Research Article

ACCENTS Transactions on Information Security, Vol 2(6)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2017.26002

An efficient ID-based partially blind signature scheme and application in electronic-cash payment system

Mahender Kumar* **and C.P. Katti**
School of Computer & Systems Sciences, Jawaharlal Nehru University, Delhi, India

Abstract
A kind of blind signature, partially blind signature, allows a user to request the signatory authority on some pre-shared information such that signatory authority only sign the message but could not able to see to message's content except the pre-shared information. In 2007, an efficient and secure ID–based partially blind signature scheme has been presented by Hu et al, but this scheme is suffer from critical forgery attack identified by Tseng et al, in 2008. In 2009, using bilinear pairing in elliptic curve, Hu et al scheme was improved by Tian et al who tackles forgery attacks. Because the computational cost of bilinear pairing on an elliptic curve is more time consuming operation than the point multiplication on an elliptic curve. Fort this reason, we present a novel efficient identity-based partially blind signature scheme (ID-PBS) based on the hardness of gap Diffie-Hellman problem and elliptic curve discrete logarithm problem. The proposed ID-PBS scheme meets the security property of partially blind signature such as untraceability, non-forgeability, completeness, and non- deniability. Finally, we proposed an electronic-payment system based on our ID-PBS scheme.

Keywords
Identity based cryptosystem, Blind signature, Partially blind signature, Elliptic curve cryptosystem, Bilinear pairing.

1.Introduction
Blind signature is a new kind of digital signature with additional property that is, it allows a user to get a signature on message without leaking any information about message to Signatory authority. The notion of Blind signature is first introduced by Chaum [1, 2]. With the incorporated properties of blindness and Untraceability, it plays an important role in many e-commerce applications where user anonymity is the main concern such as e-payment system, e-wallet [3, 4]. However, experts feel that fully blinded signature have some disadvantages, for example, except the public information; bank could not access the malicious customer for double spent money [5-8]. A kind of Blind Signature, partially blind signature allows a user to request the signatory authority on some pre-shared information such that signatory authority only sign the message but could not able to see to message's content except the pre-shared information. Abe et al [9] was the first to propose the idea of PBS scheme which tackles the issues of fully blinded signature. To design an efficient, secure and flexible electronic cash payment, PBS scheme play an exceptional role.

*Author for correspondence

Many papers of PBS scheme based on traditional public key infrastructure have been presented in [5-10].

Using the technology of identity based encryption, blind signature scheme based on user identity is presented in [11-17]. In 2005, Chow et al [5] presented a secure ID- based PBS scheme based on solving the hardness of computational Diffie-Hellman problem. However, this scheme was capable to solve the issue of key managements but it requires large computational cost. Later, Hu et al [6] improve the Chows et al's ID-based PBS scheme and claims this scheme takes less computational cost and secure in random oracle. In 2009, Tian et al [7] proposed a corresponding approach to resolve the forgery attacks, pointed by Tseng et al [8] in 2008. All these scheme are based on bilinear pairing.

In order to solve the key management issues of public key infrastructure, Shamir [17] introduce a concept of identity based cryptosystem (IBC) in 1984, but does not implement it. The idea of identity based cryptosystem is that user's public key is derived from his Identity. Boneh [13] was the first to practically implement Identify based encryption (IBE) scheme using bilinear pairing. Later, several many IBE scheme based on bilinear pairing were proposed [18-

23]. Since last decade, it can be observe that the bilinear pairing has been playing a lead role in many applications in cryptography.

It is claimed in [16] that point multiplication on Elliptic Curve is 20 times faster than a pairing on two group points on elliptic curve. ECC takes less power consumption and less storage space than others, for example, bilinear pairing, RSA etc. Additionally, ECDLP is considered a harder problem as compared to the integer factorization and DLP. Vanstone [16] claimed that system using 128-bit ECC key achieved the same security as using the 1024-bit RSA key. In short, ECC takes less power consumption and less storage space which provides strong processing time. Thus, in the following paper, we are presenting a novel ID-based PBS scheme based on the hardness of computing ECDLP problem and GDH problem that satisfy all security properties of generic partial blind signature. Finally, we propose an electronic-cash payment system based on our ID-PBS scheme.

