An Untraceable Identity-Based Blind Signature Scheme without Pairing for E-Cash Payment System

Mahender Kumar(✉), C. P. Katti, and P. C. Saxena

School of Computer and Science System, JawaharLal Nehru University,
New Delhi, India
mahendjnu1989@gmail.com,
{cpkatti,pcsaxena}@mail.jnu.ac.in

Abstract. Blind signature is an interesting cryptographic primitive which allows user to get signature on his document from signatory authority, without leaking any information. Blind signature is useful in many e-commerce applications where user's anonymity is the main concern. Since the Zhang et al., was the first to propose the identity based blind signature, many schemes based on bilinear pairing have been proposed. But the computational cost of pairing operation on elliptic curve is around 20 times the point multiplication on an elliptic curve. In order to save the running time, we present a new Identity-Based Blind Signature (ID-BS) scheme whose security is based on elliptic curve discrete logarithm problem (ECDLP). Performance comparison shows that proposed scheme reduces the cost of computation. Security analysis shows that proposed scheme is secure against the adversary and achieves the property of blindness and Non-forgeabillity. At the end; we propose an e-cash payment system based on our ID-based blind signature scheme.

Keywords: Blind signature · Identity-based encryption
Elliptic curve cryptography · Non-forgeability · Blindness

1 Introduction

Blind signature is an interesting cryptographic primitive which provides the user anonymity. This scheme allows user to get signature from signatory authority (SA) on his document without leaking any information about the document. Since, the notion of blind signature is first posed by Chaum [1, 2], many authors have presented their work on Blind Signature. All schemes are based on the traditional public key cryptosystem where certificate authority issue a digital certificate which binds the user's public key with his unique identity and public key infrastructure (PKI) is required for managing those certificates. In order to address the issue of certificate management and others issues such as key management and public key revocation, Shamir [3] proposed an idea, Identity-Based Cryptosystem (IBC), where user's public key is directly derived from his unique identity. To earn private key correspond to their identity ID, user requests the trusted third party, usually referred as the Private Key Generator (PKG). Nowadays, IBC is becoming very popular as compared to public key cryptosystem

N. Kumar and A. Thakre (Eds.): UBICNET 2017, LNICST 218, pp. 67–78, 2018.
https://doi.org/10.1007/978-3-319-73423-1_7

(PKC) and implemented in many areas, e.g., forward encryption [4], delegate decryption [4], key exchange scheme [5], electronic-voting [6], electronic-cash payment system [7–9] etc.

Using the idea of Identity-based cryptosystem, Zhang and Kim's proposals [10, 11] were the first to pose the ID-Based Blind Signature. Later, Gao et al. [12, 13], Elkamchouchi and Abouelseoud [14], Rao et al. [15], Hu and Huang [16], He et al. [17], Dong et al. [18], Kumar et al. [19] presented ID-based blind signature schemes. But due to dependency on elliptic curve pairing operations, none was found efficient because pairing operations are very expensive as compared to the scalar multiplication operation on elliptic curves. Vanstone [20] claimed that system using 128-bit elliptic curve cryptography (ECC) key achieved the same security as using the 1024-bit RSA key. Additionally, ECC takes less power consumption and less storage space which provides strong processing time. In this paper, we mainly concentrate on posing anew ID-based Blind Signature scheme based on solving the difficulty of ECDLP problem. Proposed scheme satisfied the security requirements of blind signature and identity-based cryptosystem. At the end; we propose an e-cash payment system based on our ID-based blind signature scheme.

The remainder of the paper is arranged as follows: we briefly described the preliminaries in Sect. 2. Proposed ID-BS scheme is defined in Sect. 3. Section 4 includes the security analysis and computation comparison of our scheme against with existing schemes. Section 5 includes the e-cash system based on our proposed ID-BS scheme. Finally, conclusion and open problems are made in Sect. 6.

2 Preliminaries

2.1 Elliptic Curve Cryptosystem

Suppose the elliptic curve equation $y^2 = (x^3 + mx + n) modp$, where $x,\ y \in F_p$ and $4m^3 + 27n^2 modp \neq 0$. Formally, the Elliptic Curve is a set of points $(x,\ y)$ which satisfied the above equation and an additive abelian group with point 0 (identity element). The condition $4m^3 + 27n^2 modp \neq 0$ tells that $y^2 = (x^3 + mx + n) modp$ has a finite abelian group that can be defined based on the set of points $E_p(m,\ n)$ on elliptic curve. Consider points $A = (x_A,\ y_A)$ and $B = (x_B,\ y_B)$ over $E_p(m,\ n)$, the addition operation of elliptic curve is represented as $A + B = C = (x_C,\ y_C)$, defined as following: $x_C = (\mu^2 - x_A - x_B) modp$ and $y_C = (\mu(x_A - x_C) - y_A) modp$.

