriptions
T_{ML}	Time needed to execute the modular multiplication operation
T_{EM}	Time needed to execute the elliptic curve point multiplication (Scalar multiplication in G_1) : $T_{EM} \approx 29T_{ML}$
T_{BP}	Time needed to execute the bilinear pairing operation in G_2 : $T_{BP} \approx 87T_{ML}$
T_{PX}	Time needed to execute the pairing-based exponentiation operation in G_2 : $T_{PX} \approx 43.5T_{ML}$
T_{EX}	Time needed to execute modular exponentiation operation in Z_q^* : $T_{EX} \approx 240T_{ML}$
T_{IN}	Time needed to execute modular inversion operation in Z_q^* : $T_{IN} \approx 11.6T_{ML}$
T_{MTP}	Time needed to execute a map-to-point (hash function): $T_{MTP} \approx T_{EM} \approx 29T_{ML}$
T_{PA}	Time needed to execute addition of 2 elliptic curve points. (point addition in G_1): $T_{PA} \approx 0.12T_{ML}$

We compare our scheme with Tso et al. [26] scheme and Zhang et al. [7] scheme. The comparison is summarized in Table 2.

From the security point of view, the proposed scheme does not uses the Forking lemma so that it provides tight security reduction to the CDH Problem.

From Table 2, it is clear that, the proposed scheme has equal length in signature size with Tso et al. [26] and Zhang et al. [7] schemes. So the proposed scheme is comparable with other schemes in terms of communicational point of view. Also, the computational cost for signing and verification of our scheme requires only $348\ T_{ML}$ and is less than the computational in Tso et al. [26] and Zhang et al. [7] schemes. Therefore, compared with the Tso et al. [26] and Zhang et al. [7] schemes, our scheme is efficient in computational point of view.

Table 2: Efficiency comparison of our Scheme with related schemes

Scheme	Signature length (bits)	Signing cost	Verification cost	Total cost
Tso et al. [26]	$\|q\|+\|G_1\|$	$1T_{EX}+1T_{EM}$	$1T_{BP}+1T_{EX}+1T_{EM}$	$\approx 625\ T_{ML}$
Zhang et al. [7]	$\|q\|+\|G_1\|$	$2T_{EM}+1T_{BP}+1T_{PX}+1T_{PA}$	$2T_{BP}+1T_{PX}$	$\approx 406.12T_{ML}$
Our scheme	$\|q\|+\|G_1\|$	$2T_{EM}+1T_{BP}$	$2T_{BP}+1T_{EM}$	$\approx 348\ T_{ML}$

7. Conclusions

In this paper, we proposed an identity-based signature scheme with message using bilinear pairings over elliptic curves. This scheme designed for the messages of fixed length. We proved that the IBSSMR scheme is provable secure with the assumption that the CDH problem is hard. The efficiency analysis shows that our IBSSMR scheme is efficient in terms of computational and communicational point of view. Hence, the proposed scheme can be use efficiently used in some resource constrained devices such as authentication in cell phones and wireless sensor devices where band width is one of the main concerns.

References

[1] A. Miyaji, “A Message Recovery Signature Scheme equivalent to DSA over Elliptic Curves,” ASIACRYPT 1996, LNCS, Springer, Heidelberg, Vol. 1163, pp. 1-14, 1996.

[2] C. Y. Yeun, “Digital Signature with Message Recovery and Authenticated Encryption (signcryption)- a comparison,” In: Walker, M. (ed.) Cryptography and Coding, LNCS, Springer, Heidelberg, Vol. 1746, pp. 307-312, 1999.

[3] C. Zhou, "An Improved ID-based Proxy Signature Scheme with Message Recovery," International Journal of Security and Its Applications, Vol. 9, No. 9, pp.151-164, 2015.

[4] D. He, J. Chen, J. Hu, "An ID-based proxy signature scheme without bilinear pairings," Ann. of Telecommunication, Vol. 66, pp. 657–662, 2011.

[5] D. Pointcheval, J. Stern, "Security arguments for digital signatures and blind signatures," Journal of Cryptology, Vol. 13, No. 3, pp. 361-396, 2000.

[6] E. J. Goh, S. Jarecki, "A Signature Scheme as Secure as the Diffie-Hellman Problem," EUROCRYPT'03, LNCS 2656, pp. 401-415, 2003.

[7] F. Zhang, W. Susilo, Y. Mu, "Identity-Based Partial Message Recovery Signatures," In Financial Cryptography '05, LNCS, Vol. 3570, pp. 45-56, 2005.

[8] G. K. Verma, B. B. Singh, "Efficient identity-based blind message recovery signature scheme from pairings," IET Information Security, vol. 12, Issue. 2, pp. 150-156, 2018.

[9] G. K. Verma, B. B. Singh, H. Singh, "Provably Secure Message Recovery Proxy Signature Scheme for Wireless Sensor Networks in e-Healthcare," Wireless Personal Communications, vol. 99, Issue.1, pp. 539-554, 2018.

[10] H. Singh, G. K. Verma, "ID-based proxy signature scheme with message recovery," The Journal of Systems and Software, Vol. 85, No. 1, pp. 209–214, 2012.

[11] J. H. An, Y. Dodis, T. Rabin, "On The Security of Joint Signature and Encryption," Advances in Cryptology, LNCS 2332, Springer-Verlag, pp. 83-107, 2002.

