International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 5, October 2017, pp. 2674~2682
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i5.pp2674-2682

Identity-Based Blind Signature Scheme with Message Recovery

Salome James[1], T. Gowri[2], G.V. Ramesh Babu[3], P. Vasudeva Reddy[4]
[1,4]Department of Engineering Mathematics, Andhra University, Visakhapatnam, India.
[2]Department of ECE, GIT, GITAM University, Visakhapatnam, India.
[3]Department of Computer Science, S. V.University, Tirupati, India.

Article Info

Article history:

Received Dec 10, 2016
Revised Apr 25, 2017
Accepted Jun 11, 2017

Keywords:

Bilinear pairings
Blind signature
Cdh problem
Id-based cryptography
Message recovery

ABSTRACT

Blind signature allows a user to obtain a signature on a message without revealing anything about the message to the signer. Blind signatures play an important role in many real world applications such as e-voting, e-cash system where anonymity is of great concern. Due to the rapid growth in popularity of both wireless communications and mobile devices, the design of secure schemes with low-bandwidth capability is an important research issue. In this paper, we present a new blind signature scheme with message recovery in the ID-based setting using bilinear pairings over elliptic curves. The proposed scheme is unforgeable with the assumption that the Computational Diffie-Hellman problem is hard. We compare our scheme with the related schemes in terms of computational and communicational point of view.

Corresponding Author:

P. Vasudeva Reddy,
Department of Engineering Mathematics,
Andhra University,
Visakhapatnam, A.P. Indida.
Email: vasucrypto@yahoo.com, vasucrypto.engmath@auvsp.edu.in

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 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 embedded message can be recovered by anyone without the secret information. The purpose of this kind of signatures is to minimize the total length of the original message and the appended signature. So, these are useful in any organization where bandwidth is one of the main concern or for the application in which small message should be signed.

Blind signature scheme was introduced by Chaum [1] in 1982 to provide the anonymity of the user and plays a central role in cryptographic protocols such as e-voting, e-payment[2], [3]. Such a signature allows a user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. The scheme can ensure untraceability and unlinkability.

With the advantages of ID-based cryptography, several ID-based signature schemes and and their variants have been proposed in the literature [2]-[4]. The first ID-based blind signature scheme was proposed by Zhang and Kim [5] in Asiacrypt 2002. Later, in 2003, Zhang and Kim [6] proposed a new ID-based blind signature scheme based on bilinear pairings. In 2005, Huang et al. [7] proposed ID-based blind signature schemes using bilinear pairings and showed that the schemes are not secure if the ROS problem is solvable. In 2006, Zhao et al. [8] presented another blind signature scheme is efficient than Zhang and Kim's schemes [5], [6]. A generalized ID-based blind signature from bilinear pairings was proposed in 2007 by Kalkan et al. [9]. An ID-based authenticated blind signature scheme from bilinear pairings was proposed by Zhao et al. in 2007 [10]. In 2010, B.U. Rao et al. [11] proposed ID-based blind signature schemes from

bilinear pairings and is efficient than the previous ID-based blind signature shames. In 2013 Xu et al. [12] proposed and ID-based blind signature scheme with unlinkability. In 2014, Pance et al. [13] proposed a comparison of ID-based blind signatures from pairings for e-voting protocols.

A blind signature with message recovery is important in communication which requires the smaller bandwidth for signed messages than signatures without message-recovery. In 2005, Han et al. [14] proposed a pairing-based blind signature scheme with message recovery based on modified Weil/ Tate pairings over elliptic curves. This scheme needs smaller bandwidth and improves the communication efficiency than other previous ID-based blind signatures. Also this scheme provides high security with smaller keys in size. In 2009, Wang et al. [15] proposed optimal blind signature padding with message recovery. This scheme uses an ideal cipher with a smaller block size to design a secure two-move blind signature with an optimal padding. Their scheme has the message recovery property with less bandwidth. Zhang et al. [16] proposed a kind of message-recoverable fairness blind digital signature scheme in 2011. ID-based blind signature schemes with message recovery schemes are also proposed [17]-[19]. In 2005, Han et al. [13] proposed a pairing-based blind signature with message recovery. In 2006, Hassan et al. [17] proposed a new blind ID-based signature scheme with message recovery which improves the computational efficiency in the Han et al. scheme [14]. It achieves bandwidth savings and is suitable for signing short messages.

