cryptography

MDPI

Article

# Pairing Free Identity-Based Blind Signature Scheme with Message Recovery

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

Department of Engineering Mathematics, Andhra University, Visakhapatnam 530003, India; salomecrypto@gmail.com (S.J.); gayatricrypto@gmail.com (N.B.G.)
* Correspondence: vasucrypto@andhrauniversity.edu.in; Tel.: +91-988-500-0274

Received: 17 September 2018; Accepted: 5 October 2018; Published: 9 October 2018

**Abstract:** With the rapid development of modern technology, personal privacy has become a critical concern in many applications. Various digitalized applications such as online voting systems and the electronic cash systems need authenticity and anonymity. Blind signature is an advanced technique that provides the authenticity and anonymity of the user by obtaining a valid signature for a message without revealing its content to the signer. The message recovery property minimizes the signature size and allows efficient communication in situations where bandwidth is limited. With the advantage of blind signature and message recovery properties, in this paper, we present a new pairing free blind signature scheme with message recovery in Identity-based settings. The proposed scheme is proven to be secure in the random oracle model under the assumption that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is intractable. The proposed scheme meets the security requirements such as blindness, untracebility, and unforgeability. We compare our scheme with the well-known existing schemes in the literature, and the efficiency analysis shows that our scheme is more efficient in terms of computational and communicational point of view.

**Keywords:** digital signature; blind signature; ECDLP; ID-based framework; message recovery

## 1. Introduction

Digital Signature is one of the most important applications of Public Key Cryptography (PKC) and provides authenticity, data integrity, and non-repudiation. In traditional PKC, proposed by Diffie and Hellman [1] in 1976, authentication of public key relies on the certificate issued by Certificate Authority (CA). However, certificate management leads to extra storage, large computation, and communication costs. To surmount the obstacles in traditional PKC, Shamir [2] introduced Identity–based PKC (ID-PKC). In this system, public key of a user is resulting from user's identity such as email and phone number; and secret key is generated from user's public key via a trusted third party called Private Key Generator (PKG). To implement the digital signature in the real-world applications, we need to consider different features and properties to make them adequate and proper for different usages. There are many digital signature schemes in the literature with different properties such as Proxy signature, Aggregate signature, Multi signature, Group signature, Ring signature, etc. One of such variant is Blind Signature.

Blind signature is used to protect anonymity of a user in many applications such as electronic payment on e-commerce and anonymous electronic voting systems [3–8]. The concept of blind signature was introduced by Chaum [7] in 1982. In contrast to regular digital signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. The user acquires a signature on a message from the signer, however the content of the message and the final blind signature is not known to the signer. With the development of electronic commerce, the preservation of anonymity of the user has been an imperative need. As blind signature allows secure electronic payment and protects customers' privacy or anonymity in e-cash transactions, it is a very important tool for electronic cash transmission. Similarly, e-voting uses blind signatures to obtain votes without violating the anonymity of the voter.

Message recovery is a concept where some (partial), or all (full), of the message is embedded in the signature itself. A digital signature scheme with this feature allows conserving bandwidth when transmitting a signed message, compared to a signature scheme with appendix. The digital signature scheme with a message recovery was first introduced by Nyberg and Rueppel [9] in 1993. In this signature scheme, the message itself is not required to be transmitted together with the signature. In fact, the message is embedded in the signature and can be recovered during the verification/message recovery process. In this way, the total length of the message and the appended signature can be shortened. It is very much suitable in situations where bandwidth is one of the main concerns. Combination of blind signature technique with message recovery integrates the advantages of both and provides anonymity, untraceability, and unforgeability for low bandwidth devices.