[12] J. Katz, N. Wang, "Efficiency Improvements for Signature Schemes with Tight Security Reductions," 10th ACM Conference on Computer and Communications Security, pp. 155-164, 2003.

[13] K. Nyberg, R. A. Rueppel, "A New Signature Scheme based on the DSA giving Message Recovery," In Proceedings of 1st ACM conference on communication and computer security, pp. 58-61, 1993.

[14] K. Nyberg, R. A. Ruepple, "A Message Recovery for Signature Schemes based on the Discrete Logarithm Problem," In: De Santis, A. (ed.) EUROCRYPT 1994, LNCS, Springer, Heidelberg, Vol. 950, pp. 182-193, 1995.

[15] K. Ren, W. Lou, K. Zeng, P. J. Moran, "On broadcast authentication inwireless sensor networks," IEEE Transaction on Wireless Communication, Vol. 6, No. 11, pp. 4136–4144, 2007.

[16] L. Diao, J. Gu, I-L. Yen, "A New Proxy Blind Signature Scheme with Message Recovery," Information Technology Journal, Vol. 12, No. 21, pp. 6159-6163, 2013.

[17] M. Abe, T. Okamoto, "A Signature Scheme with Message Recovery as Secure as Discrete Logarithm," ASIACRYPT 1999, LNCS, Springer, Heidelberg, Vol. 1716, pp. 378-389, 1999.

[18] M. C. Gorantla, R. Gangishetti, A. Saxena, "A survey on ID-based cryptographic primitives," In IACR Cryptology ePrint Archive, 2005, Report 2005/094, Available at http://eprint.iacr.org/2005/094.

[19] M. Li, "Provably Secure and Efficient ID-Based Strong Designated Verifier Signature Scheme with Message Recovery," TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol. 12, No. 10, pp. 7343-7352, 2014.

[20] M. Li, T. Fang, "Provably Secure and Efficient ID-based Strong Designated Verifier Signature Scheme with Message Recovery," 17th International Conference on Network-Based Information Systems (NBIS), 2014.

[21] M. Saberi, "Private and Mobile Inter-Network Routing for Wireless Sensor Networks and Internet of Things," International Journal of Communication Networks and Information Security (IJCNIS), vol. 10,no.1, pp.131-138, 2018.

[22] N. B. Gayathri, T. Gowri, R.R.V. Krishna Rao, P. Vasudeva Reddy, "Efficient and Secure Pairing-free Certificateless Directed Signature Scheme," Journal of King Saud University- Computer and Information Sciences, Article in Press, 2018.

[23] N.B. Gayathri, R.R.V. Krishna Rao, P. Vasudeva Reddy, "Efficient and Provably Secure Pairing FreeID-Based Directed Signature Scheme," In: S.M. Thampi et al. (Eds.): SSCC 2017, CCIS 746, pp. 28–38, 2017.

[24] P. S. L. M. Barreto, B. Libert, N. McCullagh, J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," In Proc. of ASIACRYPT'05, Vol. 3778 of LNCS, pp. 515-532, 2005.

[25] R. Al-Mutiri, M. Al-Rodhaan, Y. Tian, "Improving Vehicular Authentication in VANET using Cryptography," International Journal of Communication Networks and Information Security (IJCNIS), vol. 10,no.1, pp.248-255, 2018.

[26] R. Tso, C. Gu, T. Okamoto, E. Okamoto, "Efficient ID-based Digital Signatures with Message Recovery," F. Bao et al. (Eds.): CANS 2007, LNCS 4856, pp. 47-59, 2007.

[27] S. H. Tan, S. H. Heng, B. M. Goi, "Java Implementation for Pairing-Based Cryptosystems," Proceedings of the International Conference in Computational Science and Its Applications (ICCSA'10), LNCS 6019, Springer-Verlag, pp. 188-198, 2010.

[28] S. Kalkan, K. Kaya, A. A. Selcuk, "Generalized ID-based Blind Signatures from Bilinear Pairings," In the 23rd International symposium on Computer and Information Sciences (ISCIS 2008), 2008.

[29] S. Kalkan, K. Kaya, A. A. Selcuk, "Generalized ID-based ElGamal Signatures," In the 22nd International Symposium on Computer and Information Sciences (ISCIS 2007), 2007.

[30] Shamus Software Ltd. Miracl Library, Available: http://certivox.org/display/EXT/MIRACL.

[31] X. Hu, H. Xu, Y. Liu, J. Wang, W. Tan, X. Zhang, "An efficient designated verifier signature scheme with pairing-free and low cost," Security and Communication Networks, Published online in Wiley Online Library, 2017.

[32] X. Cao, W. Kou, X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," Information Sciences, Vol. 180, No. 15, pp. 2895-2903, 2010.

[33] X. Wang, H. Qian, "A Novel ID-based Signature with Message Recovery from RSA," International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT), 2011.

[34] Y. F. Chung, K. H. Huang, F. Lai, T. S. Chen, "ID-based digital signature scheme on the elliptic curve cryptosystem," Computer Standards and Interfaces, Vol. 29, No. 6, pp. 601-604, 2007.

[35] Y. Li, H. Chen, "Efficient Identity-Based Signature Scheme with Partial Message Recovery," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2007.

[36] Y.G. Chen, C. F Jia, "Signature Scheme with Arbitrary Length Message Recovery in CPK," The 4th International Conference on Mobile Ad-hoc and Sensor Networks, 2008.