Where, $\mu = \begin{cases} \left(\frac{y_B - y_A}{x_B - x_A}\right) modp, if\ A \neq B \\ \left(\frac{3x_A^2 + m}{2y_A}\right) modp,\ if\ A = B \end{cases}$

Based on elliptic curve, Koblitz [21] and Miller [22] introduced elliptic curve cryptosystem. It is noted that addition operation and multiplication operation in ECC are equivalent to modular multiplication and modular exponentiations in RSA respectively.

Discrete Logarithm problem based on elliptic curve (ECDLP): Consider $B = sA$ where $A, B \in E_p(a, b)$, and $s \in Z_q$, it is computationally easy to compute B from A and s. But it is very difficult to compute s from B and A.

Extended Euclidean Algorithm: Extended Euclidean algorithm finds the modular inverse operation, which widely helpful in public key cryptosystem [23]. In addition to compute the *gcd* of two integer, say x and y, this algorithm express the $gcd(x, y)$ in linear combination of the form $gcd(x, y) = xp + yq$, for some integers p and q.

2.2 Framework of ID-BS Scheme

Definition 1 (Identity-Based Blind Signature): Our ID-Based Blind Signature protocol consists of Four Probabilistic Polynomial-Time (PPT) algorithms, namely, Setup, Extract, BlindSig, and Verifying, run among four entities, namely, Private Key Generator (PKG), Signatory Authority, Requester, and Verifier, where

1. *Setup*: On some security parameter k, PKG computes the system parameter (*PARAM)* and master secret key s. *PARAM* includes the public parameter which is published publically and s is known to PKG only.
2. *Extract*: On given inputs *PARAM*, master key s, and SA's Identity ID_S, PKG computes the private key S_{IDS} corresponding to identity ID_S.
3. *BlindSig:* This algorithm consists of four sub-algorithms, runs between the Requester and SA.
   a. *Commitment:* SA computes public parameters (Q_1, Q_2) against his secret values (n_1, n_2), delivers (Q_1, Q_2) to the Requester and keeps secret values (n_1, n_2).
   b. *Blinding:* Upon receiving the public parameters (Q_1, Q_2) and random chosen secret values (g, h, i, j, k, l), the Requester computes the Blinded Message (b_{M1}, b_{M2}) on given Message M. Now, Requester requests the SA to issue Signature on Blinded Message (b_{M1}, b_{M2}).
   c. *Signing:* For given Blinded Message (b_{M1}, b_{M2}), SA computes the Blind Signature $\left(S'_1, S'_2\right)$ using his private key S_{IDS} and delivers the Blind Signature $\left(S'_1, S'_2\right)$ to the Requester.
   d. *Stripping:* Upon receiving the Blinded Signature $\left(S'_1, S'_2\right)$, Requester strips it against his secret key to outputs the original Signature (S, R). Finally, Requester published the message-signature pair (M, S, R) for verification.
4. *Verifying*: Verifier takes (M, S, R) and SA's Identity ID_S as inputs, runs the verifying algorithm to verifies the Signature.

Two important constraints required against the security of ID-BS scheme are: Blindness property and Non-forgeability of additional signature under parallel chosen message and ID attacks. An Identity- Based Blind Signature is considered as secure if it fulfills the following two conditions:

Definition 2 (Blindness). Blindness property is defined in terms of following game playing between the challenger C and PPT adversary A.

- *Setup*: The challenger C chooses a security parameter k and executes the *Setup* algorithm to compute the published parameter *PARAM* and master key s. Challenger C sends *PARAM* to A.
- *Phase1*: A selects two distinct message M_0 and M_1 and an ID_i, and sends to C.
- *Challenge*: C uniformly chooses a random bit $b \in \{0, 1\}$ and ask A for signature on M_b and $M_{1\text{-}b.}$ Finally, C strips both the Signatures and gives the original signatures $(\sigma_b, \sigma_{1\text{-}b})$ to A.
- *Response*: A guesses bit $b' \in \{0, 1\}$ on tuple $(M_0, M_1, \sigma_b, \sigma_{1\text{-}b})$. A wins the game if $b = b'$ holds with probability $[b = b'] > 1/2 + k^{-n}$.

To define the Non-forgeability, let us introduce the following game playing between the Adversaries A who act as Requester and the Challenger C who act as honest SA.