### *1.1. Related Work*

After the introduction of blind signatures by Chaum [7], many blind signature schemes [10–14] were proposed in traditional PKC. Advantages of Identity based cryptosystem attracted the researchers towards it [15]. The first ID-based blind signature scheme was proposed by Zhang et al. [16] in 2002. Later many identity-based blind signature schemes have been proposed in literature along with its applications in e-cash and e-voting systems [17–35]. Most of these schemes are designed using bilinear pairings over elliptic curves [17–23,25,26,28,31,35]. In 2003, Zhang et al. [17] and in 2005, Huang et al. [18] proposed different efficient ID-based blind signature schemes. In 2006, Zhao et al. [19] proposed a new identity based blind signature scheme from bilinear pairings. In 2008, Kalkan et al. [20] presented a generalized ID-based blind signature from bilinear pairings. In 2010, Rao et al. [21] proposed a blind signature scheme using bilinear pairings over elliptic curves. The proposed scheme is based on the Hess identity-based digital signature scheme [22] and the security is based on the CDH problem. In 2010, Fan et al. [23] proposed a provably secure randomized blind signature scheme based on bilinear pairings. They proved the security for unlinkability, unforgeability in ROM. In the same year, Zhang et al. [24] proposed a novel ID-based blind signature for electronic voting system and Shakerian et al. [25] proposed blind signature scheme from pairings. In 2011, He et al. [26] proposed an efficient identity-based blind signature scheme without bilinear pairings, and their work is motivated by the importance of blind signatures, which guarantees the anonymity of users. Later, Hu et al. [27] presented ID-based blind signature without random oracle model. In 2013, Xu et al. [28] presented an ID-based blind signature scheme from pairings with unlinkability. In the same year, Jain et al. [29] presented an efficient ID-based blind signature scheme in E-voting. Later, Li et al. [30] presented a partially blind signature scheme standard model. In 2014, Pance et al. [31] presented a comparison of ID-based blind signatures from pairings for E-voting. In 2015, Girish et al. [32] proposed a survey paper on Identity based blind signature schemes. In 2016, Islam et al. [33] proposed a provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system. The security analysis of the proposed scheme was presented in the random oracle model, which substantiated that it was provably secure. In 2017, Kumar et al. [34] proposed a blind signature for E-voting in ID-based setting. In the same year Sarde et al. [35] presented a blind and proxy blind signature scheme. Most of these schemes are designed using bilinear pairings over elliptic curves. In addition to these, very few ID-based blind signature schemes with message recovery have been proposed in literature [23,36–40]. In 2007, Han et al. [36] proposed a blind signature scheme with message recovery, using pairings over elliptic curves. This paper is based on modified Weil/Tate pairings over elliptic curves, which improves the key size. In 2008, Hassan et al. [37] proposed a new identity-based blind signature scheme with message recovery based on Zhang et al. scheme. Their scheme is more efficient than Han et al. [36] scheme. It requires less bandwidth and is suitable for signing short messages such as pin card numbers and short identifiers. Additionally, in

2013, Diao et al. [38] proposed a new proxy blind signature scheme with message recovery. In 2017, James et al. [39] proposed an identity-based blind signature scheme with message recovery using bilinear pairings over elliptic curves. Recently, in 2018, Verma and Singh [40] proposed an efficient identity-based blind signature scheme with message recovery using bilinear pairings. However, the above-mentioned blind signature schemes are designed using bilinear pairings over elliptic curves. Additionally, these blind signature schemes are designed with message recovery using pairings.

### *1.2. Motivation*

In any PKC, to provide the high security, the length of the key size must be sufficiently large. Larger keys in cryptographic schemes cause less computational efficiency and require more bandwidth. Thus, cryptographic schemes with smaller key size are desirable. To meet this requirement, Koblitz [41] and Miller [42] independently proposed the Elliptic Curve Cryptography (ECC) using elliptic curves. ECC has many advantages over PKC, especially; ECC provides high security with smaller keys in size. For instance, ECC with 512 bit key provides the same level of security as in AES (Advanced Encryption Standard; symmetric algorithm) with 256 bit key and in RSA with 15,360 bit key. Thus, ECC based schemes have shorter key sizes and requires low computational and communicational costs; consequently, time management, storage space, and consumption of bandwidth become very less with these small keys. Though ECC provides much security with short keys, the computational cost of a bilinear pairing over elliptic curve group is a costly operation, and is significantly more expensive than the elliptic curve scalar multiplication operation. In addition, map to point hash function is also very expensive cryptographic operation. Due to the expensive operations such as bilinear pairings and map to point hash functions, most of the cryptographic schemes are having less efficiency while implementing them. In view of this, ECC based schemes without pairing operation under general hash function would be more desirable to achieve high efficiency with the same level of security. Motivated by this, we focus on the design of new identity based blind signature scheme with message recovery in a pairing free environment.