In this paper, by considering the above advantages, we designed a new blind signature scheme with message recovery in the identity-based setting. The proposed IBBSSMR 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 anonymity of the users and bandwidth constraints are of great concern. The proposed scheme is unforgeable with the assumption that the Computational Diffie-Hellman problem is hard.

The rest of the paper is organized as follows. In section 2, mathematical preliminaries are provided. Section 3 presents the syntax and security model of the proposed IBBSSMR scheme. In Section 4, an identity-based blind 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.

2. PRELIMINARIES

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

2.1. Bilinear Pairings

It is an important cryptographic primitive and is widely adopted in many positive applications of cryptography. Let $(G_1,+)$ and $(G_2, .)$ be two cyclic groups of same prime order *q*. Let *P* be a generator of G_1. A 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 $P, Q \in G_1$.

Such a pairing $\hat{e}$ is called an admissible pairing and can be constructed by the modified Weil or Tate pairings on elliptic curves defined over a finite field.

2.2. 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. Let p be a sufficiently large prime such that $p \equiv 2 \bmod 3$ and $p = lq - 1$, 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 over F_p. Let $P \in E(F_p)$ be a point of order q and G_1 be the subgroup of points generated by P. Let G_2 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.

2.3. 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 $L: A \to G_1^*$. 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 $H_1:\{0,1\}^* \to F_p$. A Map-to-Point algorithm 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 $(y_0) = Q_{ID}$.

2.4. Computational Problems

This section presents some computational problems which will form the basis of security for our IBBSSMR scheme.

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.

3. SYNTAX AND SECURITY OF THE PROPOSED IBBSSMR SCHEME

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

3.1. Syntax of IBBSSMR

Our blind signature scheme with message recovery is an extension of ordinary blind signature scheme. This scheme consists of the following four algorithms: System Setup, Key Extract, Blind Signature Generation, Blind Signature Verification with Message Recovery. The detailed description of these algorithms is described.

1. System Setup: For a given security parameter $k \in Z^+$, the Key Generation Centre (KGC) run 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.
2. 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 through a secure channel.
3. Blind Signature Generation: This is an interactive and probabilistic polynomial time protocol, which is operated by the user and the signer. The user first blinds the message M and obtains a new version $\tilde{h}$ of M, and then sends it to the signer. The signer uses his/her private key to sign on $\tilde{h}$ and obtains $\tilde{V}$, and then sends it to the user. The user unblinds it to obtain V, which is a blind signature on the original M.
4. Blind Signature Verification with Message Recovery: For a signer's identity *ID* and a blind signature σ, a verifier runs this algorithm to recover the message and check the validity of the blind signature σ, more precisely, the algorithm *Verify* (*ID*, σ) outputs 1 if accepted, or 0 if rejected.

3.2. Security Requirements of the Proposed IBBSSMR

A secure blind signature scheme must satisfy the following requirements:

1. Correctness: If the user and the signer, both comply with the algorithm of blind signature generation, then the blind signature V will always be accepted. The correctness of the

signature of a message signed through the signature scheme can be checked by anyone using the signer's public key.

2. Blindness : A signature is said to be blind if a given message-signature pair and the signer's view are statistically independent. While correctly operating one instance of the blind signature scheme, let the output be (M, V) (i.e, message-signature pair) and the view of the protocol V'. At a later time, the signer is not able to link V' to (M, V). The content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.
3. Unforgeability : It is with respect to the user especially, i.e. the user is not able to forge blind signatures which are accepted by the algorithm of verification of blind signatures. Only the signer can give a valid signature for the associated message.

4. PROPOSED ID-BASED BLIND SIGNATURE SCHEME WITH MESSAGE RECOVERY

In this section, we present our ID-based blind signature scheme with message recovery (IBBBSSMR) scheme. As discussed in Section 3.1, the detailed functionalities of these algorithms are presented.

1. System Setup: For a given security parameter $k \in Z^+$, the KGC runs this algorithm as follows. Chooses two groups G_1, G_2 of same prime order $q \geq 2^k$ with a bilinear pairing $\hat{e}: G_1 \times G_1 \rightarrow G_2$; G_1 is an additive cyclic group with $P \in G_1$ as a generator and G_2 is a multiplicative cyclic group.
   a. Selects $s \in Z_q^*$ randomly and computes the system public key $P_{pub} = sP$.
   b. Chooses a map-to-point hash function $H_1: \{0, 1\}^* \rightarrow G_1$ and three cryptographic hash functions $H_2: \{0, 1\}^* \times G_2 \rightarrow \{0, 1\}^{l_1+l_2}$, $F_1: \{0, 1\}^{l_1} \rightarrow \{0, 1\}^{l_2}$, $F_2: \{0, 1\}^{l_2} \rightarrow \{0, 1\}^{l_1}$.
   c. Now 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.
2. 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 and then sends it to the corresponding user ID through a secure channel.
3. Blind Signature Generation : In order to sign a message $M \in \{0, 1\}^{l_1}$ blindly by a signer, whose identity is ID; the user and the signer should run the blind signature protocol.