The arrangement of paper is as follows: section 2, briefly describes the preliminaries of elliptic curve cryptosystem, bilinear pairing, mathematical problems and security properties of PBS. Our ID-based PBS is presented in section 3. In section 4, the security and efficiency analysis of our proposed scheme is discussed. Section 5 present the e-cash payment system based on our proposed ID-PBS system, finally conclusion is shown in section 6.

2.Preliminaries

A. Elliptic curve cryptosystem

In 1985, Neal Koblitz [14] and Victor Miller [15] proposed a new kind of Public Key Cryptosystem. Because the cryptosystem is based on the Elliptic Curve, the new cryptosystem is referred to the Elliptic Curve Cryptosystem (ECC). In order to have an ability to improve the current cryptosystem concerning the parameters (such as having smaller key size, smaller system parameter, lower bandwidth and power requirements, and smaller hardware requirements), ECC is recommendable for the sake of high security and efficient computation.

Suppose the elliptic curve equation $y^2 = (x^2 + mx + n) mod p$, where $x, y \in F_p$ and $4m^2 + 27n^2 mod p \neq 0$. Formally, the Elliptic Curve is a set of points (x, y) which satisfied these equations and is an additive abelian group with point 0 (identity element). The condition $4m^2 + 27n^2 mod p \neq 0$ tells that $y^2 = (x^2 + mx = n) mod p$ 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:

$x_C = (u^2 - x_A - x_B) mod p$
$y_C = (u(x_A - x_C) - y_A) mod p$

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

It is noted that addition operation and multiplication operation in ECC are equivalent to modular multiplication and modular exponentiations in RSA respectively. Maintaining the Integrity of the Specifications

B. Bilinear Pairing

Suppose G_1 and G_2 are cyclic additive and cyclic multiplicative group of the same order q, and generator of G_1 be P. A map, e: G_1 X G_1 → G_2 is a bilinear map if satisfies the following three properties:

1. Bilinearity: For every X, Y ∈ G_1, and x, y ∈ Zq
   e(x.X, y.Y) = e(X, Y)^{xy}= e(x.y.X, Y)
2. Non-Degeneracy: If X is a generator of G_1 then e(X, X) is generator of G_2 that means if there exist X ∈ G_1 such that e(X, X) ≠ 1, where 1 is the identity element of G_2.
3. Computability: There must exist an algorithm that can efficiently compute e(X, Y) for every X, Y ∈ G_1.

C. Mathematical problem

Elliptic Curve Discrete logarithm problem (ECDLP): Consider Y = x.X where X, Y ∈ E_p(a, b), and x ∈ Z_q, it is computationally easy to compute Y from X and x. But it is very difficult to compute x from Y and X.

Computational Diffie-Hellman Problem (CDH). Given x, y ∈ □q, X ∈ G_1 and <X, x.X, y.X >, compute xyX.

Decision Diffie-Hellman problem (DDH). Given x, y, z ∈□q, X ∈ G_1 and < X, x.X, y.X, z.X > check whether z = x.y mod q.

Gap Diffie-Hellman problem (GDH). Group of problem where DDHP is easy while CDHP is hard.

D. Security property

Two important constraints required against the security of ID-based PBS scheme are: Partially Blindness property and Non-forgeability of additional Signature under parallel chosen message and ID attacks. Reader may refers [21] for more details. An ID-based PBS scheme is considered as secure if it fulfils the following two conditions:

Partially 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 them to *C*.
- *Challenge*: *C* uniformly chooses a random bit $b \in \{0, 1\}$ and ask *A* for signature on M_b and $M_{1-b.}$ Finally, *C* strips both the Signatures and gives the original signatures (σ_b, σ_{1-b}) to *A*.
- *Response*: A guesses bit b'$\in \{0, 1\}$ on tuple (M_0, M_1, σ_b, σ_{1-b}). *A* wins the game if $b = b'$ holds with probability $Pr[b = b'] > 1/2 + k^{-n}$.

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

- Setup: On random Security parameter *k*, the challenger *C* execute 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 on identity ID*, A response with n valid Message-Signature (M_1, $\sigma_1 = (S'_1, M'_1, y_1)$),. ($M_2$, $\sigma_2 = (S'_2, M'_2, y_2)$)….. ($M_n$, $\sigma_n = (S'_n, M'_n, y_n)$) such that
- Each message M_i is distinct from other Message M_j in given Message-Signature (M_1, $\sigma_1 = (S'_1, M'_1, y_1)$),. ($M_2$, $\sigma_2 = (S'_2, M'_2, y_2)$)….. ($M_n$, $\sigma_n = (S'_n, M'_n, y_n)$) set.
- *Adversary A* is restricted to ask an extract query on Identity *ID**.
- Execution of BlindSig algorithm is bounded by n.