### *1.3. Our Contribution*

In this paper, we present a Pairing Free Identity based Blind Signature scheme with message recovery over elliptic curves. The blindness property provides anonymity and untraceability. This scheme is secure against forgeability and the security proof is presented in the ROM model under the hardness of ECDLP. To the best of our knowledge, this is the first blind signature scheme in identity-based setting addressing about message recovery in a pairing free environment. Our scheme achieves high efficiency and is more comfortable for resource constrained applications. We presented the comparative analysis of our scheme with existing schemes and it shows that the proposed scheme is efficient in terms of computational and communicational point of view.

### *1.4. Organization*

The remaining part of this paper is organized as follows. In Section 2, we presented some preliminaries. The syntax and security model for our PF-IDBS-MR scheme are presented in Section 3. The proposed PF-IDBS-MR scheme is presented in Section 4. Security analysis and efficiency analysis of our PF-IDBS-MR scheme are presented in Section 5. The conclusions of the paper are presented in Section 6.

## **2. Preliminaries**

This section briefly presents the fundamental concepts of ECC and the complexity assumption, on which the proposed scheme is designed and achieves the desired security.

### *2.1. Elliptic Curve Cryptography*

Elliptic curve cryptography (ECC) has become more popular and plays a very important role in modern PKC [41,42].

Let $E_q(a,b)$ be a set of elliptic curve points over the prime field $F_q$, defined by the non-singular elliptic curve equation: $y^2\text{mod}q = \left(x^3 + ax + b\right)\text{mod}p$ with $a, b \in F_q$ and $\left(4a^3 + 27b^2\right)\text{mod}q \neq 0$. The additive elliptic curve group is defined as $G_q = \left\{(x,y) : x, y \in F_q\right\}$ and $(x,y) \in E_q(a,b) \cup \{O\}$, where the point $O$ is known as "point at infinity". The order of the elliptic curve over $F_q$ is $\left(E\left(F_q\right)\right)$ satisfies the relation $1 - 2\sqrt{q} \leq \left(E\left(F_q\right)\right) \leq q + 1$. The scalar multiplication on the cyclic group $G_q$ defined as $k{\cdot}P = P + P + \cdots + P$ ($k$ times). Here, $P \in G_q$ is the generator of order $n$.

### *2.2. Elliptic Curve Discrete Logarithm Problem*

- Given a tuple $(P,Q)$, it is computationally hard for any Probabilistic Polynomial Time (PPT) algorithm $\mathcal{A}dv$ to determine $a$, where $Q = aP$ and $a \in Z_q^*$.
- The probability that any polynomial-time bounded algorithm $\mathcal{A}dv$ can solve the ECDLP is defined as $Advg^{ECDLP}_{Adv,Gg} = Prob\left\{\mathcal{A}dv(P,Q) = a \ni P, Q \in G_g \text{ and } Q = aP, a \in Z_q^*\right\}$.

### *2.3. Notations and Acronyms*

The following Table 1 presents the acronyms that are used throughout this paper.

**Table 1.** Acronyms and explanation.

| Acronyms | Explanation |
|---|---|
| ECDLP | Elliptic Curve Discrete Logarithm Problem |
| PKC | Public Key Cryptography |
| PF-IDBS-MR | Pairing-Free Identity-based Blind Signature with Message Recovery |
| ECC | Elliptic Curve Cryptography |
| PPT | Probabilistic Polynomial Time |
| PKG | Private Key Generator |
| ROM | Random Oracle Model |
| EF-ACMA | Existential Forgery under the Adaptive Chosen Message Attack |

The following Table 2 presents the symbols and their descriptions, which have been used throughout this paper.