   [Blind Signature Issuing Protocol]

   Suppose that M is the message to be signed. The blind signature protocol is shown in Figure 1.
   a. The signer randomly chooses a number $r \in Z_q^*$, computes $X = rd_{ID}$ and sends X to the user as a commitment.
   b. (Blinding) The user randomly chooses $a, b \in Z_q^*$ as blinding factors. The user computes

      $U = \hat{e}\ (aP_{pub} + bX, P)$.

      $\alpha = H_2(ID, U)$, $\beta = F_1(M) \parallel (F_2(F_1(M)) \oplus M)$.

      $h = [\alpha \oplus \beta]_{10}$.

      $\tilde{h} = b^{-1}h \bmod q$ and sends $\tilde{h}$ to the signer.
   c. (Signing) The signer sends back $\tilde{V} = X + \tilde{h}d_{ID}$.
   d. (Unblinding) The user computes $V = b\tilde{V} + aP_{pub}$.

      The user outputs (h, V) as the blind signature on the message M.

User Signer

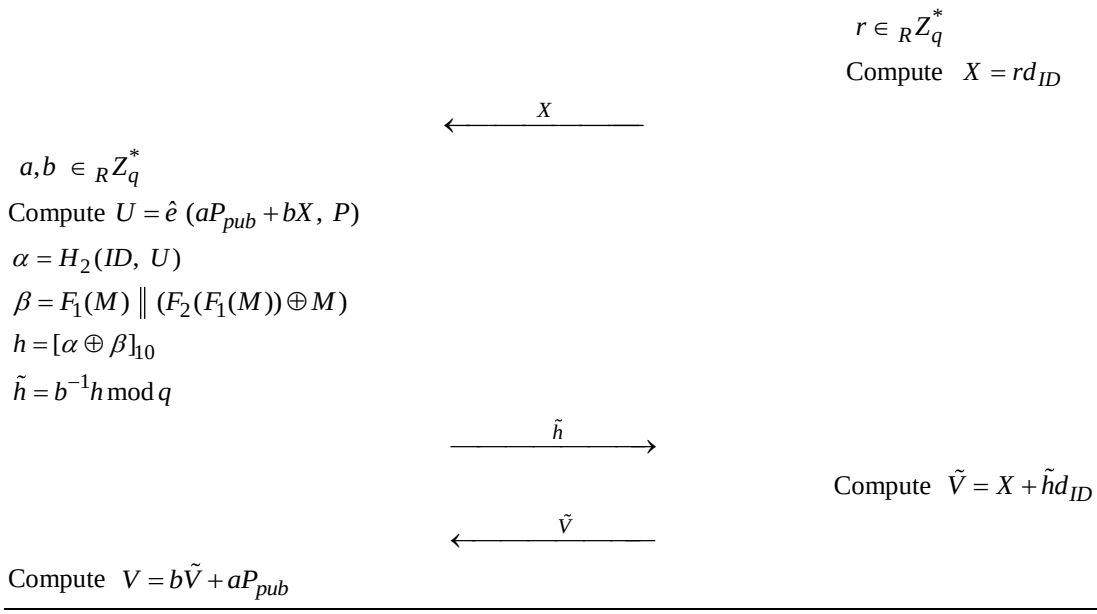

Figure 1. The blind signature issuing protocol

4. Blind Signature Verification : Given ID and the signature (h, V), any one can verify the signature and recover the message as follows:
   a. Compute $\alpha' = H_2\left(ID, \hat{e}(P, V)\, \hat{e}(P_{pub}, -hQ_{ID})\right)$.
   b. Compute $\beta' = [h]_2 \oplus \alpha'$.
   c. Recover the message as $\tilde{h} = |\beta'|_{l_1} \oplus F_2({}_{l_2}|\beta'|)$.
   d. Accept (h, V) as a valid signature on the message $\tilde{h}(= M)$ if and only if $F_1(\tilde{h}) = {}_{l_2}|\beta'|$.