Non-forgeability: An ID-based PBS 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-based PBS scheme is said to secure against one-more forgery, if no adversary *A* (t, q_E, q_B, k^{-n})-breaks the scheme.

Other important required properties of PBS scheme includes *Integrity* (Unauthorized Requester cannot alter the Message M), *Authenticity* (only an authentic SA can sign on Blinded Message), *Non-repudiation* (SA cannot deny having signed on a Blinded Message) and *Non-re-usability* (Signature generated for one Blinded Message cannot be applied to another Blinded Message).

3.Our ID-based PBS scheme

In this section, we introduce an ID-based PBS scheme based on ECDLP. *Figure 1* shows the structure of our ID-based PBS scheme.

A. Abbreviations and acronyms

Suppose *P* be the generator of group *G* of prime order *q*. Bilinear map e: G_1 X G_1 → G_2. Let the Four cryptographic hash function H_1: $\{0, 1\}^*$ → G_1, H_2: $\{0, 1\}^*$ → G_1, H_3: $\{0, 1\}^*$ → G_1 and H_4: G_2 → $\{0, 1\}^*$. Let the private key of Signatory authority and user is denoted as S_{IDS} and S_{IDU} respectively.

B. ID-PBS scheme

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

Extract: For a SA's identity ID_S, User identity ID_U and his master key *s*, PKG computes $S_{IDS} = s.Q_{IDS}$, where $Q_{IDS} = H_1(ID_S)$ and $S_{IDU} = s.Q_{IDU}$, where $Q_{IDU} = H_1(ID_U)$ and sends S_{IDS} and S_{IDU} to the SA and user respectively.

BlindSig: This algorithm consists of four steps, runs between SA and user.

Commitment: SA chooses a secret random integer $r \in Z_q$. Compute k and R and delivers R to user where, $k = H_4(e(S_{IDS}, rH_2(c)Q_{IDU}))$ and $R = rH_2(c)Q_{IDS}$.

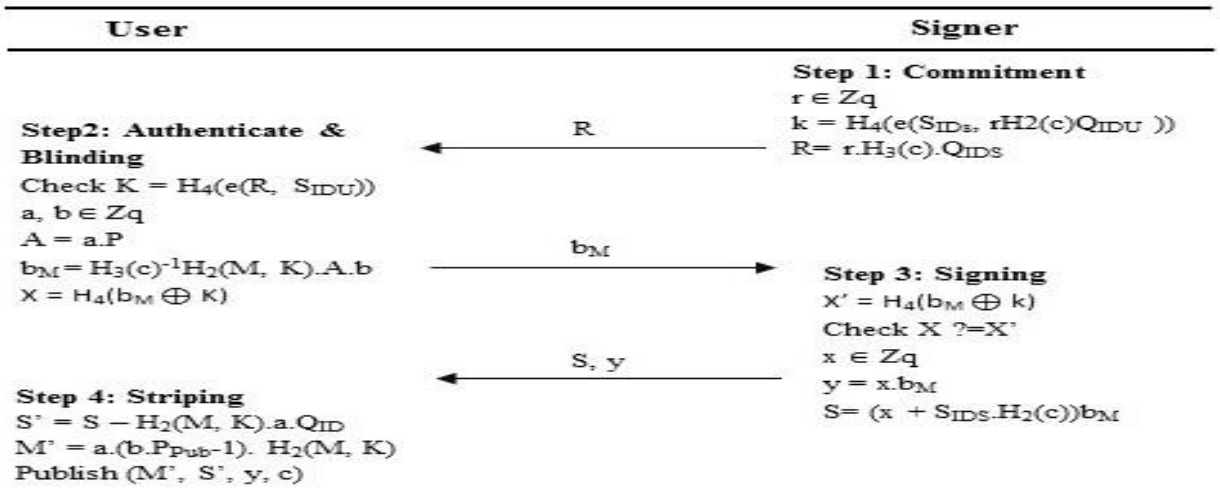

Figure 1 Proposed ID-based partial blind signature

Authenticating & Blinding: On given input R and his private key S_{IDU}, user compute $K = H_4(e(S_{IDU}, R))$. If any forging user wants to compute k with his private key S_{IDf}, he couldn't compute next step correctly because $k \neq K$. Only an authenticate user can proceed to next. Now, user chooses two random number $a, b \in Z_q$ as blinding factor. Compute $A = a.P$, blinded message $b_M = H_3(c)^{-1}H_2(M, K).A.b$ and $X = H_4(b_M \oplus K)$, then the user sends b_M and X to SA.