**Table 2.** Notation and Meaning.

| Notation | Meaning |
|---|---|
| $E(F_q)$ | Group of elliptic curve points over $F_q$ |
| $k$ | Security parameter |
| $G_1$ | An additive group which is generated by $\hat{P}$ with the order $\hat{q}$ on the super singular elliptic curve |
| $G$ | An additive cyclic group generated by a point $P$ on a non-singular elliptic curve |
| $H_1, H_2, H_3, F_1, F_2$ | Cryptographic hash functions |
| $a\|\|b$ | Concatenation of two strings $a$ and $b$ |
| $\oplus$ | X-OR computation in the binary system |
| $[x]_{10}$ | Decimal representation of $x \in \{0,1\}^*$ |
| $[y]_2$ | Binary representation of $y \in Z$ |
| ${}_{l_2}\|\beta\|$ | The first $l_2$ bits of $\beta$ from the left side |
| $\|\beta\|_{l_1}$ | The first $l_1$ bits of $\beta$ from the right side |
| $\Omega$ | Signature on the message $m$ |

## 3. Syntax and Security Model of the Proposed PF-IDBS-MR Scheme

In this section we present the syntax and security model of the proposed PF-IDBS-MR scheme.

### *3.1. Syntax of PF-IDBS-MR*

A formal model of the proposed scheme consists of the following four algorithms: System Setup, Key Extract, Blind Signature Generation, and Blind Signature Verification. The detailed description of these algorithms is described below.

1. System Setup. For a given security parameter $k \in Z^{+}$, the Private Key Generator (PKG) runs this algorithm and generates the system parameters *Params* and the master key $s$. *Params* are made public and $s$ is kept secret. *Params* are implicit input to all the following algorithms.
2. Key Extract. For a given user's identity *ID*, the PKG runs this algorithm to generate the public key and private key. PKG sends the private key to the corresponding user over a secure channel.
3. Blind Signature Generation. This is an interactive and probabilistic polynomial time protocol, which is operated by the user and the signer. The user first blinds the message $m$ and obtains a new version $\widetilde{h}$ of $m$, and then sends it to the signer. The signer uses his/her private key to sign on $\widetilde{h}$ and obtains $z_1$, and then sends it to the sender/user. The sender un-blinds it to obtain $\Omega$, which is a blind signature on the original message $m$.
4. Blind Signature Verification. For a signer's identity *ID* and a blind signature $\Omega$, a verifier runs this algorithm to recover the message and check the validity of the blind signature $\Omega$, more precisely, the algorithm *Verify* $(ID,\ \Omega)$ outputs 1 if accepted, or 0 if rejected.

### *3.2. Security Requirements of the Proposed PF-IDBS-MR*

A secure blind signature scheme must satisfy the following requirements:

1. Correctness. If the user and the signer, both comply with the algorithm of blind signature generation, then the blind signature $\Omega$ will always be accepted. The correctness of the signature can be checked by anyone using the signer's public key.
2. Blindness. A signature is said to be blind if a given message-signature pair and the signer's view are statistically independent. While correctly operating one instance of the blind signature scheme, let the output be $(m, R, Y, v)$ (i.e., message-signature pair) and the view of the protocol $V'$. At a later time, the signer is not able to link $V'$ to $(m, R, Y, v)$. Hence, the content of the message is blind to the signer.
3. Unforgeability. With this property, the user is not able to forge a valid blind signature. Only the signer can give a valid signature for the associated message.

Now we present the security definitions of blindness and unforgeability for our proposed scheme.

**Definition 1.** ***(Blindness)*** *Let $\mathcal{A}dv$ be a probabilistic polynomial-time adversary which plays the role of the signer,* $U_0$ and $U_1$ *be two honest users.* $U_0$ and $U_1$ *engage in the blind signature issuing scheme with $\mathcal{A}dv$ on messages* $m_e$ and $m_{1-e}$*, and output signatures* $\sigma_e$ and $\sigma_{1-e}$*, respectively, where $e \in \{0, 1\}$ is a random bit chosen uniformly. $(m_e, m_{1-e}, \sigma_e, \sigma_{1-e})$ are sent to $\mathcal{A}dv$ and then $\mathcal{A}dv$ outputs $e' \in \{0, 1\}$. For all such $\mathcal{A}dv$,* $U_0$ and $U_1$ *for any constant c, and for sufficiently large n, $|\Pr[e = e'] - 1/2| < n^{-c}$.*