5. ANALYSIS OF THE PROPOSED IBBSSMR

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

5.1. Proof of Correctness

The following equations give the correctness of the proposed scheme.

Consider

$$\begin{aligned}
\hat{e}(P, V)\, \hat{e}(P_{pub}, -hQ_{ID}) &= \hat{e}(P, b\tilde{V} + aP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, b\tilde{V})\, \hat{e}(P, aP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, b(X + \tilde{h}d_{ID}))\, \hat{e}(P, aP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, bX)\, \hat{e}(P, b\tilde{h}d_{ID})\, \hat{e}(P, aP_{pub})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, aP_{pub} + bX)\, \hat{e}(P_{pub}, hQ_{ID})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, aP_{pub} + bX)\, \hat{e}(P_{pub}, hQ_{ID})\, \hat{e}(P_{pub}, -hQ_{ID}) \\
&= \hat{e}(P, aP_{pub} + bX) \\
&= U.
\end{aligned}$$

5.2. Security Analysis

In the following, we will show that proposed IBBSSMR satisfies all the security requirements stated in section 3.2.

5.2.1. Blindness Property

In order to prove the blindness property, we will show that for a given message-signature pair (M, h, V) and the signer's view $(M', \tilde{h}, \tilde{V})$, there always exists a unique pair of blinding factors a, b that maps $(M', \tilde{h}, \tilde{V})$ to (M, h, V). Since the user chooses the blinding factors a, b randomly, the signer cannot get any information from his/her view and the signature scheme will be blind. For a signature (h, V) generated on a message M, during the protocol, the following equations must hold.

$$U = \hat{e}\,(aP_{pub} + bX,\ P) \tag{1}$$

$$\tilde{h} = b^{-1}h \bmod q \tag{2}$$

$$V = b\tilde{V} + aP_{pub} \tag{3}$$

Implies $b = h\tilde{h}^{-1} \bmod q$ and

$$a = \log_{P_{pub}}(V - b\tilde{V}) \bmod q.$$

The above formula, for a involves the elliptic curve discrete logarithm of $(V - b\tilde{V}) \in G_1$ with respect to the base P_{pub}. So we can use aP_{pub} in the rest of the proof instead. It is obvious that $a, b \in Z_q^*$ exists uniquely from (2) and (3). Next we show that such $a, b \in Z_q^*$ satisfies Equation (1) also.

Obviously, due to the non-degenerate property of the bilinear pairings, we have $U = \hat{e}\left(aP_{pub} + bX,\ P\right) \Leftrightarrow \hat{e}\left(U,\ P_{pub}\right) = \hat{e}\left(\hat{e}\,(aP_{pub} + bX,\ P),\ P_{pub}\right)$. So we only need to show that a and b satisfy $\hat{e}\left(U,\ P_{pub}\right) = \hat{e}\left(\hat{e}\,(aP_{pub} + bX,\ P),\ P_{pub}\right)$.

Consider

$$\begin{aligned}
&\hat{e}\,\left(\hat{e}\left(aP_{pub} + bX,\ P\right),\ P_{pub}\right)\\
&= \hat{e}\,\left(\hat{e}\left(V - b\tilde{V} + bX,\ P\right),\ P_{pub}\right)\\
&= \hat{e}\,\left(\hat{e}\,\left(V - b\left(X + \tilde{h}d_{ID}\right) + bX,\ P\right), P_{pub}\right)\\
&= \hat{e}\,\left(\hat{e}\,\left(V - b\tilde{h}d_{ID},\ P\right),\ P_{pub}\right)\\
&= \hat{e}\left(\hat{e}\,\left(V - h\tilde{h}^{-1}\tilde{h}d_{ID},\ P\right),\ P_{pub}\right)\\
&= \hat{e}\,\left(\hat{e}\,(V,\ P)\hat{e}\,(-hd_{ID},\ P),\ P_{pub}\right)\\
&= \hat{e}\left(\hat{e}\,(V,\ P)\ \hat{e}\,\left(-hQ_{ID},\ P_{pub}\right),\ P_{pub}\right)\\
&= \hat{e}\left(U,\ P_{pub}\right).
\end{aligned}$$

Thus, the unique solutions of Equations (2) and (3) satisfy Equation (1). Since the blinding factors are unique and randomly chosen during the protocol, hence the blindness property of the proposed scheme follows.

