Noname manuscript No.
(will be inserted by the editor)

Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system

SK Hafizul Islam · G. P. Biswas

Received: date / Accepted: date

Abstract The blind signature scheme permits the user to acquire a signature from the signer; however, the message and the final signature are unknown to the signer. In a partially blind signature (PBS) scheme, the signer can explicitly incorporate a common information in the signature based on some agreement with the user and without violating the blindness property. Many PBS schemes have been proposed recently either by using certificate authority-based public infrastructure (CA-PKI) or pairing along with map-to-point function. The CA-PKI-based PBS scheme needs huge computation and storage to keep public keys and certificates. On the other hand, pairing and map-to-point function are costly operations. Thus, the ID-PBS scheme without pairing is more appropriate for real environments, and an efficient pairing-free ID-PBS scheme is proposed in this paper. In the random oracle model, our scheme is analyzed to be provably secure. The proposed scheme is used to design an online e-cash system, in which a bank agrees on a common piece of information with a customer and can blindly sign some messages. It may be noted that our e-cash system has the properties of unforgeability, unlinkability, and non-deniability and can prevent the double-spending of e-cash.

Keywords Identity-based cryptosystem · Elliptic curve · Bilinear pairings · Partially blind signature · Electronic cash · Double-spending

1 Introduction

With the rapid growth of network technologies, e-commerce gains increasing demand due to its many applications such as electronic payment, electronic funds transfer, financial electronic data exchange, supply chain management, internet marketing, inventory management

SK Hafizul Islam **(Corresponding author)**
Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India.
Tel.: +91-8797369160
E-mail: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in
G. P. Biswas
Department of Computer Science and Engineering, Indian School of Mines Dhanbad, Jharkhand 826 004, India.
E-mail: gpbiswas@gmail.com

systems, automated data collection system, etc. There are different types of electronic payment systems such as (1) online credit card payment [1], [2] (2) smartcard-based electronic payment [3], (3) electronic cheque (e-cheque) [4], [5], (4) e-cash system [6], [7], [8] have been proposed. Nowadays e-cash system becomes more and more popular because it can ensure the privacy of customers, the risk of customer identity theft and customer fraud in various electronic transactions [9]. However, the efficient implementation of an e-cash system is still an important issue in the electronic commerce research area. To design an efficient e-cash system, Chaum [10] firstly proposed the notion of blind signature scheme that allows a user to acquire a signature from the signer on a message. However, the content of the message and the final blind signature are not known to the signer. In general, e-cash system can be categorized as (1) online e-cash system [6], [8], [11], [13], [12], [14], [15], [16] and (2) offline e-cash system [7], [11], [12], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28].

In general, e-cash model consists of three entities like a bank, a customer and a merchant, and requires following protocols for *opening an account*, *bank registration*, *e-cash withdrawl*, *e-cash payment* and *e-cash deposit*. To acquire some goods or service from a merchant, the user first withdraws an e-cash from the bank and then handover to the merchant. Finally, the merchant verifies the e-cash and deposit it to the bank. After validating the e-cash, the bank credited merchant's account. One of the most important properties of any e-cash system is the prevention of *double-spending*. Since e-cash is digital data, which can be copied easily and thus it may be spent more than one time either by dishonest customer or merchant. In an online e-cash scheme, payment and deposit steps took place in a single transaction i.e., the e-cash is checked by the bank during payment and thus, the bank stays online in each transaction and to prevent the double-spending of e-cash, the merchant must confer with the bank before accepting any e-cash. In case of offline system, bank stays offline and the merchant accepts an e-cash anonymously from the customer, and later the bank checks the validity of e-cash. Subsequently, the bank has applied some efficient mechanism that can identify the double-spending of e-cash. In addition, the bank verifies the e-cash after the transaction, so the risk of *double-spending* is very high in offline system. Thus, the offline e-cash is suitable for payment systems that includes transaction with small amounts, however, for applications involving large payment amounts, the online e-cash is more suitable. In this article, we will construct a robust and efficient online e-cash system for payment of any amounts.

As we know, customer anonymity is of great importance in e-cash [8], [14], so the blind signature [29], [30], which hides customer identity, can play an important role in this application. For e-cash system, anonymity ensures that the bank and the merchant cannot trace the customer from the e-cash spent previously. Although the blind signature achieves the property of *blindness*, *anonymity*, *verifiability* and *unforgebility*, it cannot be applied fully in e-cash system for real-life applications due to some limitations. Some of them are given now. For different face value of e-cash, the bank must keep different private and public key pairs as the customer provides the face value of e-cash. For this, the customer and merchant includes the list of bank's public keys in some electronic tokens. In addition, to prevent the forgery of the double-spending of same e-cash, it is also required by a bank to keep information about all previously spent e-cashes. Accordingly, the size of the bank's database increases over time. As the inclusion of face value, time, and expiration date of e-cash are not possible in blind signature, therefore, the blind signatures are not suitable for simple e-cash system.

Abe and Fujisaki [31] put forwarded the concept of partially blind signature (PBS) scheme. In a PBS scheme, signer and user first negotiate a common information, which

is to be included in the signature and then the user obtains a blind signature, which is constructed by the signer by signing a blinded message. The final partially blind signature explicitly includes some commonly agreed information, which are visible without violating the blindness property. Therefore, PBS scheme removes the disadvantages of blind signature schemes such as (1) the bank is allowed to incorporate some common information like *expiration time*, *date*, *face value* into each e-cash; (2) the signer and merchant are not restricted to keep the list of bank's public keys; and (3) the size of the bank's database used to store the e-cashes those has been spent previously would be limited in size over time.

1.1 Previous works

In 1983, Chaum [10] gave the definition of blind signature scheme since then many such techniques are implemented in the literature by means of traditional CA-PKI or Shamir's [32] identity-based cryptosystem (IBC). Eslami and Talebi [7] proposed an untraceable offline e-cash system using RSA-based blind signature under the assumptions that the discrete logarithm problem (DLP) and integer factorization problem (IFP) are intractable in a large cyclic group of prime order. Their scheme can exchange the old e-cash into new ones by adopting a mechanism called an exchange protocol that can greatly reduce the bank's database. Also, their scheme employed ElGamal signature to prevent the double-spending of e-cash. Based on the map-to-point (MTP) function and bilinear pairings, in 2005, Chow et al. [33] first devised an identity-based partially blind signature (ID-PBS) scheme. Their scheme is efficient and eliminates the public key certificate compared to other CA-PKI-based PBS schemes. However, the scheme [33] requires some expensive computations to be carried out by the users. Abe and Okamoto [34] gave the definition of formal security of their scheme. Based on the hardness of the quadratic residue problem (QRP), Fan and Lei [35] proposed a PBS scheme. Zhang et al.'s scheme [36] proposed another PBS scheme using bilinear pairings.

Based on the discrete logarithm problem (DLP) and Chinese Remainder Theorem (CRT), in 2003, Huang and Chang [29] proposed a novel PBS scheme and they state that the scheme gives required security and computation efficiency. Unfortunately, Zhang and Chen [37] show that the scheme [29] cannot achieve the partial blindness property in which an adversary can forge the signer's signature by incorporating a forge blind factor and removing the original blind factor. In 2008, Hu and Huang [38] constructed an ID-PBS scheme with bilinear pairings and argued that is it provably secure against the random oracle model [39]. However, the forgery of Hu and Huang' scheme [38] is possible as proven by Tseng et al. [40]. Chen et al. [41] first proposed an ID-based restrictive PBS from bilinear pairings by incorporating the advantages of PBS scheme and restrictive blind signature. Hu and Huang [38] analyzed that the scheme [41] is insecure and it does not satisfy *restrictiveness property* and *double-spending*. Lin et al. [23] proposed a provably secure self-certified PBS scheme and a security model, and analyzed that it is secured in the designed model, but, Zhang and Gao [42] analyzed that Lin et al.'s scheme [23] is weak insecure where an adversary can create a forged signature on any message.

1.2 Our contributions

We have studied several blind signature or PBS schemes in the previous subsection, which shows that the most of them are not applicable in e-cash system due to high computation

costs [33], [34]. Also, some of the schemes do not meet the security criteria such double-spending [38], [41], unforgebility [38], [40], partial blindness [37], [43], non-repudiation [42], [44] of an e-cash system. In addition, for practical implementation, all of the aforementioned schemes can be realized either by using CA-PKI-based cryptosystem or bilinear pairings with a special hash function, called map-to-point function [63], [64], [65]. As we know, CA-PKI-based PBS schemes need huge computation and storage costs to manage the public keys and certificates. Also, the computational cost of the bilinear pairing and the probabilistic map-to-point hash function is high compared to other cryptographic operations [45], [46], [47]. Thus, ID-PBS scheme without bilinear pairing requires less computation cost and easily implementable and none of such schemes proposed so far, the ID-PBS scheme without bilinear pairings will be more appropriate for practical applications [63].

Recently, many secure and computation efficient pairing-free protocols have been proposed in [48], [49], [50], [51], [52], [53], [54], [55], [56]. Based on elliptic curve [63], [64], [65] and Schnorr's signature [57], in this paper, we proposed a pairing-free ID-PBS scheme. From our analysis, one can observe that our scheme is robust and computation cost than other PBS schemes. Our scheme is also provably secure in the random oracle model [39] based on the infeasibility of elliptic curve discrete logarithm problem. We then develop an efficient and secure online e-cash system using the proposed pairing-free ID-PBS scheme, which has real-life applications.