- *Setup*: On random Security parameter k, the challenger C executes the *Setup* algorithm and computes the parameter *PARAM* and master key s. Challenger C sends *PARAM* to A.
- *Queries*: Adversary A can performs numbers of queries as follows:
  - *Hash function queries*: For requested input, challenger C computes the hash function values and sends it to the attacker A.
  - *Extract queries*: A selects an Identity ID and ask for S_{ID} to A.
  - *BlindSig queries*: A selects an ID and Message M blindly requested the Signature from $C.C$ compute signature on Message M with respect to ID.
- *Forgery*: Game is in favor of A, if against identity ID*, A response with n valid Message-Signature $(M_1, \sigma_1 = (S_1, R_1, r_1)),. (M_2, \sigma_2 = (S_2, R_2, r_2)).... (M_n, \sigma_n = (S_n, R_n, r_n))$ such that
  - Each message M_i is distinct from other Message M_j in given Message-Signature $(M_1, \sigma_1 = (S_1, R_1, r_1)), (M_2, \sigma_2 = (S_2, R_2, r_2))..... (M_n, \sigma_n = (S_n, R_n, r_n))$ set.
  - *Adversary A* is restricted to ask an extract query on Identity *ID**.
  - Execution of BlindSig algorithm is bounded by n.

Definition 3 (Non-forgeability). An ID-BS scheme is break by an Adversary A (t, q_E, q_B, k^{-n}), if A runs no more than t, A make Extract queries no more than q_E and runs *BlindSig* phase no more than q_B, with an advantage more than equal to k^{-n}. Under the adaptive chosen message and ID attacks, our ID-BS scheme is said to secure against one-more forgery, if no adversary A (t, q_E, q_B, k^{-n})-breaks the scheme.

3 Our Scheme: ID-BS Protocol

In this section, we introduce a new ID-BS scheme based on ECDLP. Suppose P be the generator of group G_1 of prime order q. Let the two cryptographic hash function $H_1 : \{0,1\}^* \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \rightarrow Z_q^*$. *absc(P)* denotes the abscissa of point P on G_1. Our scheme consists of four algorithm, as given in definition 1 in Sect. 2, runs as follows:

Setup: PKG select randomly $s \in Z_q$ and compute public key $P_{Pub} = s.P$. Publishes $PARAMS = \{G, q, P, P_{Pub}, H_1, H_2\}$, and keep secret key s secretly.

Extract: For a String identity $\mathrm{ID_S}$ and his master key s, PKG computes SA's private key $S_{IDS} = s.Q_{IDS} modn$, where $Q_{IDS} = H_1(ID_S)$ and sends to the SA.

Blind Signature: This algorithm consists of four steps, runs between SA and the Requester as shown in Fig. 1.

Commitment: SA chooses two secret random integer $n_1, n_2 \in Z_q^*$. Computes Q_1, Q_2, q_1 and q_2 and publish them. Where,

$$Q_1 = n_1.P \in G_1 \, and \, q_1 = abscQ_1) \in Z_q^*$$

$$Q_2 = n_2.P \in G_1 \, and \, q_2 = absc(Q_2) \in Z_q^*$$

Blinding: On given parameters (Q_1, Q_2, q_1, q_2) and Message M, Requester chooses four random numbers $g, h, i, j \in Z_q$ such that $gcd(i, j) = 1$. Selects two random number k and l such that $ki + lj = gcd(i, j)$ (according to the extended Euclidean algorithm). Now, Requester computes R_1, R_2, r_1, and r_2 and requests to the SA for Signature on Blinded Message ($\mathrm{b_{M1}}$, $\mathrm{b_{M2}}$). Where,

$$\begin{gathered} R_1 = g.i.Q_1 \in G_1 \, and \, r_1 = absc(R_1) \in Z_q^* \\ R_2 = h.j.Q_2 \in G_1 \, and \, r_2 = absc(R_2) \in Z_q^* \\ r = r_1.r_2 modq \in Z_q^* \\ b_{M1} = k.H_2(M).q_1.r^{-1}.g^{-1} \in Z_q^* \\ b_{M2} = l.H_2(M).q_2.r^{-1}.h^{-1} \in Z_q^* \end{gathered}$$

Signing: On given Blinded Message ($\mathrm{b_{M1}}$, $\mathrm{b_{M2}}$), SA creates the Blind Signature $\left(\mathrm{S}_1', \mathrm{S}_2'\right)$ using their private key $\mathrm{S_{IDS}}$ and sends it to the Requester, where,