**Definition 2.** ***(Unforgeability)*** *The proposed* ***PF-IDBS-MR*** *is secure against existential forgery under the adaptive chosen message attack (EF-ACMA) and identity attacks if there is no probabilistic polynomial time adversary has a non-negligible advantage in the following game.*

Our proposed scheme is existentially unforgeable in the Random Oracle Model (ROM) under an adaptive chosen-message and an adaptive chosen-ID attack. In this model (Game), a forger can choose its messages and its identities adaptively. We give the forger the power to request private keys on identities of its choice. The forger is also given access to the signing oracle for any messages for desired identities. A forger's advantage $Advg_{IBSSMR,\ \mathcal{A}dv}$ is defined as its probability of success in the following game between a challenger $\xi$ and a forger $\mathcal{A}dv$. The advantage to win the above game by a PPT-bounded adversary $\mathcal{A}dv$ with the help of $\xi$ is defined as $Advg_{\mathcal{A}dv} = \Pr[\mathcal{A}dv \text{ succeeds}]$.

**Game Model.**

- Setup. The challenger $\xi$ takes a security parameter $k$ and executes the setup algorithm of the PF-IDBS-MR. $\xi$ returns the system *Params* to $\mathcal{A}dv$ and keeps the master secret with itself.
- Queries. The forger $\mathcal{A}dv$ adaptively makes the following different queries to the challenger $\xi$.
  - Hash Queries. When the involved hash functions are modeled by random oracles $\mathcal{A}dv$ also performs adaptive queries to the hash functions. The Challenger $\xi$ answers these queries of the forger of this oracle, providing it with consistent and totally random values.
  - Extract Queries. When $\mathcal{A}dv$ requests the private key of an identity $ID$ of its choice, the challenger $\xi$ runs the key extraction algorithm on ID and forwards the output $d_{ID}$ to $\mathcal{A}dv$.
  - Sign Queries. When $\mathcal{A}dv$ requests, adaptively, a signature on a given message $m$ with an identity ID, $\xi$ returns a signature $\Omega$.
- Output. $\mathcal{A}dv$ outputs $(m^*,\ ID^*,\ \Omega^*)$ and we say that $\mathcal{A}dv$ succeeds if:

  (i) $ID^*$ has never requested to the private key extraction oracle;
  (ii) $\Omega^*$ has not been obtained as an answer of the challenger to a sign query $(m^*, ID^*)$;
  (iii) $\Omega^*$ is a valid signature.

## 4. Proposed PF-IDBS-MR Scheme

The proposed Pairing Free Identity based Blind signature with Message Recovery scheme consists of the following four algorithms:

- System Setup. For a given security parameter $k \in Z^+$, the PKG runs this algorithm as follows.
  1. Choose a cyclic additive group $G$ of prime order $q$ with the points on an elliptic curve $E$ and $P$ as the generator of $G$.
  2. Select $s \in Z_q^*$ randomly and compute the system public key $P_{pub} = sP$.
  3. Choose $H_1 : \{0,1\}^* \to Z_q^*,\ H_2 : \{0,1\}^* \to Z_q^*,\ H_3 : G \to \{0,1\}^{|q|}$ and $F_1 : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$, $F_2 : \{0,1\}^{l_2} \to \{0,1\}^{l_1}$ as hash functions. $l_1$ and $l_2$ are positive integers such that $|q| = l_1 + l_2$.
  4. PKG publishes the system parameters $Params = \left\{E, G, q, P, P_{pub}, H_1, H_2, H_3, F_1, F_2, l_1, l_2\right\}$ as public and keeps the master key $< s >$ as secret.
- Key Extract. Given a user's identity $ID$, the PKG runs this algorithm by choosing $r \in Z_q^*$ and computes $R = rP; h_1 = H_1\left(ID, R, P_{pub}\right); d = (r + sh_1)\mathrm{mod}q$.
  This algorithm returns $D = (d, R)$ and sends it securely to the corresponding user $ID$ as his private key.
- Blind signature generation. In order to sign a message $m \in \{0,1\}^{l_1}$ blindly by a signer, whose identity is $ID$, the user and the signer should follow the scenario given below:
  1. Signer: Chooses a number $k \in Z_q^*$ and computes $X = kP$ and sends $X, R$ to the user as a commitment.
  2. Blinding: The user chooses blinding factors $a, b \in Z_q^*$ randomly and computes