1.3 Outline of the paper

We organized the paper as follows. Section 2 provides basic information about the elliptic curve group, computational problem and zero-knowledge protocol. In section 3, formal definition of the ID-PBS scheme is given. The security properties of ID-PBS scheme are addressed in Section 4. Section 5 describes the proposed scheme and its analysis is presented in Section 6. Based on our ID-PBS scheme, an efficient online e-cash system and its security discussion are implemented in Section 7. Finally, Section 8 summarizes the paper.

2 Preliminaries

2.1 Backgrounds of elliptic curve

Let E/F_p be a set over the prime field F_p, which consisting the point from the following equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \tag{1}$$

where $x, y, a, b \in F_p$ and $(4a^3 + 27b^2) \bmod q \neq 0$. We defined $G = \{(x, y) : x, y \in F_p$ and $(x, y) \in E/F_p\} \cup \{O\}$, is an additive cyclic group, where the point *"O"* served as the identity element. The point *"O"* is known as *"point at infinity"* or *"zero point"*. A brief discussion about the elliptic curve group properties [58], [59], [63], [64], [65] is given below:

- **Point addition**. Let P, Q are two points on the curve (1), then $P + Q = R$, where the line joining P and Q intersects the curve (1) at $-R$, and the reflection of it with respect to the *x-axis* is the point R.

- **Point subtraction**. If $Q = -P$, then $P + Q = P - P = O$, the line joining P and $-P$ intersects the curve (1) at O.
- **Point doubling**. Point doubling is the addition of a point P on the curve (1) to itself to obtain another point Q on (1). Let $2P = Q$, the tangent line at P intersects the curve (1) at $-Q$; reflection of it with respect to the *x-axis* is the point Q.
- **Scalar point multiplication**. We define the scalar point multiplication as $kP = P + P + \cdots + P$ (k times), where $k \in Z_p^*$ is a scalar.
- **Order of a point**. We can say the point P has order n if $nP = O$, where $n > 0$ is the smallest integer.

2.2 Cryptographic assumptions

Definition 1 (Elliptic curve discrete logarithm problem (ECDLP)) Given $\langle P, Q \rangle$, it is hard to output a such that $Q = aP$ and $a \in_R Z_p^*$. The probability that a polynomially bounded algorithm $\mathcal{A}$ can solve the ECDLP is defined as $Succ_{\mathcal{A},G}^{ECDLP} = Pr[\mathcal{A}(P, Q) = a : a \in Z_p^*, Q = aP]$.

Definition 2 (Elliptic curve discrete logarithm (ECDL) assumption) The success probability $Succ_{\mathcal{A},G}^{ECDLP}$ is negligible for every probabilistic polynomial-time algorithm $\mathcal{A}$.

2.3 Zero-knowledge protocol based on ECDLP

In this section, we described the elliptic curve version of zero-knowledge protocol based on ECDLP. It is used to prove to the *Verifier* that the *Prover* knows the secret x such that $Q = xP$ without revealing the secrecy of x to the *Verifier*. Initially, *Prover* and *Verifier* agree on G over F_p and a generator $P \in G$. They both know $Q \in G$ and *Prover* claims that he knows x. He then runs the following four steps and if *Verifier*'s check in the forth step is correct, then the *Prover* proofs to the *Verifier* that he knows the secret x.

- *Prover* selects $r \in_R Z_p^*$, executes $T = rP$ and delivers it to the *Verifier*.
- *Verifier* chooses $c \in_R Z_p^*$ and forwards it to the *Prover*.
- *Prover* executes $s = r + cx \pmod p$ and delivers it to the *Verifier*.
- *Verifier* verifies that whether $T = sP - cQ$ holds, i.e., $sP - cQ = (r + cx)P - cQ = rP + cxP - cxP = rP = T$.

2.4 Zero-knowledge test of elliptic curve discrete logarithm equality

Suppose that *Prover* knows two publicly known points P and Q of a group G that have the same discrete logarithm x. The *Prover* argues that he knows x such that $Y_1 = xP$ and $Y_2 = xQ$ and wants to prove the knowledge of this fact without revealing x. The *Prover* and *Verifier* first agree on G over F_p and then execute the following procedure:

- *Prover* selects $r \in_R Z_p^*$, performs $T_1 = rP$ and $T_2 = rQ$, and then delivers (T_1, T_2) to the *Verifier*.
- *Verifier* chooses $c \in_R Z_p^*$ and forwards it to the *Prover*.
- *Prover* calculates $s = r + cx \pmod p$ and delivers it to the *Verifier*.
- *Verifier* examines whether $sP - cY_1 = (r + cx)P - cxP = rP + cxP - cxP = rP = T_1$ and $sQ - cY_2 = (r + cx)Q - cxQ = rQ + cxQ - cxQ = rQ = T_2$ hold.

3 Definition of an ID-PBS scheme

The concept of the formal definition of PBS scheme is given by Abe and Okamoto [34], where it is assumed that a signer and a user first agree on a common information Δ (say) that is composed of the information of the user and the signer. In real-life applications, Δ may be calculated by both user and signer, while in some other situations the signer selects Δ and delivers it to the signer. The information Δ as a part of the signature σ (say) is computed according to the information of the user and signer represented by Δ_1 and Δ_2, respectively. For example, let us assume that Δ is used to add a validity date to a signature, and in that case, Δ_1 would hold the information that the user wants to have a signature with any validity date, and on the other hand, Δ_2 would hold the information that the signer does only sign with a validity period for a week (say). Thus, Δ would then hold the corresponding validity date with the duration of one week. The definition of ID-PBS scheme is given below.

Definition 3 An ID-PBS scheme consists of the following four algorithms: *Setup*, *Extract*, *Issue* and *Verify* whereas the *Issue* one composed of five algorithms, called *Agree*, *Commitment*, *Blind*, *Sign* and *Unblind*.

- **Setup:** The PKG runs this probabilistic polynomial time (PPT) algorithm. The inputs of this algorithm is the security parameter $k \in \mathbb{Z}^+$ and the output are the system's parameter Ω, master private key msk and master public key mpk. The system's parameter Ω is publicly known, while msk is kept secret by PKG.
- **Extract:** The PKG executes this algorithm, which takes the system's parameter Ω, an identity ID_i as input and returns the private/public key (d_i, P_i) as output. The PKG deliver the private key d_i to the user ID_i through a secure channel.
- **Issue:** Assume that the signer ID_i issues a blind signature for the user without knowing the original message. Now using this algorithm (by both user and signer) that takes a message $m \in \{0,1\}^*$, the system's parameter Ω, and $(ID_i, d_i, P_{pub}, \Delta)$ as input and outputs the signature σ in the following way:
  - **Agree:** The user negotiates a public and common information Δ with the signer ID_i whose public key is P_i. The agreed information Δ is to be attached to the signed message m for final signature generation.
  - **Commitment:** On input of a random string r, the signer ID_i makes a commitment R and sends it to the user.
  - **Blind:** On input of two random strings a, b and a message m, the user generates a string h then it is sent to the signer ID_i. The value h is used to sign the message m blindly by ID_i.
  - **Sign:** On input of h and d_i, this algorithm returns σ', and then delivers σ' to the user.
  - **Unblind:** On input of σ' and blind factors a, b, it returns σ as the unblinded signature.
- **Verify:** This algorithm accepts $(\Omega, \sigma, m, \Delta, ID_i, P_i)$ as input and outputs "1" if (m, Δ, σ) is valid against (Ω, ID_i, P_i), and "0" otherwise.

4 Security properties of an ID-PBS scheme

The following properties must be satisfied by an ID-PBS scheme.

– **Completeness:** The partially blind signature (m, Δ, σ) can be verified by anyone. If *Verify*$(ID_i, P_i, \Delta, m, \sigma) = 1$ holds, then (m, Δ, σ) it is correct, otherwise the signature is incorrect.

Definition 4 If the user and the signer correctly follow the signature generation protocol, then the signature scheme is said to complete if, for every $n > 0$, there exists a k_0 such that the signer returns *completed* and Δ, and the user returns (m, Δ, σ) that fulfills Verify$(ID_i, P_i, \Delta, m, \sigma) = 1$ with the probability at least $(1 - 1/k^n)$ for $k > k_0$.

– **Partial blindness:** In any PBS scheme, one of the important properties is *partial blindness*, which is defined in terms of the following *unlinkability* game executed by an algorithm/challenger $\mathcal{C}$ and a polynomial time adversary $\mathcal{A}$.
  – **Setup:** $\mathcal{C}$ accepts $k \in \mathbb{Z}^+$ as input and executes this algorithm to calculate Ω and msk. $\mathcal{C}$ sends Ω to $\mathcal{A}$ and kept msk away from $\mathcal{A}$.
  – **Preparation:** $\mathcal{A}$ selects two different messages m_0 and m_1, Δ and an identity ID_i, and delivers them to $\mathcal{C}$.
  – **Challenge:** $\mathcal{C}$ takes a random bit $b \in \{0, 1\}$, and asks $\mathcal{A}$ to partially sign (m_b, Δ) and (m_{1-b}, Δ). Now, $\mathcal{C}$ unblinds both the signatures and returns the signature of m_b to $\mathcal{A}$.
  – **Response:** $\mathcal{A}$ returns the guess bit b'. We can say $\mathcal{A}$ wins the game if $b' = b$ holds.