$$S_1' = S_{IDS}.b_{M1} - q_1.n_1 \in Z_q^*$$

$$S_2' = S_{IDS}.b_{M2} - q_2.n_2 \in Z_q^*$$

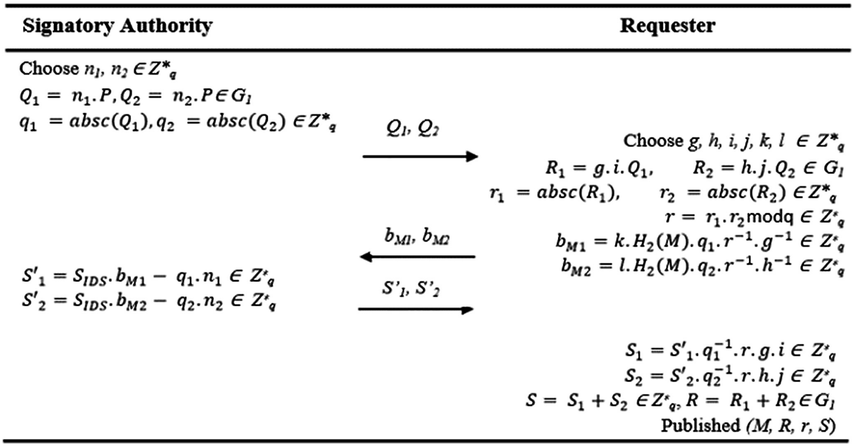
Stripping: On receiving the Blind Signature $\left(\mathrm{S}_1', \mathrm{S}_2'\right)$, the Requester strips and computes the actual signature $\sigma = (S, R, r)$. Where,

$$\begin{gathered} S_1 = S_1'.q_1^{-1}.r.g.i \in Z_q^* \\ S_2 = S_2'.q_2^{-1}.r.h.j \in Z_q^* \\ S = (S_1 + S_2) modq \in Z_q^* \, \text{and} \, R = (R_1 + R_2) modq \in Z_q^* \end{gathered}$$

Finally, requester publishes *(M, σ = (S, R, r))* for verification.

Verify: On given message-signature pair (M, $\sigma = (S, R, r)$), public parameter P_{Pub}, and $Q_{IDS,}$ user accepts the signature if and only if

$$P_{Pub}.Q_{IDS}.H_2(M) = S.P + r.R$$



Signatory Authority | **Requester**

Choose $n_1, n_2 \in Z^*_q$

$Q_1 = n_1.P, Q_2 = n_2.P \in G_1$

$q_1 = absc(Q_1), q_2 = absc(Q_2) \in Z^*_q$

Q_1, Q_2 →

Choose $g, h, i, j, k, l \in Z^*_q$

$R_1 = g.i.Q_1, \quad R_2 = h.j.Q_2 \in G_1$

$r_1 = absc(R_1), \quad r_2 = absc(R_2) \in Z^*_q$

$r = r_1.r_2 \bmod q \in Z^*_q$

$b_{M1} = k.H_2(M).q_1.r^{-1}.g^{-1} \in Z^*_q$

$b_{M2} = l.H_2(M).q_2.r^{-1}.h^{-1} \in Z^*_q$

← b_{M1}, b_{M2}

$S'_1 = S_{IDS}.b_{M1} - q_1.n_1 \in Z^*_q$

$S'_2 = S_{IDS}.b_{M2} - q_2.n_2 \in Z^*_q$

S'_1, S'_2 →

$S_1 = S'_1.q_1^{-1}.r.g.i \in Z^*_q$

$S_2 = S'_2.q_2^{-1}.r.h.j \in Z^*_q$

$S = S_1 + S_2 \in Z^*_q, R = R_1 + R_2 \in G_1$

Published (M, R, r, S)

Fig. 1. BlindSig algorithm of our proposed scheme.

Since, S = S_1 + S_2, then we have,

$$
\begin{aligned}
S.P + r.R &= (S_1 + S_2).P + r.R \\
&= (S'_1.q_1^{-1}.r.g.i + S'_2.q_2^{-1}.r.h.j).P + r.R \\
&= ((S_{IDS}.b_{M1} - q_1.n_1).q_1^{-1}.r.g.i + (S_{IDS}.b_{M2} - q_2.n_2).q_2^{-1}.r.h.j).P + r.R \\
&= \left(S_{IDS}.b_{M1}.q_1^{-1}.r.g.i - n_1.r.g.i + S_{IDS}.b_{M2}.q_2^{-1}.r.h.j - n_2.r.h.j\right).P + r.R \\
&= \left(S_{IDS}.r.\left(b_{M1}.q_1^{-1}.g.i + b_{M2}.q_2^{-1}.h.j\right) - r.(n_1.g.i + n_2.h.j)\right).P + r.R \\
&= \left(S_{IDS}.r.\left(k.H_2(M).q_1.r^{-1}.g^{-1}.q_1^{-1}.g.i + l.H_2(M).q_2.r^{-1}.h^{-1}.q_2^{-1}.h.j\right)\right. \\
&\quad \left. -r.(n_1.g.i + n_2.h.j)\right).P + r.R \\
&= (S_{IDS}.H_2(M).(k.i + l.j) - r.(n_1.g.i + n_2.h.j)).P + r.R \\
&= (S_{IDS}.H_2(M) - r.(n_1.g.i + n_2.h.j)).P + r.R \\
&= S_{IDS}.H_2(M).P - r.(n_1.g.i + n_2.h.j).P + r.R \\
&= msk_{Pr}.Q_{IDS}.H_2(M).P - r.(R_1 + R_2) + r.R \\
&= P_{Pub}.Q_{IDS}.H_2(M) - r.R + r.R \\
&= P_{Pub}.Q_{IDS}.H_2(M)
\end{aligned}
$$

This proved the correctness of proposed scheme.