$$\beta = F_1(m)\|(F_2(F_1(m)) \oplus m), Y = aX + b\beta P, h_2 = H_2(ID, R, Y), \widetilde{h} = a^{-1}h_2\mathrm{mod}q.$$

Now the user sends $\widetilde{h}$ to the signer.

3. Signing: The signer computes $z_1 = \left(k + \widetilde{h}d\right)\text{mod}q$ and sends back to the user.
4. Unblinding: The user computes the following.

$$z_2 = (az_1 + b\beta)\text{mod}q, \alpha = H_3(ID, z_2P), v = [\alpha \oplus \beta]_{10}.$$

The user outputs $(m, Y, R, v)$ and $\Omega = (Y, R, v)$ is the blind signature on the message $m$. The blind signature issuing protocol is shown in Table 3.

- Blind signature verification. To verify the signature $\Omega = (Y, R, v)$ for the message $m$ and the identity $ID$, the verifier computes $h_1 = H_1\left(ID, R, P_{pub}\right)$, $h_2 = H_2(ID, R, Y)$, $\widetilde{\alpha} = H_3\left(ID, Y + h_2\left(R + h_1P_{pub}\right)\right)$, $\widetilde{\beta} = [v]_2 \oplus \widetilde{\alpha}$.
  The verifier recovers the message $\widetilde{m} = \left|\widetilde{\beta}\right|_{l_1} \oplus F_2\left[{}_{l_2}\left|\widetilde{\beta}\right|\right](= m)$.
  Accept the signature $\Omega$ as valid on $\widetilde{m} = m$ iff ${}_{l_2}\left|\widetilde{\beta}\right| = F_1(\widetilde{m})$.

**Table 3.** The blind signature issuing protocol.

| User | | Signer |
|---|---|---|
| | | $k \in Z_q{}^*$<br>Compute $X = kP$ |
| | $\xleftarrow{X,R}$ | |
| Chooses $a, b \in Z_q{}^*$<br>Computes $\beta = F_1(m)\|(F_2(F_1(m)) \oplus m)$<br>$Y = aX + b\beta P$<br>$h_2 = H_2(ID, R, Y)$<br>$\widetilde{h} = a^{-1}h_2\text{mod}q$ | | |
| | $\xrightarrow{\widetilde{h}}$ | |
| | | Compute $z_1 = \left(k + \widetilde{h}d\right)\text{mod}q$ |
| | $\xleftarrow{z_1}$ | |
| Compute $z_2 = (az_1 + b\beta)\text{mod}q$<br>$\alpha = H_3(ID, z_2P)$<br>$v = [\alpha \oplus \beta]_{10}$<br>$\Omega = (Y, R, v)$ is the blind signature on message $m$ | | |

## 5. Analysis of the Proposed PF-IDBS-MR Scheme

This section presents the security analysis and efficiency analysis of the proposed PF-IDBS-MR scheme.

### 5.1. Security Analysis of the Proposed Scheme

In the following we will analyse the security of our PF-IDBS-MR scheme. We prove the correctness property, blindness property and unforgeability of our PF-IDBS-MR scheme by the following two theorems.

**Theorem 1.** *(Proof of Correctness) The proposed scheme satisfies the property of correctness.*

**Proof of Theorem 1.** The following equations give the correctness of the proposed scheme.

Consider $z_2P = \{az_1 + b\beta\}P$
$= \left\{a\left[k + \widetilde{h}d\right] + b\beta\right\}P = \left\{a\left[k + \widetilde{h}(r + h_1s)\right] + b\beta\right\}P$
$= \left\{a\left[k + a^{-1}h_2(r + h_1s)\right] + b\beta\right\}P = akP + h_2(r + h_1s)P + b\beta P$
$= aX + h_2\left(R + h_1P_{pub}\right) + b\beta P$
$= (aX + b\beta P) + h_2\left(R + h_1P_{pub}\right)$
$= Y + h_2\left(R + h_1P_{pub}\right)$.