Definition 5 An ID-PBS scheme fulfills the the partial blindness, if for every constant $n > 0$, there exists a bound k_0, $\mathcal{A}$ returns a guess bit b' such that $b' = b$ holds with probability at most $(1/2 + 1/k^n)$ for $k > k_0$.

– **Unforgeability:** In any PBS scheme, *unforgeability* is an important property which ensures that other than the signer anyone cannot produce the valid signature on a message. To define the *unforgeability*, we introduced a *challenge-response* game as described below. This game is simulated by the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$. In this game, the $\mathcal{A}$ acts as user and the challenger $\mathcal{C}$ acts as signer.
  – **Setup:** $\mathcal{C}$ accepts $k \in \mathbb{Z}^+$ as input and runs the *Setup* algorithm to compute the system's parameter Ω, master secret key msk. The challenger $\mathcal{C}$ sends the system's parameter Ω to the adversary $\mathcal{A}$.
  – **Hash queries:** $\mathcal{A}$ can ask the output of hash function for the selected input.
  – **Extract queries:** $\mathcal{A}$ takes an identity ID_i and delivers it to $\mathcal{C}$. $\mathcal{C}$ then calculates the private key d_i by executing *Extract* algorithm and sends d_i to $\mathcal{A}$.
  – **Issues queries:** $\mathcal{A}$ picks a message m, an information Δ, an identity ID_i and public key P_i of ID_i and delivers (ID_i, P_i, m, Δ) to $\mathcal{C}$. $\mathcal{C}$ then computes a signature σ and delivers it to $\mathcal{A}$.
  – **Forgery:** At the end of this game, $\mathcal{A}$ returns $(m^*, \Delta^*, \sigma^*, ID_i^*, P_i^*)$, which must follow the conditions given below:
    - σ^* must satisfies *Verify* algorithm.
    - $\mathcal{A}$ is not allowed to ask the Extract query for the signer ID_i^*.
    - The tuple $(m^*, \Delta^*, ID_i^*, P_i^*)$ has never been submitted for *Issue* oracle.

Definition 6 An ID-PBS scheme is existential unforgeable in the random oracle model under the adaptive chosen message and identity attacks if there is no polynomial-time bounded adversary who can win the above challenge-response game with non-negligible advantage.

5 The proposed pairing-free ID-PBS scheme

We motivated from Schnorr's signature scheme [57] and identity-based pairing-free schemes proposed in [48], [49], [50], [51], [52], [53], [54], [55], [56], and proposed an efficient and secure pairing-free ID-PBS scheme using ECC [63], [64], [65]. In our scheme, there are three entities namely a trusted authority PKG, a signer B and a user C. For any partially blind signature, B and C must agree on a common information Δ. The PKG is responsible to generate the system's parameter Ω and helps the signer B to construct a correct blind signature σ for C on a message m and a common information Δ. The proposed ID-PBS scheme includes the following algorithms: *Setup*, *Extract*, *Issue* and *verify*, as described below. It may be noted that in our proposed ID-PBS scheme, the user and signer must prove their witness using zero-knowledge protocol before executing the signature issuing protocol. The notations employed in our scheme is explained in Table 1.

Table 1 Various notations and their meaning used in the proposed scheme.

Notation	Meaning
$C/B/M$	The User (Customer)/Signer (Bank)/Merchant
ID_i	Identity of the entity i
F_p	A prime field of order q
E/F_p	Set of elliptic curve points
G	Additive cyclic group of elliptic curve points
p	k-bit prime number
P	Generator of G
x	Private key of PKG
P_{pub}	Public key of PKG, where $P_{pub} = xP$
(d_i, P_i)	Private/public key of the entity ID_i, where $P_i = d_iP$
H_0, H_1	Secure and one-way cryptographic hash functions (e.g., SHA-1)

- **Setup:** The input of this algorithm is the security parameter $k \in \mathbb{Z}^+$. It outputs system's parameter and PKG's master key. This phase can be executed by the PKG as follows:
  - Select a tuple $\{F_p, E/F_p, G, P\}$.
  - Choose $x \in_R Z_p^*$ and $P_{pub} = xP$ as the master secret key and public key.
  - Selects two hash functions $H_0 : \{0,1\}^* \times G \rightarrow Z_p^*$ and $H_1 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_p^*$.
  - Disclose $\Omega = \{F_p, E/F_p, G, P, P_{pub}, H_0, H_1\}$ as system's parameter and keep x secret.
- **Extract:** It takes (Ω, x) and B's identity ID_B as input. This algorithm returns the identity-based private key of B. The signer B sends his identity ID_B to PKG over a secure channel and the PKG works as:
  - Choose $r_B \in_R Z_p^*$ and calculates $R_B = r_BP$, $h_B = H_0(ID_B, R_B)$.
  - Compute $d_B = r_B + h_Bx \bmod p$.

  Now, PKG sends (d_B, R_B) to B using a secure/out-of-band channel. The public key of B is $P_B = R_B + h_BP_{pub}$ and the private/public key pair (d_B, P_B) can be checked by analyzing whether $P_B = d_BP = R_B + h_BP_{pub}$ holds. Since we have,

$$\begin{aligned} P_B &= R_B + H_0(ID_B, R_B)P_{pub} \\ &= r_B P + H_0(ID_B, R_B)xP \\ &= (r_B + H_0(ID_B, R_B)x)P \\ &= (r_B + h_B x)P \\ &= d_B P \end{aligned} \tag{2}$$

The pair (d_B, P_B) is valid if the above verification is correct.

- **Issue:** To get a partially blind signature on a message m from the signer B, the user C executes this algorithm as follows:
  - **Agree:** Assume that C and B negotiate the common information Δ.
  - **Commitment:** B chooses $r \in_R Z_p^*$, calculates $R = rP_B$ and delivers (R, R_B) to C.
  - **Blind:** C picks two blind factors $a, b \in_R Z_p^*$ and executes $R' = aR + abP + ab[R_B + H_0(ID_B, R_B)P_{pub}] = aR + abP_B + abP$ and $h = a^{-1}H_1(m, R', \Delta) + b$. Then C forwards h to B.
  - **Sign:** B calculates $S = (r + h)d_B$ and delivers it to C.
  - **Unblind:** C computes $S' = a(S + b)$ and outputs (m, Δ, R_B, R', S') as the final partially blind signature.
- **Verify:** To validate the signature (m, Δ, R_B, R', S') for m and Δ, the verifier performs:
  - Calculate $H_1(m, R', \Delta)$.
  - Accept (m, Δ, R_B, R', S') if and only if $S'P = R' + H_1(m, R', \Delta)[R_B + H_0(ID_B, R_B)P_{pub}]$, i.e., $S'P = R' + H_1(m, R', \Delta)P_B$ holds.

For further understanding, the proposed scheme is depicted in Fig. 1.

6 Analysis of the proposed ID-PBS scheme

6.1 Security analysis

Theorem 1 The proposed ID-PBS scheme satisfies the property of completeness.

Proof We can justified the correctness of the signature (m, Δ, R_B, R', S') for the message m and the common information Δ from the following derivation:

$$\begin{aligned} S'P &= a(S + b)P \\ &= aSP + abP \\ &= a(r + h)d_B P + abP \\ &= a(r + a^{-1}H_1(m, R', \Delta) + b)[r_B + h_B x] + abP \\ &= ar[r_B P + h_B xP] + H_1(m, R', \Delta)[r_B P + h_B xP] + ab[r_B P + h_B xP] + abP \\ &= arP_B + abP_B + H_1(m, R', \Delta)[r_B P + h_B xP] + abP \\ &= aR + abP_B + abP + H_1(m, R', \Delta)[R_B + h_B P_{pub}] \\ &= R' + H_1(m, R', \Delta)[R_B + H_0(ID_B, R_B)P_{pub}] \\ &= R' + H_1(m, R', \Delta)P_B \end{aligned}$$

This proves our claim.

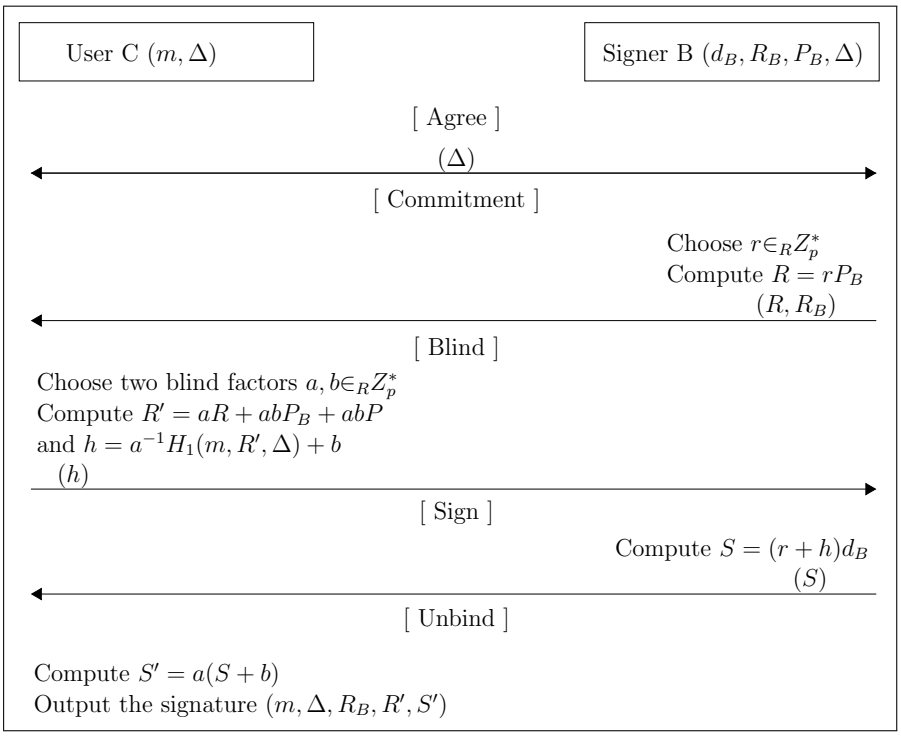

Fig. 1 Proposed pairing-free ID-PBS scheme.