Signing: On given blinded message (b_M, X), the SA computes $X' = H_4(b_M \oplus k)$. if $X' = X$ holds, SA $x \in Zq$ and computes signature $y = x.b_M$ and $S= (x + S_{ID}.H(c))b_M$ using S_{IDS} and sends it to the user.

Stripping: On receiving the blinded signature (S, y) from SA, user strips it and computes the actual signature (S', M'), where
$S' = S – H_2(M, K).a.Q_{ID}$
$M' = a.(b.P_{Pub}-1). H_2(M, K)$

Finally, user publishes (M', S', y, c) for verification
Verify: On given (M', S', y, c), verifier with signer ID_S and accept the signature is valid if and only if
$y = S' - M'.Q_{IDS}$

4.Analysis of our scheme

This section gives the analysis of our proposed scheme in terms of security and computational efficiency.

A. Security analysis

Completeness: Following equations signify the completeness of our ID-based PBS scheme:
$y = S' - M'.Q_{IDS}$
$= S – H_2(M, K).a.Q_{IDS} - M'.Q_{IDS}$
$= S – H_2(M, K).a.Q_{IDS} - a.(b.P_{Pub}-1).H_2(M, K).Q_{IDS}$
$= S – H_2(M, K).a.Q_{IDS} - a.b.P_{Pub}.H_2(M, K).Q_{IDS} + a.H_2(M, K).Q_{IDS}$
$= S – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$= (x + S_{IDS})b_M – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$= x.b_M + S_{IDS}.H(c)b_M – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$=x.b_M + S_{IDS}.H_3(c).H_3^{-1}(c)H_2(M, K).A.b – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$= x.b_M + s.Q_{IDS}.H_2(M, K).a.P.b – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$= x.b_M + Q_{IDS}.H_2(M, K).a.P_{Pub}.b – a.b.P_{Pub}.H_2(M, K).Q_{IDS}$
$= x.b_M = y$

Non-forgeability: This proof is similar to the proof of Tian et al in [7]. Consider an Adversary A supposed to forge the signature, he should compute the correct value of $k = H_4(e(S_{IDS}, rH_2(c)Q_{IDU}))$. But private key is known only to the SA so he must choose random S_{IDA} as the private key or k_A as the share information to compute $k_A = H_4(e(S_{IDA}, r_A.H_2(c)Q_{IDU}))$ and subsequently compute $y_A = x_A.b_M$ and $S_A= (x_A + S_{IDA}.H_2(c))b_M$ with random choose r_A and x_A. finally, $S_A' = S_A – H_2(M, K).a.Q_{IDS}$ and $M' = a.(b.P_{Pub}-1). H_2(M, K)$ are computed on user side. The recipient can check the verification of signature through following equation:
$S_A' - M_A'.Q_{IDA}$
$= S_A – H_2(M, K).a.Q_{IDA} - M_A'.Q_{IDA}$
$= S_A – H_2(M, K).a.Q_{IDA} - a.(b.P_{Pub}-1).H_2(M, K).Q_{IDA}$
$= S_A – H_2(M, K).a.Q_{IDA} - a.b.P_{Pub}.H_2(M, K).Q_{IDA} + a.H_2(M, K).Q_{IDA}$
$= S_A – a.b.P_{Pub}.H_2(M, K).Q_{IDA}$
$= (x_A + S_{IDA})b_M – a.b.P_{Pub}.H_2(M, K).Q_{IDA}$
$= x_A.b_M + S_{IDA}.H(c)b_M – a.b.P_{Pub}.H_2(M, K).Q_{IDA}$

$= x.b_M + S_{IDA}.H_3(c).H_3^{-1}(c)H_2(M, K).A.b - a.b.P_{Pub}.H_2(M, K).Q_{IDA}$

$= x_A.b_M + S_{IDA}.H_2(M, K).a.P.b - S_{IDA}.H_2(M, K).a.P.b$

$= x_A.b_M = y_A \neq y$

To forge the signature, adversary must know S_{IDS}, r_A and x_A. Otherwise, the adversary could not forge the partially blinded signature on M.