5.2.2. Unforgeability

In order to prove unforgeability, we first assume that there exists a probabilistic polynomial time algorithm A, which can create forged signatures of the signer. We can then use A to solve the CDH (Computational Diffie-Hellman) problem. Assume that A is able to forge valid blind signatures which can be accepted by the verification algorithm with non-negligible probability. By the Oracle replay attack and the Forking Lemma [18], assume A has constructed two different valid blind signatures for a message M.

$$\tilde{\sigma}_1 = (\tilde{h}_1,\ \tilde{V}_1) \quad \text{and} \quad \tilde{\sigma}_2 = (\tilde{h}_2,\ \tilde{V}_2)$$

Since these two valid blind signatures obtained from the same random tape with different oracles $\tilde{h}_1$ and $\tilde{h}_2$. It is admissible to assume that

$$\tilde{V}_1 = X + \tilde{h}_1 d_{ID} \quad \text{and} \quad \tilde{V}_2 = X + \tilde{h}_2 d_{ID} \quad \text{where} \quad \tilde{h}_1 \neq \tilde{h}_2.$$

Thus, we have $(\tilde{V}_1 - \tilde{V}_2) = (\tilde{h}_2 - \tilde{h}_1) d_{ID}$ and we can compute d_{ID} as follows $d_{ID} = (\tilde{h}_2 - \tilde{h}_1)^{-1}\ (\tilde{V}_1 - \tilde{V}_2)$. By the system initialization algorithm of the blind signature, we are able to solve an instance of the CDH problem, namely given $(P,\ Q_{ID} = aP,\ P_{pub} = sP)$, it is possible to compute $d_{ID} = sQ_{ID} = saP$, which is a contradiction, which arises due to the assumption that A successfully constructed two different valid blind signatures for M. Hence the blind signature is unforgeable.

5.3. Efficiency of the Proposed IBBSSMR

In this section, we analyze the performance of our IBBSSMR scheme and then we compare it with the related schemes in terms of computational and communicational (signature length) cost point of view. From the experimental results [19]-[21], to achieve the comparable security with 1024-bit RSA key where the bilinear pairing (Tate pairing) is defined over the supersingular 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 Cao et al. [19], He et al. [20], Ren et al. [21] using MIRACL [22], 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. (2007) [23], 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 Cao et al. [19] and He et al. [20] 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 Baretto et al. 2004 [24] and Tan et al. 2010 [25], $1T_{BP} \approx 3T_{EM}$ 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 analyze the efficiency of our proposed IBBSSMR scheme by comparing it with the existing schemes [14], [17]. The comparison is summarized in Table 2.

Table 2. Efficiency comparison of our Scheme with related schemes

Scheme	Signature length (bits)	Signing cost	Verification cost	Total cost
Han et al. scheme [14]	$2\|G_1\|$	$6T_{EM} + 2T_{BP} + 1T_{IN} + 2T_{PA}$	$3T_{BP} + 1T_{PX}$	$\approx 664.34T_{ML}$
Hassan et al. scheme [17]	$\|q\| + \|G_1\|$	$6T_{EM} + 1T_{BP} + 1T_{IN} + 2T_{PA}$	$2T_{BP} + 1T_{PX}$	$\approx 490.34T_{ML}$
Proposed IBBSSMR	$\|q\| + \|G_1\|$	$6T_{EM} + 1T_{BP} + 1T_{IN} + 2T_{PA}$	$2T_{BP} + 1T_{EM}$	$\approx 475.84T_{ML}$

From Table 2, it is clear that the signature length of the proposed IBBSSMR scheme is $(|q| + |G_1|)$, which is less than Han et al. [14] scheme and equal length with Hassan et al. scheme [17]. Also, the computational cost for signing and verification of the proposed IBBSSMR scheme is $\approx 475.84T_{ML}$ which is less than Han et al. [14] and Hassan et al. [17] schemes; and so our scheme is computationally more efficient than the Han et al. [14] and Hassan et al. [17] schemes. Hence, from the above discussion, the proposed IBBSSMR scheme is computationally and communicationally efficient than the related schemes.

6. CONCLUSION

In this paper, we proposed a new blind signature scheme with message recovery in the ID-based setting using bilinear pairings over elliptic curves. This scheme combines the advantages of blind signature, message recovery with ID-based cryptography and plays an important role in cryptographic protocols such as e-voting and e-payment. The Blindness property of our scheme provides the anonymity of the user and message recovery property provides to work with low band width devices like PDAs, mobile devices etc. Also the proposed scheme is secure with the assumption that the CDH problem is intractable. Efficiency analysis of our scheme with other schemes shows that the proposed IBBSSMR is efficient in terms of computational and communicational point of view.