Theorem 2 The proposed ID-PBS scheme holds the property of non-deniability.

Proof The proposed ID-PBS scheme is non-deniable that is, if B generates a signature (m, Δ, R_B, R', S') for C but, later on he cannot deny the signature generation. Because the final partially blind signature (m, Δ, R_B, R', S') is calculated using B's private key d_B and a common information Δ agreed by both B and C, where $S' = a(S + b) = a(r + h)d_B + ab$. The above equation shows that anyone who does not have the knowledge about B's private key d_B, cannot generate the signature (m, Δ, R_B, R', S'). In addition, the verification equation $S'P = R' + H_1(m, R', \Delta)[R_B + H_0(ID_B, R_B)P_{pub}] = R' + H_1(m, R', \Delta)P_B$ ensures that B's public key P_B must involve in the verification operation. Thus, B cannot deny the signature generation and accordingly the non-deniability property is preserved in our ID-PBS scheme.

Theorem 3 The proposed scheme satisfies the partially blindness property.

Proof Let us assume that a probabilistic polynomial-time bounded adversary $\mathcal{A}$ acts as the signer B and (m, Δ, R_B, R', S') is one of two signatures subsequently transferred to $\mathcal{A}$. Let (R, h, S) be the data appearing in view of $\mathcal{A}$ during one of the executions of the *Issue* protocol. In order to demonstrate the partial blindness, we analyzed that for given a signature (m, Δ, R_B, R', S') and any view (R, h, S) of it, the blind factors $\alpha, \beta \in_R Z_p^*$ are always unique. Assume that $\mathcal{A}$'s identity is ID_B, the corresponding public key is P_B and $\mathcal{A}$ acquires the signatures $\{m_b, \Delta, R_B, \sigma_b = (R'_b, S'_b)\}$ and $\{m_{1-b}, \Delta, R_B, \sigma_{1-b} =$

$(R'_{1-b}, S'_{1-b})\}$ when the *Issue* protocol is executed. Let (R_i, h_i, S_i) for $i = 0, 1$ be the data appeared to $\mathcal{A}$ during the executions of *Issue* protocol. To show the uniqueness of $\alpha, \beta \in_R Z_p^*$ that maps (R_i, h_i, S_i) to (R'_j, S'_j) for $i, j, b \in \{0, 1\}$, consider the following equations:

$$R'_j = \alpha R_i + \alpha\beta P + \alpha\beta P_B \tag{3}$$
$$h_i = \alpha^{-1} H_1(m, \Delta, R'_j) + \beta \tag{4}$$
$$S_i = (r + h_i) d_B \tag{5}$$
$$S'_j = \alpha(S_i + \beta) \tag{6}$$
$$S'_j P = R'_j + H_1(m, \Delta, R'_j) P_B \tag{7}$$

From the above, α and β can be computed uniquely from equations (6) and (4) as $\alpha = S'_j/(S_i + \beta)$ and $\beta = (h_i S'_j - S_i H_1(m, \Delta, R'_j))/(H_1(m, \Delta, R'_j) + S'_j)$, respectively. Now, we prove that $\alpha, \beta \in_R Z_p^*$ got from (4) and (6) satisfy the equation (7) with the help of the equation (5). Let $a = S'_j$, $c = h_i$, $b = S_i = (r + c)d_B$ and $d = H_1(m, \Delta, R'_j)$. Therefore, $\beta = \frac{ac-bd}{a+d}$ and $\alpha = \frac{a+d}{b+c}$, and we have

$$\begin{aligned}
R'_j + H_1(m, \Delta, R'_j) P_B &= \alpha R_i + \alpha\beta P + \alpha\beta P_B + H_1(m, \Delta, R'_j) P_B \\
&= \frac{a+d}{b+c} r d_B P + \frac{a+d}{b+c}\frac{ac-bd}{a+d} P + \frac{a+d}{b+c}\frac{ac-bd}{a+d} d_B P + d d_B P \\
&= \frac{a+d}{b+c} r d_B P + \frac{ac-bd}{b+c} P + \frac{ac-bd}{b+c} d_B P + d d_B P \\
&= [\frac{a+d}{b+c} r d_B + \frac{ac-bd}{b+c} + \frac{ac-bd}{b+c} d_B + d d_B] P \\
&= [\frac{ard_B + drd_B + ac - bd + acd_B - bdd_B + bdd_B + dcd_B}{b+c}] P \\
&= [\frac{ard_B + drd_B + ac - bd + acd_B + dcd_B}{b+c}] P \\
&= [\frac{ard_B + drd_B + ac - d_B(r+c)d + acd_B + dcd_B}{b+c}] P \\
&= [\frac{ard_B + drd_B + ac - drd_B r + cdd_B + acd_B + dcd_B}{d_B(r+c) + c}] P \\
&= [\frac{ard_B + ac + acd_B}{d_B(r+c) + c}] P \\
&= [\frac{a(rd_B + c + cd_B)}{d_B(r+c) + c}] P \\
&= [\frac{a(rd_B + c + cd_B)}{rd_B + c + cd_B}] P \\
&= aP \\
&= S'_j P \quad [\because \ a = S'_j]
\end{aligned}$$

where $m = m_0$ or $m = m_1$. Thus, the blinding factors $\alpha, \beta \in_R Z_p^*$ always exist uniquely, which leads to the same relation as defined in the *Issue* protocol. Accordingly, an adversary $\mathcal{A}$ returns a guess bit b' such that $b' = b$ with probability $\frac{1}{2}$. Thus, the proposed ID-PBS scheme includes the *partially blindness* property.

Theorem 4 In the random oracle model, our ID-PBS scheme is existential unforgeable against the adaptively chosen message and identity attacks with the infeasibility assumption of ECDLP.

Proof Assume that the proposed ID-PBS scheme can be forged by a polynomial-time bounded adversary $\mathcal{A}$ under the adaptive chosen message and identity attacks, then it is possible to design a polynomial time algorithm $\mathcal{C}$, which helps $\mathcal{A}$ to solve an instance of ECDLP that is, $\mathcal{A}$ outputs a from a random tuple $(P, Q = aP)$, where $a \in_R Z_p^*$ is completely unknown to the adversary $\mathcal{A}$.

- **Setup:** $\mathcal{C}$ sets PKG's public key as $P_{pub} = aP$. Here, the hash functions H_i $(i = 0, 1)$ are considered as random oracle. $\mathcal{C}$ sets the system's parameter as $\Omega = \{F_p, E/F_p, G, P, P_{pub} = aP, H_0, H_1\}$ and answers $\mathcal{A}$'s queries in the following way.
- **Extract queries:** $\mathcal{C}$ maintains an initial-empty H_0-oracle list L_{H0}^{list}, which includes the tuples in the form of (ID_i, d_i, R_i, h_i). To obtain ID_i's private key, $\mathcal{A}$ makes this query to $\mathcal{C}$, in the following, $\mathcal{C}$ looks for ID_i in the list L_{H0}^{list} and returns the output to $\mathcal{A}$ as follows:
  - If $(ID_i = ID_B)$, $\mathcal{C}$ terminates the protocol.
  - If $(ID_i \neq ID_B)$, $\mathcal{C}$ selects $a_i, b_i \in_R Z_p^*$ and sets $d_i = b_i, R_i = a_i P_{pub} + b_i P$, and $h_i = H_0(ID_i, R_i) = -a_i$. It is clear that (d_i, R_i) satisfies the equation $P_i = d_i P = R_i + h_i P_{pub}$. Then $\mathcal{C}$ outputs d_i as the secret key of the user ID_i and incorporates the tuple (ID_i, d_i, R_i, h_i) to L_{H0}^{list} and returns d_i to $\mathcal{A}$.
- **Hash queries to H_1:** $\mathcal{C}$ also maintains an initially-empty H_1 oracle list L_{H1}^{list}, which incorporates the tuple like $(m_i, \Delta_i, R_i', h_i)$. Suppose that $\mathcal{A}$ makes at most q_{H1} times H_1 queries. For each H_1 query, $\mathcal{C}$ checks the list L_{H1}^{list}:
  - If the tuple $(m_i, \Delta_i, R_i', h_i)$ is in L_{H1}^{list}, $\mathcal{C}$ sets $H_1(m_i, \Delta_i, R_i') \leftarrow h_i$ and returns it to the adversary $\mathcal{A}$.
  - If not, that is $H_1(m_i, \Delta_i, R_i')$ has not been queried to H_1-oracle, $\mathcal{C}$ selects $h_i \in_R Z_p^*$ such that there is no item $(\cdot, \cdot, \cdot, h_i)$ in L_{H1}^{list}; $\mathcal{C}$ then includes $(m_i, \Delta_i, R_i', h_i)$ to the list L_{H1}^{list} and returns h_i to $\mathcal{A}$.
- **Issue queries:** In this case, $\mathcal{A}$ can make at most q_I times *Issue* queries. For each query of the form $(ID_i, P_i, m_i, \Delta_i)$, $\mathcal{C}$ does the following:
  - Choose $S_i', h_i \in_R Z_p^*$.
  - Set $H_1(m_i, \Delta_i, R_i') \leftarrow h_i$ and store $(m_i, \Delta_i, R_i', h_i)$ to the list L_{H1}^{list}.
  - Compute $R_i' = S_i' P - h_i P_B$.
  - Output the signature $(m_i, \Delta_i, R_i, R_i', S_i')$.
- **Forgery:** At the end of this game, $\mathcal{A}$ returns a valid signature (m, Δ, R_B, R', S'). It follows from the *forking lemma* [61] that if $\epsilon \geq 10(q_I + 1)(q_I + q_{H1})/2^k$, then $\mathcal{C}$ which can construct two valid signatures (m, Δ, R_B, R', S') and $(m, \Delta, R_B, R'^*, S'^*)$ on the same message m such that $R' = R'^*$ but $h \neq h^*$. Then we can write,