4 Analysis of Our Proposed Scheme

4.1 Security Analysis

Theorem 1 (Blindness). *The proposed ID-BS scheme holds the property of blindness.*

Proof. Suppose adversary *A* which acts as SA and challenger *C* which acts as honest Requester, both involves in the *BlindSig* phase. *A* determines bit *b* with probability ½.

Let the information appearing during one of the execution of *BlindSig* phase in the view of *A* be $\left(b_{M1}, b_{M2}, S'_1, S'_2\right)$. Let the Signature be ($R = R_1 + R_2$, $S = S_1 + S_2$). There must be a tuple of random blinding factor (*g, h, i, j, k, l*) that maps the $\left(b_{M1}, b_{M2}, S'_1, S'_2\right)$ to ($R = R_1 + R_2$, $S = S_1 + S_2$).

Let $i = R_1.g.Q_1^{-1}$ and $\mathrm{g} = R_1.h.Q_2^{-1}$ such that there exist a pair of unique blinding factor (*g, h*) which satisfied the equations $\mathrm{S_1 = S'_1.q_1^{-1}.r.g.i}$ and $\mathrm{S_2 = S'_2.q_2^{-1}.r.h.j}$ respectively. However, it is intact to solve the blinding factor (*g, h, i, j*), we only need to exploit the existence of them. Let $k = \mathrm{b_{M2}.r.g.}q_1^{-1}.H_2^{-1}(\mathrm{M})$, so there exist a unique factor *l* that satisfied the equation $\mathrm{b_{M2}} = \mathrm{l}.H_2(m).\mathrm{q_2.r^{-1}.h^{-1}}$.

Thus, there exist the blinding factors (*g, h, i, j, k, l*) which leads to the similar relation as in the *BlindSig* phase in Definition 1. Therefore, based on the hardness of ECDLP assumption, a strong adversary *A* determines *b* with probability 1/2 + $\mathrm{k^{-n}}$.

Theorem 2 (Non-forgeability). *Under the hardness assumption of the ECDLP, our ID-BS Scheme is existential non-forgeable against the adaptive chosen message and identity attacks in the random oracle model.*

Proof. Suppose any PPT-bounded adversary *A* can forge ID-BS scheme under the adaptive chosen message and identity attack. Let a PPT-bounded algorithm *B* which helps *A* to solve the ECDLP problem, i.e. *A* would able to compute *x* from equation $Y = x.X$, where $x \in Z_q$ is unknown to *A*.

Setup: B considers P_{Pub} and gives public parameter $PARAM = \{G, q, P, P_{Pub}, H_1, H_2\}$ to *A*.

Queries: Adversary *A* can performs number of queries as follows:

Hash1 queries: B makes an empty list H_1^{List} having tuple (ID_i, $H_1(ID_i)$, a_i). When A queries to H_1^{List} at an Identity ID_i, *B* response as follows:

- *B* gives $H_1(ID_i)$ to *A*, if ID_i found in the H_1^{List} in tuple of (ID_i, $H_1(ID_i)$, a_i) or (*IDi*, $H_1(IDi)$, *).
- *B* sets $H_1(ID_i) = Q_{ID}$ and gives to *A* and adds the tuple (ID_i, $H_1(ID_i)$, *) to list H_1^{List}, if $ID_i = ID*$.
- *B* chooses randomly $a_i \in Z_q$ and gives $H_1(ID_i) = a_i.P$ to *A* and adds tuple (ID_i, $H_1(ID_i)$, a_i) to list H_1^{List}, otherwise.

Since H1 is random oracle so $H_1(ID)$ gives no information to *A* until he queries H_1 oracle on *ID*.

Hash2 queries: *B* provides $M_j \in G_1$ on applying queries M_j to $H_2(M_j)$ and gives to *A*.

Extract queries: For some unknown $s \in Z_q$. Let $X = sP$, *B* computes $S_{IDi} = sH_1(ID_i) = a_i.X$, i.e. $H_1(ID_i) = a_i.P$. Now *B* sends S_{IDi} to *A*.

BlindSig queries: Suppose A wants to obtain a blind signature on message M_i with identity $\mathrm{ID_i}$. Let $\left(b_{M'1}, b_{M'2}\right)$ be blinded message which *A* gives to *B*. *B* response this queries as follows:

- If $ID_i \neq ID*$, using *IDi* corresponding to H_1^{List}, B finds the private key $S_{IDi} = a_iX$. Using S_{IDi}, *B* finds the blinded signature as in Sign phase in *BlindSig* algorithm.
- If $ID_i = ID*$, *B* sends $(b_{M'1i}, b_{M'2i})$ to A. Let $\sigma_i = (R_i, S_i, r_i)$ be corresponding response.