Table 1 Comparison of our scheme with [5, 6, and 7]

Schemes	Computational cost			
	SA	User	Verify	Total
Chow et al [5]	$1G_1A + 4G_1M + 1MTP$	$3G_1A + 6G_1M + 1MTP + 2Z_qM + 2Z_qd$	$1G_1A + 1G_1M + 1MTP + 3Pa$	$5G_1A + 11G_1M + 3MTP + 3Pa + 2Z_qM + 2Z_qd$
Hu et al [6]	$1G_1A + 3G_1M + 1Z_qM$	$3G_1A + 3G_1M + 2Z_qM$	$1G_1A + 2G_1M + 2Pa$	$5G_1A + 8G_1M + 2Pa + 3Z_qM$
Tian et al [7]	$1G_1A + 3G_1M + 1Z_qM + 1Pa$	$1G_1A + 3G_1M + 2Z_qM + 1Pa$	$1G_1A + 3G_1M + 2Pa$	$3G_1A + 9G_1M + 4Pa + 3Z_qM$
Proposed	$1G_1A + 3G_1M + 1Z_qM + 1Pa$	$1G_1A + 4G_1M + 1Z_qM + 1Pa$	$1G_1A + 1G_1M$	$3G_1A + 8G_1M + 2Pa + 1Z_qM + 1Z_qd$

Additionally, in order to get the original signature, adversary could not forge the user. Suppose adversary wants to replace the original message M with forged message M', he should forge the value of k, which is equivalent to solve the GDP problem and computes $A_A = a_A.P$ and $b_{MA} = H(c)^{-1}H_2(M_A, K_A).A_A.b_A$ and $X_A = H_4(b_{MA}\ exor\ K_A) = X$. Because of the inconsistency, SA will refuse to sign on forged partially blinded signature b_{MA}.

Partially blindness: In *blinding* phase, user introduce two integers *a* and *b* as the blinding factor to blind a message *M*. So, signatory authority could not know about the content of message *M* except the pre-agreed information c. Additionally, the original Signature *(S', M')* could not reveal any information and also know the original signature as it would obtained by eliminating the blinding factor *a* and *b*, which is equivalent to solve the ECDLP.

Non-Repudiation: In signing phase, Signer signs on blinded message with his private key and the pre-computed information k is required to obtain the partially blinded signature in *BlindSig* Phase. Corresponding Public key of the signer is required in verify phase. Thus, the signer could not refuse the signature on message *M*.

B. Computational analysis

In this section, our proposed Identity-based partially based blind signature is compared in terms of computation cost, with existing scheme [5, 6, 7] shown in *Table 1*. Here, according to [6], we represent G_1A as the point addition on elliptic curve G_1, G_1M as the point multiplication on elliptic curve G_1, *Pa* denote as the pairing operation on elliptic curve, *MTP* represent as the map-to-point hashing operation, Z_qM denotes the multiplication operation on Z_q and Z_qd denotes the division operation on Z_q. Among these operations, pairing on elliptic curve is considered as the most time consuming operation. However, [19, 20] improves the complexity of pairing operation, but the pairing on elliptic curve is still a time consuming task. Readers may easily see that verify phase takes only $1G_1M$ and $1G_1A$ operations, avoids pairing operation as compared to [5], [6] and [7] which consumes 3, 2 and 2 pairing operations respectively. Generally, signature is created once and published, but it requires verify many times for validity at recipients. In such environment our approach may considered gives better performance as it consumes less number of pairing operation which avoids map-to-hash operations at verification side. If we talk about the participation of pairing operation in total computational time, our scheme takes 2 pairing operations as compared to [5], [6] and [7] which consumes 3, 2 and 4 pairing operations respectively. Additionally, our scheme avoids the map-to-hash operation with less G_1A and G_1M operations.

5.Application in E-Cash

Recall from our proposed ID-based PBS scheme, an e-cash payment system based on it has been presenting. Suppose four entities involves in an e-cash payment system: Customers C, Bank B, Shop S and Third Party T, which going through the following six stages to complete one transaction: Setup, Registration, Account-Opening, Withdrawal, Spending and Deposit.

1. **Setup:** Identical to setup phase in our proposed model, Third party T selects random integer $s \in Z_q$ and computes public key $P_{Pub} = s.P$. T publishes

PARAMS = {*G, q, P, P_{Pub}, H_1, H_2, H_3, H_4*}, and keep secret key *s* secretly.