$$\begin{aligned} S'P &= R' + h[R_B + H_0(ID_B, R_B)P_{pub}] \\ &= R' + hP_B \end{aligned} \tag{8}$$

$$\begin{aligned} S'^*P &= R' + h^*[R_B + H_0(ID_B, R_B)P_{pub}] \\ &= R' + h^*P_B \end{aligned} \tag{9}$$

Subtracting the Eq. (8) from the Eq. (9) and we have

$$\begin{aligned} S'^{*}P - S'P &= R' + h^{*}P_B - R' - hP_B \\ &= h^{*}P_B - hP_B \\ &= (h^{*} - h)P_B \end{aligned} \tag{10}$$

Let $R_B = a_B P_{pub} + b_B P = a_B aP + b_B P$. Therefore, from the Eq. (10), we get

$$\begin{aligned} (S'^{*} - S')P &= (h^{*} - h)[R_B + h_B aP] \\ &= (h^{*} - h)[a_B aP + b_B P + h_B aP] \\ &= (h^{*} - h)(a_B + h_B)aP + (h^{*} - h)b_B P \end{aligned} \tag{11}$$

Now, from the Eq. (11), we can solve

$$a = [(S'^{*} - S') - (h^{*} - h)b_B]/[(h^{*} - h)(a_B + h_B)] \tag{12}$$

Therefore, $\mathcal{A}$ solves $a = [(S'^{*} - S') - (h^{*} - h)b_B]/[(h^{*} - h)(a_B + h_B)]$. According to the *forking lemma*, $\mathcal{A}$ can solve the ECDLP within the expected time $t' \leq 120686 q_{H1} t/\epsilon$. But the ECDLP is computationally infeasible by any polynomial time-bounded algorithm. Therefore, based on the intractability assumption of ECDLP, our ID-PBS scheme is provably secure in the random oracle against the adaptive chosen message and identity attacks.

6.2 Efficiency analysis

In this section, we estimated the computation costs of our ID-PBS scheme and compared it with other related schemes. Since the proposed scheme incorporates the merits of IBC and ECC, so the cost of public key and certificate is removed. In addition, our scheme is free from two time-consuming cryptographic operations, namely bilinear pairing and MTP hash function. For efficiency analysis of our scheme, we used the time complexity notations [45], [46], [47], [55], [56] defined in Table 2.

Table 2 Definition and conversion of various operation units

Notations	Meaning
T_{ML}	Time required for a modular multiplication operation
T_{EX}	Time required for a modular exponentiation operation, $T_{EX} \approx 240T_{ML}$
T_{EM}	Time required for a elliptic curve point multiplication operation, $T_{EM} \approx 29T_{ML}$
T_{BP}	Time required for a bilinear pairing operation, $T_{BP} \approx 3T_{EM} \approx 87T_{ML}$
T_{PX}	Time required for a pairing-based exponentiation operation, $T_{PX} \approx 43.5T_{ML}$
T_{EA}	Time required for an addition operation of two elliptic curve points, $T_{EA} \approx 0.12T_{ML}$
T_{MTP}	Time required for a map-to-point function, $T_{MTP} \approx T_{EM} \approx 29T_{ML}$
T_{IN}	Time required for a modular inversion operation, $T_{IN} \approx 11.6T_{ML}$
T_H	Time required for a simple hash function, which is negligible

The proposed scheme executes four T_{ML}, one T_{EA} and one T_{IN} for *Issue* protocol and two T_{ML} and one T_{EA} for signature verification. Thus, the proposed scheme needs

Table 3 Comparison of computation efficiency

Schemes	Computation Cost		Total Computation Cost
	Issue phase	Verification phase	
Ref. [4]	$5T_{ML} + T_{EA} + T_{MTP} + T_{IN}$	$T_{ML} + T_{EA} + T_{MTP} + 2T_{BP}$	$6T_{ML} + 2T_{EA} + 2T_{MTP} + T_{IN} + 2T_{BP} \approx 417T_{ML}$
Ref. [8]	$6T_{ML} + 5T_{EA} + 2T_{BP} + T_{MTP} + 2T_{PX}$	$3T_{BP} + T_{PX}$	$6T_{ML} + 5T_{EA} + T_{MTP} + 5T_{BP} + 3T_{PX} \approx 769T_{ML}$
Ref. [34]	$7T_{EX}$	$4T_{EX}$	$11T_{EX} \approx 2640T_{ML}$
Ref. [36]	$4T_{ML} + 3T_{EA} + T_{MTP} + T_{IN}$	$T_{ML} + T_{EA} + T_{MTP} + 2T_{BP}$	$5T_{ML} + 4T_{EA} + 2T_{MTP} + T_{IN} + 2T_{BP} \approx 389T_{ML}$
Ref. [38]	$4T_{ML} + 4T_{EA} + T_{MTP}$	$2T_{ML} + T_{EA} + 2T_{BP}$	$6T_{ML} + 5T_{EA} + T_{MTP} + 2T_{BP} \approx 377T_{ML}$
Ref. [62]	$5T_{EX}$	$T_{EX} + T_{BP}$	$6T_{EX} + 2T_{BP} \approx 1614T_{ML}$
Proposed	$4T_{ML} + T_{EA} + T_{IN}$	$2T_{ML} + T_{EA}$	$6T_{ML} + 2T_{EA} + T_{IN} \approx 185T_{ML}$

$(6T_{ML} + 2T_{EA} + T_{IN}) \approx 185T_{ML}$ time totally. Now we conducted a comparative study of the proposed scheme with the scheme in [4], [8], [34], [36], [38], [62] and summarizes the results in Table 3. According to the Table 3, we can argue that our ID-PBS scheme is more efficient than the scheme in [4], [8], [34], [36], [38], [62].

7 Application of the proposed ID-PBS scheme

The partial blind signatures play the central role in cryptographic protocols to provide the anonymity of users in e-cash system. It allows the signer to explicitly include common information in the blind signature under some agreement with the user but, the signer learns neither the message nor the resulting signature. Several partial blind signatures have been found in the open literature but, all of them can be realized either using PKI or by bilinear pairings with a MTP hash function. Thus, ID-PBS is useful in e-cash system since no public key certificate management is needed but, the computation cost is still high due to the involvement of bilinear pairings and MTP hash function. To achieve the desired level of security and computation efficiency, we proposed an online e-cash scheme using the proposed ID-PBS scheme that is free from bilinear pairings and MTP hash function, in this section.

7.1 Descriptions

Nowadays the electronic commerce (e-commerce) becomes popular due to its many applications such as electronic payment, electronic funds transfer, financial electronic data exchange, etc. Here we proposed an anonymous online e-cash system based on the proposed ID-PBS scheme. The proposed online e-cash system consists of four entities: (1) a trusted third party, called PKG, (2) the bank (B), (3) the customer (C) and (4) the Merchant (M) and five phases: (1) *Setup phase* (2) *Bank registration phase* (3) *Opening an account phase* (4) *Withdrawal phase* and (5) *Payment-deposit phase*. We assume that, before initiating a withdrawal phase of e-cash, C and the bank B prove their witness in an interactive manner by means of *zero-knowledge proof* protocol. With this protocol, C can prove the fact to B that he knows B's secret d_B without revealing it. The PKG is responsible to generate the system's parameter Ω and helps the bank B to issue an e-cash for the customer C. In an e-cash life cycle, B first registers to PKG for the private key. To obtain an e-cash, C opens an account to B. Then, C performs a payment protocol for purchasing some goods from M by using the e-cash that has not been spent previously. On receiving the e-cash, M sends it to B and the bank transfer the corresponding money to M's account provided that the e-cash is valid and fresh. The data flow occurs in an online e-cash system is outlined in Fig. 2.