□

**Theorem 2.** ***(Blindness)*** *The proposed scheme satisfies the blindness property.*

**Proof of Theorem 2.** We consider the condition in Definition 1. Let $(m, R, Y, v)$ be one of the two signatures given to adversary $\mathcal{A}dv$. Let $\left(X, \widetilde{h}, z_1\right)$ be the data exchanged during one of the signature issuing schemes in the view of $\mathcal{A}dv$. It is sufficient to show that there exists two random factors $(a, b)$ that map $\left(X, \widetilde{h}, z_1\right)$ to $(m, R, Y, v)$. From the description of the scheme, we know the following equations must hold.

$$Y = aX + b\beta \tag{1}$$

$$\widetilde{h} = a^{-1}h_2 \bmod q \tag{2}$$

$$z_2 = (az_1 + b\beta) \bmod q \tag{3}$$

From Equation (3), we get $b\beta = z_2 - az_1 \bmod q$ and if replacing $b\beta = z_2 - az_1 \bmod q$ in Equation (1), we get that it is obvious that $a \in Z_q^*$ is unique. Then $b$ is unique, since $b\beta = z_2 - az_1 \bmod q$. Thus, $\left(X, \widetilde{h}, z_1\right)$ and $(m, R, Y, v)$ have exactly the same relation defined by the signature issuing protocol. Such $a, b$ always exist regardless of the values of $\left(X, \widetilde{h}, z_1\right)$ and $(m, R, Y, v)$. Even an infinitely powerful $\mathcal{A}dv$ outputs a correct value $e'$ with a probability exactly 1/2. Thus, the proposed scheme is unconditionally blind. □

**Theorem 3.** ***(Unforgeability)*** *The proposed scheme is existential unforgeable against the adaptive chosen message and identity attacks based on the infeasibility assumption of the ECDLP.*

**Proof of Theorem 3.** Let $\xi$ be an ECDLP challenger, and it is given a random instance $Q = sP$ of the ECDL problem in $G$ for a randomly chosen $s \in Z_q^*$. Its goal is to compute $s$. Let $\mathcal{A}dv$ be an adversary who interacts with $\xi$, as described in security model of the proposed scheme (Section 3.2). Now, we prove that $\xi$ can solve the ECDLP using $\mathcal{A}dv$. During the simulation process, $\xi$ needs to guess the target identity of $\mathcal{A}dv$. Without loss of generality, $\xi$ takes $ID^*$ as target identity of $\mathcal{A}dv$ on a message $m$.

- Initialization phase. $\xi$ runs the setup algorithm and sets $P_{pub} = Q = sP$ as public key and generates system parameters *params* and sends *params*, $P_{pub}$ to $\mathcal{A}dv$.
- Queries phase. $\mathcal{A}dv$ can access the following oracle in an adaptive manner and the algorithm $\xi$ responds to these oracles as follows.
  - Extraction oracle. $\xi$ maintains an initial-empty $H_1$-oracle list $\mathcal{L}_1$, which includes the tuples like $\left(ID_i, R_i, P_{pub}, d_i, h_{1i}\right)$ when $\mathcal{A}dv$ makes this query on identity $ID_i$, $\xi$ looks for $ID_i$ in the list $\mathcal{L}_1$ and returns the output to $\mathcal{A}dv$ as follows.
    1. If $ID_i = ID^*$, $\xi$ aborts.
    2. If $ID_i \neq ID^*$, $\xi$ selects $a_i, b_i \in Z_q^*$ and sets $d_i = b_i$, $R_i = a_iP_{pub} + b_iP$ and $\mathrm{h}_{1i} = -a_i$. Clearly $(d_i, R_i)$ satisfies the equation $d_iP = R_i + h_{1i}P_{pub}$. Then $\xi$ outputs $d_i$ as secret

key of the user $ID_i$ and incorporates the tuple $\left(ID_i, R_i, P_{pub}, d_i, h_{1i}\right)$ to $\mathcal{L}_1$ list and returns $d_i$ to $\mathcal{A}dv$.