REFERENCES

[1] D. Chaum, "Blind signatures for untraceable payments," *In Proc. of CRYPTO'82, New York: Plenum Press* pp.190-203, 1983.

[2] R. A. Sahoo, and S. Padhye, "ID-based signature scheme from bilinear pairings: A survey," *Front. Electr. Electron. Engg. China*, vol. 6(4), pp. 487-500, 2011.

[3] M.li, Provable secure and efficient ID-based strong designated verifier signature scheme with message recovery," *Indonesian Journal of Electrical Engineering and Computer Science*, vol.12, No. 10, pp. 7343-7352, 2014.

[4] G. Swapna *et al.* "An efficient ID-based proxy signcryption scheme," *International Journal of Networks Security*,, vol. 1, no. 3, pp. 200-206, 2012.

[5] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," *ASIACRYPT-2002*, LNCS, vol. 2507, pp. 533–547, 2002.

[6] Hua Sun, "New Certificateless Blind Ring Signature Scheme," *TELKOMNIKA Indonesian Journal of Electrical Engineering.*, vol. 12, no. 1, pp. 778-783, 2014.

[7] Huang, *et al.,* "Efficient identity-based signatures and blind signatures," *CANS'05, LNCS 3810, Springer-Verlag*, pp.120-133, 2005.

[8] Z. Zhao, *et al.*, "A New ID-Based Blind Signature from Bilinear Pairings," *Proceedings of the ICWMMN 2006*, pp.402-403, 2006.

[9] S. Kalkan, *et al.*, "Generalized ID-based Blind Signatures from Bilinear Pairings," *In proceeding of the 23 International Symposium on Computer and Information Sciences (ISCIS 2007)*, pp 45-48, 2007.

[10] Z. Zhao, " ID-Based Authenticated Blind Signature Scheme from Bilinear Pairings," proceedings of the *Int. Conf. on Computational Intelligence and Security Workshops*, IEEE, pp. 725-728, 2007.

[11] B. Umaprasada Rao, *et al.*, "An ID-Based Blind Signature Scheme from Bilinear Pairings," *International Journal of Computer Science and Security*. vol. 4 (1), pp. 98-106, 2010.

[12] G. Xu and G. Xu, "An ID-based Blind Signature from Bilinear Pairing with Unlinkability," *IEEE conference on Information security*, pp.101-104, 2012.
[13] R. Pance and A. Ljupcho, "Comparison of ID-Based Blind Signatures from Pairings for E-voting Protocols," *MIPRO 2014*, Opatija, Croatia pp.26-30, 2014.
[14] S. Han, and E. Chang, "A Pairing-Based Blind Signature Scheme with Message Recovery," *International Journal of Information Technology*, vol. 2 (4), 2005.
[15] J. Wang and H. Qian, "An Optimal Blind Signature Padding with Message Recovery," *Fifth International Conference on Information Assurance and Security*, 2009.
[16] J. S. Zhang, "A Kind of Message-Recoverable Fairness Blind Digital Signature Scheme," *Proceedia Engineering* vol.15, pp. 2103-2107, 2011.
[17] E. Hassan and A. Yasmine, "A New Blind Identity- Based Signature Scheme with Message Recovery," *The Online Journal of Electronics and Electrical Engineering (OJEEE)*, vol.2 (2), 2006.
[18] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13(3), pp.361-396, 2000.
[19] X. Cao, *et al., "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges*," *Information Sciences*, vol. 180(15), pp. 2895-2903, 2010.
[20] D. He, *et al.*, "An ID-based proxy signature scheme without bilinear pairings," *Ann. of Telecommunication*, vol. 66, pp. 657–662, 2011.
[21] K. Ren, *et al.*, "On broadcast authentication in wireless sensor networks," *IEEE Transaction on Wireless Communication*, vol. 6(11), pp. 4136–4144, 2007.
[22] Shamus Software Ltd. Miracl Library. Available: http://certivox.org/display/EXT/MIRACL.
[23] Y. F. Chung, *et al*., "ID-based digital signature scheme on the elliptic curve cryptosystem," *Computer Standards and* Interfaces, vol. 29(6), pp. 601-604, 2007.
[24] P. S. L. M. Barreto, *et al., "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] S. H. Tan, et al., "Java Implementation for Pairing-Based Cryptosystems," *Proc. of the Int. Conference in Computational Science and Its Applications* (*ICCSA'10*), LNCS 6019, pp. 188-198, 2010.