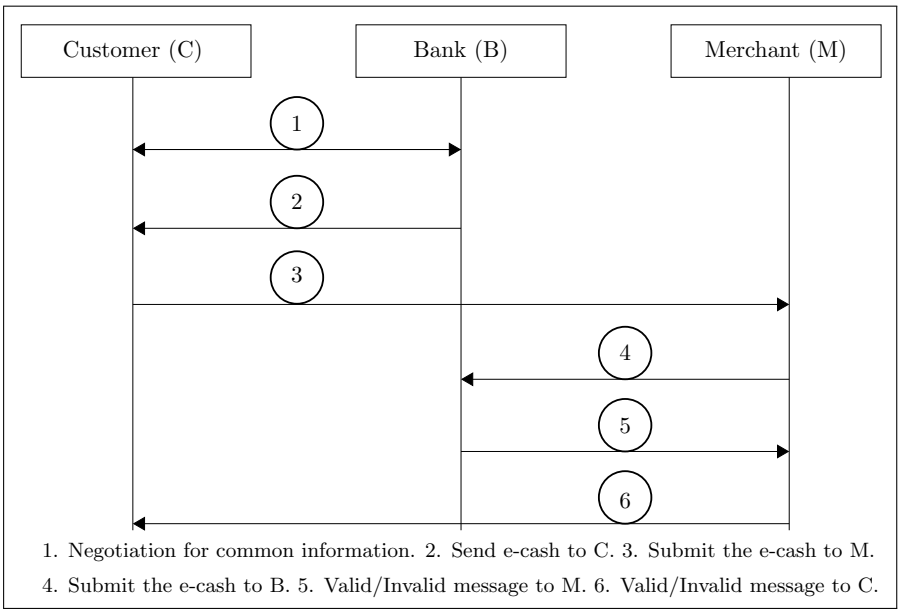

Fig. 2 Overview of the proposed online e-cash system.

7.1.1 Setup phase

In this phase, PKG accepts the security parameter $k \in \mathbb{Z}^+$ as input and outputs (x, P_{pub}, Ω), where $x \in_R Z_p^*$ is the master secret key and $P_{pub} = xP$ is the master public key of the PKG, and $\Omega = \{F_p, E/F_p, G, P, P_{pub}, H_0, H_1\}$ is the system's parameter. Here H_0, H_1 are the general cryptographic hash functions.

7.1.2 Bank registration phase

In this phase, the bank B with identity ID_B registers to PKG for the identity-based private/public key pair. The bank B sends his identity ID_B to PKG, then PKG chooses a number $r_B \in_R Z_p^*$, computes $R_B = r_B P$, $h_B = H_0(ID_B, R_B)$ and the private key $d_B = r_B + h_B x$, and then sends (d_B, R_B) securely to B. Therefore, (d_B, P_B) is the private/public key pair of B, where $P_B = R_B + h_B P_{pub}$.

7.1.3 Opening an account phase

This phase is executed between B (bank) and C (customer) when the customer wants to purchase some goods or needs some service from B for which he has to pay some money through the Internet, he will go to the bank to apply for opening an account in advance. For this, C sends the opening account application with some information such as passport number, billing information, etc. from which B can uniquely identify C. The bank B identifies C based on the supplied information and then opens an account ACC_C against the customer C.

7.1.4 Withdrawal phase

In this phase, if C wants to withdraw an e-cash with face value v from B, he then sends his account information ACC_C to B. Then B checks whether ACC_C is valid. If it is, B is ready to withdraw an e-cash for C with the face value v. Before issuing an e-cash, both B and C negotiate a common agreed information Δ. Then C selects a message m and blinds it and then submits the blinded message to B. Then B blindly sign the received blinded message using explicit common information Δ that includes the face value v and other information agreed by both parties, like expiry date of the e-cash to be issued. On receiving the blind signature, C will unblind it and calculate a final signature on m including v. The final signature is accept as the e-cash for the face value v. The description of withdrawal phase is given below.

- C and B negotiate a common information Δ. The face value v is now attached to the common information Δ.
- B chooses $r \in_R Z_p^*$, calculates $R = rP_B$ and delivers (R, R_B) to C.
- On receiving (R, R_B), C chooses a message m, two blind factors $a, b \in_R Z_p^*$ and executes $h = a^{-1}H_1(m, \Delta, R') + b$, where $P_B = R_B + h_B P_{pub} = d_B P$ and $R' = aR + abP + abP_B$, and C then sends h to B.
- Upon receiving h, B calculates $S = (r + h)d_B$ and forwards it to C.
- Then C computes $S' = a(S + b)$ and outputs the e-cash (m, Δ, R_B, R', S').

Further, we illustrated the e-cash withdrawal phase in Fig. 3.

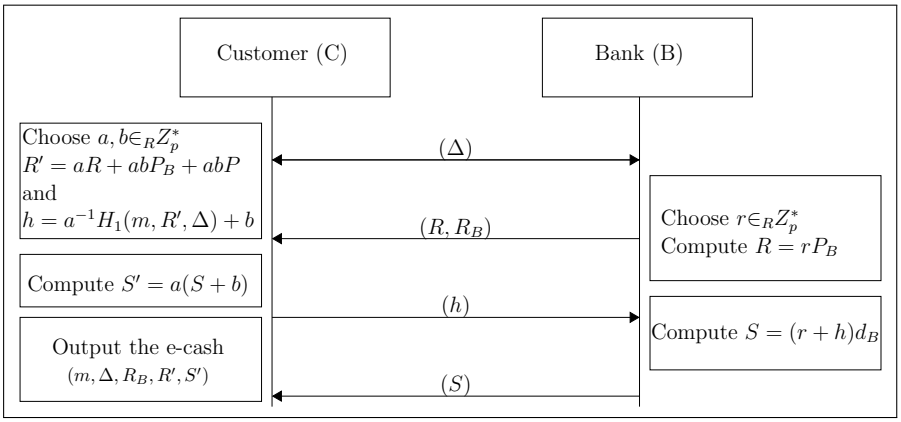

Fig. 3 Proposed withdrawal phase.

7.1.5 Payment-deposit phase

When C wants to purchase some goods, he sends an e-cash (m, Δ, R_B, R', S') to the merchant M. After receiving (m, Δ, R_B, R', S'), M first verifies whether it is correct by checking it against B's public key P_B. If (m, Δ, R_B, R', S') is valid, M interacts with B to check

the double-spending of it, otherwise sends an error message to C. To prevent the double-spending of (m, Δ, R_B, R', S'), B searches his own database (where the information about the previously spent e-cashes is stored) that m does not exist there. If (m, Δ, R_B, R', S') is correct against above two verifications, B increase M's account by the amount v. Now, we describe the payment-deposit phase below.

- C sends the e-cash (m, Δ, R_B, R', S') to M.
- Then M checks the validity of received e-cash (m, Δ, R_B, R', S') by verifying whether the equation $S'P = R' + h[R_B + H_0(ID_B, R_B)P_{pub}] = R' + hP_B$ holds.
- If it does not hold, M rejects the process, otherwise, sends the e-cash (m, Δ, R_B, R', S') with his account information to the bank B.
- Then B checks the validity of (m, Δ, R_B, R', S') by executing the above said equation and compare it with the list stored on his database to identify *double-spending* of the received e-cash (m, Δ, R_B, R', S'). If (m, Δ, R_B, R', S') is fresh, B credits M's account by an amount v and sends a validity message to M. Otherwise, B sends a message that indicates that the received e-cash (m, Δ, R_B, R', S') is invalid.
- Depending on the result of above step, M sends Valid/Invalid message to C.

It is to be noted that, in the proposed system, B's does not required huge storage space to maintain the database. Since the face value v, expiry date and time, etc. are included in the common information Δ, so B will not store the information about all e-cashes those have been spent previously. The bank's database contains the information about those e-cashes which are valid with respect to expiry date and time. If B finds any expired e-cash in its database, he/she simply removes the e-cash from the database. The payment-deposit phase is depicted in Fig. 4.

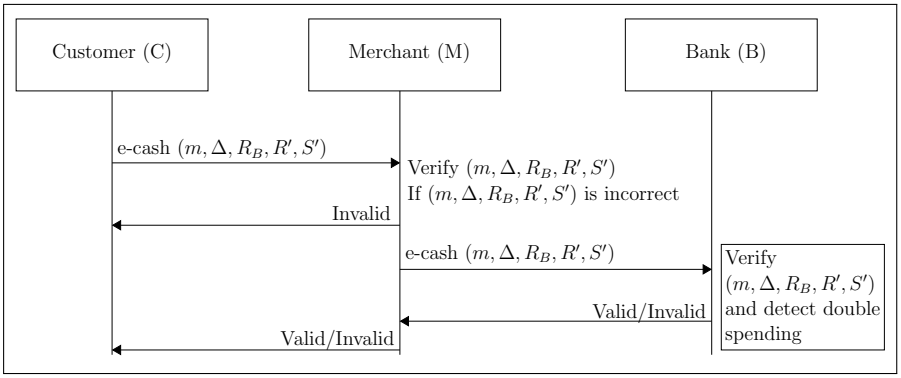

Fig. 4 Proposed payment-deposit phase.