Forgery: A response with n valid Message-Signature $(M_1, \sigma_1 = (S_1, R_1, r_1)), (M_2, \sigma_2 = (S_2, R_2, r_2)).....(M_n, \sigma_n = (S_n, R_n, r_n))$ against identity $ID*$.

On applying the forking lemma, suppose adversary *A* creates two different valid blind signature (σ_A, σ_B) for message M, where

$$\begin{aligned}
&\sigma_A = (S_A, \mathrm{r}_A)\, \mathit{and}\, \sigma_B = (S_B, \mathrm{r}_B)\\
&S_A = S_{1A} + S_{2A}\\
&= S'_{1A}.q_{1A}^{-1}.r_A.g.i + S'_{2A}.q_{2A}^{-1}.r_A.h.j\\
&= (S_{ID}.b_{m1A} - q_{1A}.n_{1A}).q_{1A}^{-1}.r_A.g.i + (S_{ID}.b_{m2A} - q_{1A}.n_{1A}).q_{2A}^{-1}.r_A.h.j\\
&= S_{ID}.b_{m1A}.q_{1A}^{-1}.r_A.g.i - n_{1A}.r_A.g.i + S_{ID}.b_{m2A}.q_{2A}^{-1}.r_A.h.j - n_{1A}.r_A.h.j\\
&= S_{ID}.r_A.(b_{m1A}.q_{1A}^{-1}.g.i + b_{m2A}.q_{2A}^{-1}.h.j) - n_{1A}.r_A.(g.i + h.j)
\end{aligned}$$

Similarly, $S_B = S_{1B} + S_{2B}$

$$\begin{aligned}
&= S'_{1B}.q_{1B}^{-1}.r_B.g.i + S'_{2B}.q_{2B}^{-1}.r_B.h.j\\
&= (S_{ID}.b_{m1B} - q_{1B}.n_{1B}).q_{1B}^{-1}.r_B.g.i + (S_{ID}.b_{m2B} - q_{2B}.n_{2B}).q_{2B}^{-1}.r_B.h.j\\
&= S_{ID}.b_{m1B}.q_{1B}^{-1}.r_B.g.i - n_{1B}.r_B.g.i + S_{ID}.b_{m2B}.q_{2B}^{-1}.r_B.h.j - n_{1B}.r_B.h.j\\
&= S_{ID}.r_B.(b_{m1B}.q_{1B}^{-1}.g.i + b_{m2B}.q_{2B}^{-1}.h.j) - n_{1B}.r_B.(g.i + h.j)
\end{aligned}$$

Now, we compute

$$\begin{aligned}
S_B - S_A = {} & S_{ID}.g.i\big(b_{m1B}.q_{1B}^{-1}.r_B - b_{m1A}.q_{1A}^{-1}.r_A\big)\\
& + S_{ID}.h.j.\big(b_{m2B}.q_{2B}^{-1}.r_B - b_{m2A}.q_{2A}^{-1}.r_A\big)\\
& -(g.i + h.j).(n_{1B}.r_B - n_{1A}.r_A)\\
S_{ID}.\big(g.i\big(b_{m1B}.q_{1B}^{-1}.r_B - b_{m1A}.q_{1A}^{-1}.r_A\big) & \\
+ h.j.\big(b_{m2B}.q_{2B}^{-1}.r_B - b_{m2A}.q_{2A}^{-1}.r_A\big)\big) & \\
= S_B - S_A + (g.i + h.j).(n_{1B}.r_B - n_{1A}.r_A) &
\end{aligned}$$

So, we can compute $\mathrm{S_{ID}}$ as follows:

$$\begin{aligned}
S_{ID} = {} & \big(g.i\big(b_{m1B}.q_{1B}^{-1}.r_B - b_{m1A}.q_{1A}^{-1}.r_A\big)\\
& + h.j.\big(b_{m2B}.q_{2B}^{-1}.r_B - b_{m2A}.q_{2A}^{-1}.r_A\big)\big)^{-1}.(S_B - S_A\\
& + (g.i + h.j).(n_{1B}.r_B - n_{1A}.r_A))
\end{aligned}$$

In order to compute S_{ID}, Adversary *A* should know the value of secret values (n_1, n_2) the Signatory Authority holds. To compute (n_1, n_2) is equivalent to solve the ECDLP problem. Alternatively, on given $(P, Q_{ID} = aP, P_{pub} = sP)$ it is easily to compute

$S_{ID} = sQ_{ID} = saP$ if the master key would not have compromised. But assuming the ECDLP problem is hard to solve, it is very difficult for an adversary A to compute S_{ID}.