2. **Registration**: Bank B registered itself with T against their Identity ID_B. *T* computes *B's* private key $S_{IDB} = s.Q_{IDB}$ and C's private key $S_{IDC} = s.Q_{IDC}$ with his master key s, where $Q_{IDB} = H_1(ID_B)$and $Q_{IDC} = H_1(ID_C)$. Now, T then sends S_{IDB} and S_{IDC} securely to B and C respectively.
3. **Account-Opening**: To open an account in Bank B, Customer C runs Account-Opening-Stage algorithm. B recognized C through his unique Identifier ID_C (which may include the Ration Card, Voter-Identity Card, Passport, Social Security number etc.). B chooses $x \in Z_q$ and computes $A_{CC} = x.Q_{IDC}$, where $Q_{IDC} = H_1(ID_C)$ and sends A_{CC} to the C. On successfully opening an account in Bank B, C can issue an amount in the form of electronic from B.
4. **Withdrawal**: Customer C runs Withdrawal-Stage, when he requires to issue an e-cash of face value *f* from Bank B with sending his account information A_{CC}. Bank B verified A_{CC} if correct, C is allowed to get e-cash with face value *f* from B. Now the rest of the process will process as follows:

- B chooses a secret random integer $r \in Z_q$. Compute $k = H_4(e(S_{IDB}, rH_2(c)Q_{IDC}))$ and $R = rH_2(c)Q_{IDB}$ and delivers R to C.
- On given parameters R and his private key S_{IDS}, C computes $K = H_4(e(S_{IDC}, R))$. If any forging customer wants compute *k* with his private key S_{IDf}, he couldn't compute next step correctly because $k \neq K$. Only an authenticate customer can proceed to next. Now, C chooses two random number $a, b \in Z_q$ as blinding factor and *f* as face value and compute $A = a.P$, blinded message $b_M = H_3(c, f)^{-1}H_2(M, K).A.b$ and $X = H_4(b_M \oplus K)$. Then the user sends *f*, b_M and *X* to SA.
- S*igning*: On given blinded message (b_M, X), the B computes $X' = H_4(b_M \oplus k)$. if $X' = X$ holds, B chooses $x \in Z_q$ and compute signature $y = x.b_M$ and $S = (x + S_{IDB}.H(c, f))b_M$ using their private key S_{IDB} and sends it to the user.
- Now, On receiving the partially blinded signature (S, y) from B, C strips it and computes the actual signature (S', M'), where $S' = S - H_2(M, K).a.Q_{IDB}$ and $M' = a.(b.P_{Pub}\text{-}1).H_2(M, K)$ and sends the e-cash (*S', M', f, y, c*) to C.

5. **Spending:** To purchase items, C runs Spending protocol as follows:

- C sends e-cash (*S', M', f, y, c*) to shop S.
- S first verifies the correctness of e-cash (*S', M', f, y, c*) with B's public key P_{Pub} if the equation $y = S' - M'.Q_{IDS}$ holds.
- If e-cash is valid, S delivers the e-cash (*S', M', f, y, c*) to Bank B for double-spending of e-cash. Otherwise, S informs the C for invalid payment and discard the e-cash.

6. **Deposit**: On receiving an e-coin (*S', M', f, y, c*) from shop S, B runs Deposit protocol as follows:

- B checks the validity by running the *verify* phase of proposed ID-PBS scheme, if the $y = S' - M'.Q_{IDS}$ holds. To detect the double-spending of e-cash, B will check his database whether the received e-cash is fresh.
- If yes, B add an amount of money *f* to S's account and sends a validity message to S.
- Otherwise, B sends a warning message to S which indicate the invalid e-cash.

Because proposed e-cash payment system is based on ID-based partial blind signature scheme, so it holds the security property of Non-forgeability and partially blindness. Non-forgeability of e-coin denotes that a user cannot spend more coins than the number of coin he withdrawal. Whenever, customer requests for an e-coin by providing his identity and face value *f*, bank creates an e-coin for customer and stores in his database. If any customer wants to spend an e-coin two or times, at the time of deposit bank could check their database for detecting double spent an e-coin.