7.2 Analysis of the proposed online e-cash system

Here, we demonstrate the proposed system provides a secure and computation efficient online e-cash system. The proposed scheme includes all the related security of an online e-cash systems.

7.3 Anonymity

In a simple e-cash system, *anonymity* is the basic requirement which ensures that, when a customer C draws an e-cash from the bank B and spent it to the merchant M, however, B and M couldn't be able to trace C from the previously spent e-cash. The proposed online e-cash system scheme supports *anonymity* of the customer through the use of PBS scheme. The inherent *unlinkability* of PBS scheme ensures none can determine that the two payments are executed by the same customer. The theorem 3 shows that the e-cash is *unlinkable*, the bank B wouldn't know anything about C except the face value v of e-cash (m, Δ, R_B, R', S'), since B would have the record message m of the e-cash (m, Δ, R_B, R', S'). However, B cannot find any link with blinded message he signs and the issued e-cash (m, Δ, R_B, R', S'). Because the blind factors a, b are used to blind the message m and these are unknown to B. Thus, the proposed online e-cash system provides the security of the customer anonymity.

7.4 Non-deniability

The non-deniability is also an important property in an e-cash system. This property states that, once B issues an e-cash (m, Δ, R_B, R', S') for C, the bank B later on cannot deny the e-cash generation against the customer C. In the proposed e-cash system, B computes $S = (r + h)d_B$ and C unblinds it as $S' = a(S + b)$. Since, the e-cash (m, Δ, R_B, R', S') is a PBS scheme, which is calculated using the private key d_B of B and a shared information Δ, and B's public key is required in the final verification equation $S'P = R' + h[R_B + H_0(ID_B, R_B)P_{pub}] = R' + hP_B$. Therefore, a valid e-cash (m, Δ, R_B, R', S') can be computed by the bank B only, none can generate it without knowing B's private key d_B. Otherwise, the above verification equation wouldn't be satisfied. Therefore, B cannot repudiate the valid e-cash generation on the message m.

7.5 Double-spending detection

In our proposed system, B can easily detect any doubly spent e-cash, which is a great concern in any e-cash system, using the parameters of that e-cash. On receiving an e-cash (m, Δ, R_B, R', S'), B checks the local database (which contains information about previously spent e-cashes) to see whether m, Δ, R_B, R' and S' are unique. If so, the e-cash (m, Δ, R_B, R', S') is fresh, otherwise it is spent doubly.

7.6 Unforgeability

An online e-cash system is unforgeable, if and only if except B, anyone cannot generate the e-cash (m, Δ, R_B, R', S'). The theorem 4 ensure that e-cash (m, Δ, R_B, R', S') generated by our ID-PBS scheme is unforgeable in the random oracle model. Therefore, unforgeability property is preserved in our e-cash system.

8 Conclusion

In this paper, we proposed an ID-PBS scheme over elliptic curve group. The scheme is computation efficient compared with other related schemes as it has been implemented without bilinear pairings. We prove that our signature scheme is secured against adaptively chosen message and identity attacks based on the difficulties of ECDLP in the random oracle model. Based on our ID-PBS scheme, we design an efficient and secure online e-cash system which satisfies all the necessary security requirements such as unforgeability, anonymity, non-deniability and detection of double-spending of e-cashes. Finally, the proposed online e-cash system has several advantages that suit for real-life applications.

References

1. Hwang, J-J., Yeh, T-C., Lib, J-B. Securing on-line credit card payments without disclosing privacy information. Computer Standards & Interfaces, 25, 2003, 119-129.
2. Li, Y., and Zhang, X. Securing credit card transactions with one-time payment scheme. Electronic Commerce Research and Applications, 4, 2005, 413-426.
3. Stirland, M. Smartcards in Secure Electronic Commerce. Information Security Technical Report, 3, 2, 1998, 41-54.
4. Chen W.K. Efficient on-line electronic checks. Applied Mathematics and Computation, 162, 2005, 1259-63.
5. Chang,C-C., Chang, S-C., Lee, J-S. An on-line electronic check system with mutual authentication. Computers and Electrical Engineering, 35, 2009, 757-763.
6. Chaum, D. Security without identification: transaction systems to make big brother obsolete. Communications of the ACM, 28, 10, 1985, 1030-1044.
7. Eslami, Z., and Talebi, M. A new untraceable off-line electronic cash system. Electronic Commerce Research and Applications, 10, 2011, 59-66.
8. Zhang, L., Zhang, F., Qin, B., and Liu, S. Provably-secure electronic cash based on certificateless partially-blind signatures. Electronic Commerce Research and Applications, 2011. doi:10.1016/j.elerap.2011.01.004.
9. Ashrafi, M.Z., and Ng, S.K. Privacy-preserving e-payments using one-time payment details. Computer Standards & Interfaces, 31, 2009, 321 - 328.
10. Chaum, D. Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, and A. T. Sherman (eds.), Advances in Cryptology: Proceedings of Crypto 1982, Santa Barbara, CA, 1982, Plenum Publishing, New York, NY, 1983, 199-203.
11. Chaum, D. Online cash checks. In J. J. Quisquater and J. Vandewalle (eds.), Advances in Cryptology: Proceedings of the Workshop on the Theory and Applications of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989. Lecture Notes in Computer Science, Vol. 434), Springer, New York, NY, 1990.
12. Nakanishi, T., and Sugiyama, Y. An efficient on-line electronic cash with unlinkable exact payments. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A10, 2005, 2769-2779.
13. Song, R., and Korba, L. How to make e-cash with non-repudiation and anonymity. Proceedings of the International Conference on Information Technology: Coding and Computing, 2004, ITCC 2004, Washington DC, April 5-7, 2004. IEEE Computer Society, 2004, 167-172.
14. Camenisch, J., Lysyanskaya,A., and Meyerovich, M. Endrosed e-cash. IEEE Symposium on Security and Privacy (SP'07), Berkeley, CA, May 20-23, 2007. IEEE Computer Society, Washington, DC, 2007, 101-115.
15. Anand, R. S., and Madhavan, C. E. An online, transferable e-cash payment system. In B. K. Roy and E. Okamoto (eds.), Progress in Cryptology, Proceedings of the 1st International Conference on Cryptology in India, Calcutta, India, December 10-13, 2000. Lecture Notes in Computer Science, Vol. 1977), Springer, New York, NY, 2000.
16. Shi, L., Carbunar, B., and Sion, R. Conditional e-cash. In S. Dietrich and R. Dhamija (eds.), Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security, Scarborough, Trinidad and Tobago, February 12-17, 2007. Lecture Notes in Computer Science, Vol. 4886), Springer, New York, NY, 2007.