4.2 Performance Comparison

In this section, we compared the computational cost of our proposal with other existing scheme. Since, our proposal has the advantages of Blind Signature, ECC, and IBC, the overhead of public key revocation and certificate management is eliminated and most time consuming cryptographic operation such as bilinear pairing on elliptic curve does not affect our proposal.

To achieve 1024-bit RSA level security for pairing-based cryptosystem, we assume the Tate pairing defined over super-singular elliptic curve on a finite field F_q, where $|\mathrm{q}| = 512$ bits [24]. Same security level for ECC based scheme, we have to use secure elliptic curve on a finite field F_p, where $|\mathrm{p}| = 160$ bits [24]. We assume e, E, M_ecc and M_pair as pairing, modular exponentiation, ECC-based scalar multiplication and pairing-based scalar multiplication with running time 20.01 ms, 11.20 ms, 0.83 ms and 6.38 ms respectively [24].

As compared to bilinear pairing operations, ECC-based scalar multiplication, pairing-based scalar multiplication and modular exponentiation, the computation cost of hash function operation is very less. Thus, we ignored the computation cost of hash function operation. So, in order to compare the performance, we just focus on the pairing operations, ECC-based scalar multiplication, pairing-based scalar multiplication and modular exponentiation.

Table 1. Comparison of our proposed scheme with existing schemes, in terms of running computational cost (in ms) and signature size (in Bytes).

Proposal	Running cost (in ms)		Size of signature
	BlindSig	Verify	
Zhang et al.'s proposal [10]	1e + 6M_pair ≈ *58.29*	2e + 1E ≈ *51.22*	*148B*
Gao et al.'s proposal [13]	4e + 3M_pair ≈ *99.18*	4e ≈ *80.04*	*384B*
He et al.'s proposal [17]	5 M_ecc ≈ *4.15*	3 M_ecc ≈ *2.49*	*104B*
Dong et al.'s proposal [18]	6 M_ecc ≈ *4.98*	4 M_ecc ≈ *3.32*	*104B*
Tian et al.'s proposal [25]	2e + 6M_pair ≈ *78.30*	2e + 3_pair 59.16	*324B*
Our proposal	4 M_ecc ≈ *3.32*	3 M_ecc ≈ *2.49*	*104B*

Observation and result in [24, 26, 27] shows the running cost of pairing on elliptic curve, modular exponentiation operation and pairing-based multiplication operation is 24, 13 and 8 times the ECC-based multiplication operation. Using their observation, BlindSig algorithm in proposed proposal is 5.69%, 3.34%, 80%, 66.66% and 4.24% of Zhang and Kim's proposal [10], Gao et al.'s proposal [13], He et al.'s proposal [17], Dong et al.'s proposal [18] and Tian et al.'s proposal [25] respectively. The running cost of verify algorithm in proposed proposal is 4.86%, 3.11%, 100%, 75% and 4.20% of that in Zhang et al.'s proposal [10], Gao et al.'s proposal [13], He et al.'s proposal

[17], Dong et al.'s proposal [18] and Tian et al.'s proposal [25] respectively. Additionally, signature size generated in our proposal is 70.27%, 27.08%, 100%, 100% and 32.09% of that in Zhang et al. [10], Gao et al.'s proposal [13], He et al.'s proposal [17], Dong et al.'s proposal [18] and Tian et al.'s proposal [25] respectively, as shown in Table 1. Hence, the proposed ID-based blind signature gives better performance as compared against the previous schemes.

5 Application: E-Cash Payment System

In this section, we are presenting an online e-cash system based on our proposed ID-BS scheme. The proposed e-cash system consists of four entities: *Customers, Bank, Shop and Third Party*, which runs the six algorithms, namely, *Setup, Registration, Account-Opening, Withdrawal, Payment and Deposit*, to complete one transaction as given as follows:

Setup: Third party computes his public key against a random secret key. Third party publishes public parameter and keep secret key.

Registration: Third party registers and computes the bank private key corresponding to their unique identity and gives private key to bank.

Account-Opening: Customer requests for an account number to the Bank and got corresponding to his identity.

Withdrawal: Customer requests for an e-coin of face value f from Bank by providing his account information by running BlindSig sub-algorithm of our proposed ID-BS scheme. Bank verifies customer account by running Verify sub-algorithm, if correct, it releases e-coin (M, f, R, S, r) with face value f to customer.

Spending: With e-coin (M, f, R, S, r), Customer can purchase a product by paying amount f to shop. Shop first verifies the coin using Verify sub-algorithm. If it is valid, shop deposit this coin to the bank, otherwise, informs the customer for invalid coin.

Deposit: On receiving the e-coin (M, f, R, S, r), bank again checks the validity of e-coin by running the verify sub-algorithm. Bank adds this coin to his database, if the received coin is fresh, otherwise sends a warning message to shop for invalid e-cash.