6.Conclusion

PBS is a kind of blind signature which allows signatory authority to sign a PBS on message M having some pre-agreed information. In given paper, an efficient and secure identity-based PBS scheme has been proposed that incorporates the benefits of IBC, PBS system and ECC. Proposed ID-PBS scheme takes less computational power as compared to Chow et. al., Hu et. al., and Xia et. al, as shown in *Table 1*. For example, in m-transferable e-cash payment system, single e-coin is spends m times and then deposit to the bank B so it runs $(m+1)^{th}$ times the *verify* phase. Recall that our scheme consumes less computation cost in *verify* phase. It can predict that proposed scheme is more comfortable for m-transferable e-cash system. Because our scheme is based on the ECDLP and GDP; so, it achieves the same security with less computation cost. Finally, we have built an e-cash system based on our proposed ID-PBS system, which provides the customer anonymity, Non-forgeability, and detects the Double Spending e-coin.

Acknowledgment
This research work has been partially supported by the Council of Scientific and Industrial Research, a research and development organisation 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

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Chaum D. Blind signatures for untraceable payments. In advances in cryptology 1983 (pp. 199-203). Springer US.
[2] Chaum D, Fiat A, Naor M. Untraceable electronic cash. In proceedings on advances in cryptology 1990 (pp. 319-327). Springer Berlin Heidelberg.
[3] Wang H, Zhang Y. A protocol for untraceable electronic cash. In international conference on web-age information management 2000 (pp. 189-97). Springer Berlin Heidelberg.
[4] Wang H, Zhang Y, Cao J. An electronic cash scheme and its management. Concurrent Engineering. 2004; 12(3):247-57.
[5] Chow SS, Hui LC, Yiu SM, Chow KP. Two improved partially blind signature schemes from bilinear pairings. In australasian conference on information security and privacy 2005 (pp. 316-28). Springer Berlin Heidelberg.
[6] Hu X, Huang S. An efficient ID-based partially blind signature scheme. In software engineering, artificial intelligence, networking, and parallel/distributed computing, 2007. SNPD 2007. Eighth ACIS international conference on 2007 (pp. 291-6). IEEE.
[7] Tian XX, Li HJ, Xu JP, Wang Y. A security enforcement ID-based partially blind signature scheme. In international conference on web information systems and mining 2009 (pp. 488-92). IEEE.
[8] Tseng YM, Wu TY, Wu JD. Forgery attacks on an ID-based partially blind signature scheme. International Journal of Computer Science. 2008; 35(3):301-4.
[9] Abe M, Fujisaki E. How to date blind signatures. In international conference on the theory and application of cryptology and information security 1996 (pp. 244-51). Springer Berlin Heidelberg.
[10] Islam SH, Amin R, Biswas GP, Obaidat MS, Khan MK. Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. Arabian Journal for Science and Engineering. 2016:1-4.
[11] Zhang F, Kim K. Efficient ID-based blind signature and proxy signature from bilinear pairings. In australasian conference on information security and privacy 2003 (pp. 312-23). Springer Berlin Heidelberg.
[12] Zhang F, Kim K. ID-based blind signature and ring signature from pairings. In international conference on the theory and application of cryptology and information security 2002 (pp. 533-47). Springer Berlin Heidelberg.
[13] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In annual international cryptology conference 2001 (pp. 213-29). Springer Berlin Heidelberg.
[14] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987; 48(177):203-9.
[15] MilierV S. Use of elliptic curve in cryptography. Advannce in Cryptology-CRYPTO. 85:417-26.
[16] Vanstone SA. Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report.1997;2(2):78-87.
[17] Shamir A. Identity-based cryptosystems and signature schemes. In workshop on the theory and application of cryptographic techniques 1984 (pp. 47-53). Springer Berlin Heidelberg.
[18] Kumar M, Katti CP, Saxena PC. An id-based authenticated key exchange protocol. International Journal of Advanced Studies in Computers, Science and Engineering. 2015;4(5):11-25.
[19] Barreto PS, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. In annual international cryptology conference 2002 (pp. 354-69). Springer Berlin Heidelberg.
[20] Barreto PS, Lynn B, Scott M. On the selection of pairing-friendly groups. In international workshop on selected areas in cryptography 2003 (pp. 17-25). Springer Berlin Heidelberg.
[21] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of cryptology. 2000;13(3):361-96.
[22] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM conference on computer and communications security 2008 (pp. 417-26). ACM.
[23] Choon JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. In international workshop on public key cryptography 2003 (pp. 18-30). Springer Berlin Heidelberg.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.