17. Varadharajan, V., Neguyen, K. Q., and Mu, Y. On the design of efficient RSA-based off-line electronic cash schemes. Theoretical Computer Science - Special issue: cryptography, 226, 1999, 1-2.
18. Wang, H., and Zhang, Y. Untraceable off-line electronic cash flow in ecommerce. Proceedings of the 24th Australasian Computer Science Conference, 2001. ACSC 2001, 29 January - 1 February 2001, Gold Coast, Queensland, Australia. IEEE Computer Society, 2001, 191-198.
19. Camenisch, J., Hohenberger, S., and Lysyanskaya, A. Compact e-cash. In R. Cramer (ed.), Advances in Cryptology, 24th International Conference on the Theory and Applications of Cryptographic Techniques, Aarhuis, Denmark, May 22-26, 2005. Lecture Notes in Computer Science, Vol. 3494), Springer, New York, 2005.
20. Hanatani, Y., Komano, Y., Ohta, K., and Kunihiro, N. Provably secure electronic cash based on blind multisignature scheme. In G. D.i Crescenzo and A. Rubin (eds.), Financial Cryptography and Data Security: 10th International Conference, FC 2006, Anguilla, British West Indies, February 27 - March 2, 2006, Lecture Notes in Computer Science, Vol. 4107, Springer, New York, NY, 2006, 236-250.
21. Qiu, W., Chen, K., and Gu, D. A new offline privacy protecting e-cash system with revokable anonymity. In A. H. Chen and V. Gligor (eds.), Information security: 5th International Conference, ISC 2002, Sao Paulo, Brazil, Sept. 30 - Oct. 2, 2002. Lecture Notes in Computer Science, Vol. 2433), Springer-Verlag, London U.K., 2002, 177-190.
22. Popescu, C. An off-line electronic cash system with revocable anonymity. In Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference, MELECON 2004, May 12-15, 2004, Dubrovnik, Croatia. IEEE Computer Society, 2004, 763-767.
23. Hou, X., and Tan, C.H. Fair traceable off-line electronic cash in wallets with observers. The 6th International Conference on Advanced Communication Technology, Feb. 9-11, 2004, Phoenix Park, Korea. IEEE Computer Society, 2004, 595-599.
24. Au, M., Wu, Q., Susilo, W., and Mu, Y. Compact e-cash from bounded accumulator. In A. Masayuki (ed.), Topics in Cryptology - CT-RSA 2007: The Cryptographer's Track at the RSA Conference 2007, San Francisco, CA, February 5-9, 2007. Lecture Notes in Computer Science, Vol. 4377), Springer, New York, NY, 2007.
25. Canard, S., and Gouget, A. Multiple denominations in e-cash with compact transaction data. In R. Sion (ed.), Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, January 25-28, 2010. Lecture Notes in Computer Science, Vol. 6052), Springer, New York, NY, 2010.
26. Canard, S., Gouget, A., and Traore, J. Improvement of efficiency in (unconditional) anonymous transferable e-cash. In G. Tsudik (ed.), Financial Cryptography and Data Security: 12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008. Lecture Notes in Computer Science, Vol. 5143), Springer, New York, NY, 2008, 202-214.
27. Chen, Y., Chou, J-S., Sun, H-M., and Cho, M-H. A novel electronic cash system with trustee-based anonymity revocation from pairing. Electronic commerce research and applications, 2011. doi:10.1016/j.elerap.2011.06.002
28. Fuchsbauer, G., Pointcheval, D., and Vergnaud, D. Transferable constant-size fair ecash. In J. A. Garay, A. Miyaji, and A. Otsuka (eds.), Cryptology and Network Security: Proceedings of 8th International Conference on Cryptology and Network Security, Kanazawa, Japan, 2009. Lecture Notes in Computer Science, Vol. 5888), Springer, New York, NY, 2009.
29. Huang, Z., Chen, K., and Wang, Y. Efficient identity-based signatures and blind signatures. In Y. G. Desmedt et al. (eds.), Cryptology and Network Security: 4th International Conference, CANS 2005, Xiamen, China, December 14-16, 2005. Lecture Notes in Computer Science, Vol. 3810), Springer, New York, NY, 2005, 120-133.
30. Zhang, F., and Kim, K. ID-based blind signature and ring signature from pairings. In Y. Zheng (ed.), Advances in Cryptology, Proceedings of the 2002 International Conference on the Theory and Applications of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002. Lecture Notes in Computer Science, Vol. 2501), Springer, New York, NY, 2002.
31. Abe, M., and Fujisaki, E. How to date blind signatures. In K. Kim and T. Matsumoto (eds.), Advances in Cryptology, Proceedings of the 1996 International Conference on the Theory and Applications of Cryptology and Information Security, Kyingju, Korea, November 3-5, 1996. Lecture Notes in Computer Science, Vol. 1163), Springer, New York, NY, 1996, 244-251.
32. Shamir, A. Identity-based cryptosystems and signature schemes. In G.R. Blakley and D. Chaum (eds.), Advances in Cryptology - CRYPT0'84, Proceedings of 4th Annual Cryptology Conference, Santa Barbara, California, USA, August 19-22, 1984. Lecture Notes in Computer Science, Vol. 196), Springer-Verlag, New York, USA, 1984, 47-53.
33. Chow, S., Hui, L., Yiu, S., and Chow, K. Two improved partially blind signature schemes from bilinear pairings. In C. Boyd and J. G. Nieto (eds.), Proceedings of 10th Australasian Conference on Information Security and Privacy, Brisbane, Australia, July 4-6, 2005. Lecture Notes in Computer Science, Vol. 3574), Springer, New York, NY, 2005.

34. Abe, M., and Okamoto, T. Provably secure partially blind signatures. In M. Bellaire (ed.), Advances in Cryptology, Proceedings of 20th Annual Cryptology Conference, Santa Barbara, CA, August 20-24, 2000. Lecture Notes in Computer Science, Vol. 1880), Springer, New York, NY, 2000, 271-286.
35. Fan, C.I., and Lei, C.L. Low-computation partially blind signatures for electronic cash. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E81- A(5), 1998, 818-824.
36. Zhang, F., Safavi-Naini, R., and Susilo, W. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. In T. Johansson and S. Maitra (eds.), Progress in Cryptology - INDOCRYPT 2003, Fourth International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003. Lecture Notes in Computer Science, Vol. 2904), Springer, New York, NY, 2003, 191-204.
37. Zhang, F., and Chen, X. Cryptanalysis of Huang-Chang partially blind signature scheme. The Journal of Systems and Software, 76, 2005, 323-325.
38. Hu, X., and Huang, S. An Efficient ID-Based Partially Blind Signature Scheme. Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2007, July 30-August 1, 2007, Qingdao, China. IEEE Computer Society, Vol. 3), 2007, 291-296.
39. Bellare, M., and Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, November 3-5, 1993, ACM Press, New York, NY, 1993.
40. Tseng, Y-M., Wu, T-S., and Wu, J-D. Forgery Attacks on an ID-Based Partially Blind Signature Scheme. IAENG International journal of Computer science, 35, 3, 2008.
41. Chen, X., Zhang, F., and Liu, S. ID-based restrictive partially blind signatures and applications. The Journal of Systems and Software, 80, 2007, 164-171.
42. Zhang, J., and Gao, S. Cryptoanlaysis of a Self-certified Partially Blind Signature and a Proxy Blind Signature. In proceedings of the WASE International Conference on Information Engineering, Shanxi, China, July 10-11, 2009. IEEE Computer Society Washington DC, USA, 2009, 184-187.
43. Hu, X., and Huang, S. Analysis of ID-based restrictive partially blind signatures and applications. The Journal of Systems and Software, 81, 2008, 1951-1954.
44. Lin, X., Lu, R., Zhu, H. Ho, P., and Sherman, X. Provably Secure Self-certified Partially Blind Signature Scheme from Bilinear Pairings. IEEE International Conference on Communications, 2008. ICC'08. Beijing, China, May 19-23, 2008. IEEE Computer Society, 2008, 1530-1535.
45. Barreto, P. Lynn, B., and Scott, M. On the selection of pairing-friendly groups. In M. Matusi and R. Zuccherato (eds.), Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2004, Ottawa, Canada, August 14-15, 2004. Lecture Notes in Computer Science, Vol. 3006), Springer-Verlag, New York, NY, 2004, 17-25.
46. Barreto, P., Kim, H., Lynn, B., and Scott, M. Efficient algorithms for pairing-based cryptosystems. In M. Yung (ed.), Advances in Cryptology - CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002. Lecture Notes in Computer Science, Vol. 2442), Springer-Verlag, New York, NY, 2002, 354-368.
47. Boneh, D., and Franklin, M. Identity-based encryption from the Weil pairing. SIAM Journal on Computing. 32, 2003, 586-615.
48. Cao, X., Kou, W., and Du, X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Information Sciences, 180, 2010, 2895-2903.
49. Cao, X., Kou, W., Yu, Y., and Sun, R. Identity-based authentication key agreement protocols without bilinear pairings. IEICE Transaction on Fundamentals, E91-A (12), 2008, 3833-3836.
50. He, D., Chen, Y., Chen, J., Zhang, R., and Han, W. A new two-round certificateless authenticated key agreement protocol without bilinear pairings. Mathematical and Computer Modelling, 54, 2011, 3143-3152.
51. He, D., Chen, J., and Hu, J. A pairing-free certificateless authenticated key agreement protocol. International Journal of Communication Systems, 25(2), 2012, 221-230.
52. He, D., Chen, J., and Hu, J. Identity-based digital signature scheme without Bilinear Pairings. Cryptology ePrint Archive, Report 2011/079, 2011. http://eprint.iacr.org/2011/079/.
53. He D., Chen J., Zhang R. An efficient identity-based blind signature scheme without bilinear pairings. Computers and Electrical Engineering, 37(4), 2011, 444-450.
54. He, D., Chen, J., and Hu, J. An ID-based proxy signature schemes without bilinear pairings. Annals of Telecommunications, 66(11-12), 2011, 657-662.
55. Islam, S. H., and Biswas, G. P. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile network. Annals of Telecommunications, 2012. DOI: 10.1007/s12243-012-0296-9.
56. Islam, S. H., and Biswas, G. P. An improved pairing-free identity-based authenticated key agreement protocol based on ECC. In: Proceedings of the International Conference on Communication Technology and System Design, Procedia Engineering, Vol. 30, 2012, 499-507.

57. Schnorr, C.P. Efficient identification and signatures for smart cards, In: Proceedings of the Cryptology (Crypto'89), LNCS 435, 239-251, Springer-Verlag, 1990.
58. Koblitz, N. Elliptic curve cryptosystem. Journal of Mathematics of Computation, 48, 177, 1987, 203-209.
59. Miller, V.S. Use of elliptic curves in cryptography. In H. C. Williams (ed.), Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985. Lecture Notes in Computer Science, Vol. 218), Springer-Verlag, New York, 1985, 417-426.
60. Hankerson, D., Menezes, A., and Vanstone, S. Guide to elliptic curve cryptography, Springer-Verlag, New York, USA, 2004.
61. Pointcheval, D., and Stern, J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 13, 2000, 361-396.
62. Chen, W., Qin, B., Wu, Q., Zhang, L., and Zhang, H. ID-based Partially Blind Signatures: A Scalable Solution to Multi-Bank E-Cash. International Conference on Signal Processing Systems, Yantai, China, May 15-17, 2009, 433 - 437.
63. Islam, S. H and Biswas, G. P., A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. Annals of telecommunications, 67 (11-12), 547-558, 2012.
64. Islam, S. H and Biswas, G. P., Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings. Journal of King Saud University-Computer and Information Sciences, 25 (1), 51-61, 2013.
65. Islam, S. H and Biswas, G. P., Design of improved password authentication and update scheme based on elliptic curve cryptography. Mathematical and Computer Modelling, 57 (11), 2703-2717, 2013.
66. Zhang, F., Kim, K., Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings, Proceedings of the Information Security and Privacy, LNCS 2727, 2003, 312-323.