6 Conclusion

In this paper, a new ID-BS scheme has been proposed that incorporates the benefits of Identity-Based Cryptosystem, Blind Signature and Elliptic Curve Cryptosystem whose security is based on the ECDLP. Additionally, under the random oracle model, proposed scheme is non-forgeable against the chosen message and identity attack, and holds the property of blindness. We compared our scheme with some existing schemes and found that our scheme gives better performance. Our proposed is suitable for implementing E-cash payment system. Proposed scheme suffers from key escrow problem which could be solved by using threshold key issuing [28], Hierarchical-Identity Based Encryption [29] techniques, etc.

Acknowledgement. This research work has been partially supported by the Council of Scientific and Industrial Research, a research and development organization in India, with sanctioned no. 09/263(1052)/2015 EMR-I and the UPE-II grant received from JNU. Additionally, the author would like to sincere thanks to the anonymous reviewers for their fruitful comments.

References

1. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2), 84–90 (1981)
2. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 199–203. Springer, Boston (1983). https://doi.org/10.1007/978-1-4757-0602-4_18
3. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
4. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
5. Kumar, M., Katti, C.P., Saxena, P.C.: An ID-based authenticated key exchange protocol. Int. J. Adv. Stud. Comput. Sci. Eng. **4**(5), 11–25 (2015)
6. Gray, D., Sheedy, C.: E-voting: a new approach using double-blind identity-based encryption. In: Camenisch, J., Lambrinoudakis, C. (eds.) EuroPKI 2010. LNCS, vol. 6711, pp. 93–108. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22633-5_7
7. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 319–327. Springer, New York (1990). https://doi.org/10.1007/0-387-34799-2_25
8. Islam, S.K.H., Amin, R., Biswas, G.P., Obaidat, M.S., Khan, M.K.: Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. Arab. J. Sci. Eng. 1–14 (2016)
9. Kumar, M., Katti, C.P.: An efficient ID-based partially blind signature scheme and application in electronic-cash payment system. ACCENTS Trans. Inf. Secur. **2**(6) (2017)
10. Zhang, F., Kim, K.: ID-based blind signature and ring signature from pairings. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 533–547. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_33
11. Zhang, F., Kim, K.: Efficient ID-based blind signature and proxy signature from bilinear pairings. In: SN, R., Seberry, J. (eds.) ACISP 2003. LNCS, vol. 2727, pp. 312–323. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-45067-X_27
12. Gao, W., Wang, G., Wang, X., Li, F.: One-round ID-based blind signature scheme without ROS assumption. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 316–331. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85538-5_21
13. Gao, W., Wang, G., Wang, X., Li, F.: Round-optimal ID-based blind signature schemes without ROS assumption (2012)
14. Elkamchouchi, H.M., Abouelseoud, Y.: A new blind identity-based signature scheme with message recovery. IACR Cryptol. ePrint Arch. 38 (2008)
15. Rao, B.U., Ajmath, K.A., Reddy, P.V., Gowri, T.: An ID-based blind signature scheme from bilinear pairings. Int. J. Comput. Sci. Secur. **4**(1), 98 (2010)
16. Hu, X.-M., Huang, S.-T.: Secure identity-based blind signature scheme in the standard model. J. Inf. Sci. Eng. **26**(1), 215–230 (2010)

17. He, D., Chen, J., Zhang, R.: An efficient identity-based blind signature scheme without bilinear pairings. Comput. Electr. Eng. **37**(4), 444–450 (2011)
18. Dong, G., Gao, F., Shi, W., Gong, P.: An efficient certificateless blind signature scheme without bilinear pairing. An. Acad. Bras. Cienc. **86**(2), 1003–1011 (2014)
19. Kumar, M., Katti, C.P., Saxena, P.C.: A new blind signature scheme using identity-based technique. Int. J. Control Theor. Appl. **10**(15), 115–124 (2017)
20. Vanstone, S.A.: Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments. Inf. Secur. Tech. Rep. **2**(2), 78–87 (1997)
21. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)
22. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). https://doi.org/10.1007/3-540-39799-X_31
23. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Springer, Berlin (2009). https://doi.org/10.1007/978-3-642-04101-3
24. Cao, X., Kou, W., Du, X.: A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf. Sci. (Ny) **180**(15), 2895–2903 (2010)
25. Tian, X.-X., Li, H.-J., Xu, J.-P., Wang, Y.: A security enforcement ID-based partially blind signature scheme. In: Web Information Systems and Mining, pp. 488–492 (2009)
26. He, D., Chen, J., Hu, J.: A pairing-free certificateless authenticated key agreement protocol. Int. J. Commun Syst **25**(2), 221–230 (2012)
27. Chen, L., Cheng, Z., Smart, N.P.: Identity-based key agreement protocols from pairings. Int. J. Inf. Secur. **6**(4), 213–241 (2007)
28. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
29. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_26