- Queries on oracle $H_2 : H_2(ID_i, R_i, Y_i)$. When $\mathcal{A}dv$ asks a $H_2$ query with the input $(ID_i, R_i, Y_i)$, $\xi$ then replies with previous value $h_{2i} \in Z_q^*$, if the tuple $(ID_i, R_i, Y_i, h_{2i})$ is in $\mathcal{L}_2$. Otherwise $\xi$ picks a random $h_{2i} \in Z_q^*$ and returns $h_{2i}$ to $\mathcal{A}dv$ and adds $(ID_i, R_i, Y_i, h_{2i})$ to the list $\mathcal{L}_2$.
- Queries on oracle $H_3 : H_3(ID_i, z_{2i}P)$. $\xi$ maintains a list $\mathcal{L}_3$, which is initially empty. It contains tuples of the form $(ID_i, z_{2i}P, h_{3i})$. After receiving the query on $(ID_i, z_{2i}P)$, if a tuple $(ID_i, z_{2i}P, h_{3i})$ exists on $\mathcal{L}_3$, $\xi$ returns $h_{3i} \in Z_q^*$. Otherwise, $\xi$ picks a random $h_{3i} \in Z_q^*$ and returns $h_{3i}$. $\xi$ adds $(ID_i, z_{2i}P, h_{3i})$ to $\mathcal{L}_3$.
- Queries on $F_1, F_2$: $\xi$ maintains two separate lists $\mathcal{F}_1 - list, \mathcal{F}_2 - list$, which are initially empty. If the queries are made earlier, then it returns the same answer. Otherwise, $\xi$ picks random numbers from $\{0,1\}^{l_2}$ and $\{0,1\}^{l_1}$ respectively, and returns to adversary. $\xi$ stores these values in $\mathcal{F}_1, \mathcal{F}_2$ lists, respectively.
- Signing oracle. When $\mathcal{A}dv$ makes this query on $(ID_i, m_i)$, $\xi$ first makes queries on $H_2, H_3, F_1, F_2$ oracles and recovers the tuples $(ID_i, R_i, Y_i, h_{2i})$, $(ID_i, z_{2i}P, h_{3i})$ from lists, respectively. Then, $\xi$ does the following.

  1. Choose $z_{2i}, h_{2i} \in {}_R Z_q^*$
  2. Set $H_2(ID_i, R_i, Y_i) \leftarrow h_{2i}$ and store $(ID_i, R_i, Y_i, h_{2i})$ to the list $\mathcal{L}_2$.
  3. Compute $\alpha_i = H_3(ID_i, z_{2i}P)$, $\beta_i = F_1(m_i) \| (F_2(F_1(m_i)) \oplus m_i)$, $Y_i = z_{2i}P - h_{2i}\left(R_i + h_{1i}P_{pub}\right)$, $v_i = [\alpha_i \oplus \beta_i]_{10}$.

Finally, $\xi$ responds to $\mathcal{A}dv$ with the signature $(m_i, Y_i, R_i, v_i)$.

**Forgery**. After forgery, a valid signature $\left(m_i^*, Y_i^*, R_i^*, v_i^*\right)$ on the message $m_i^*$ under the identity $ID_i^*$ by $\mathcal{A}dv$, $\xi$ recovers the corresponding tuples $\left(ID_i^*, R_i^*, Y_i^*, h_{2i}^*\right), \left(ID_i^*, z_{2i}^*P, h_{3i}^*\right)$ from $\mathcal{L}_2, \mathcal{L}_3$ lists. From the tuples, if $ID_i^* \neq ID^*$, then $\xi$ halts and fails. Otherwise, if $ID_i^* = ID^*$, then $\xi$ computes the value of $s$ as follows. From Forking Lemma (Pointcheval et al. [43]), if we have a replay of $\xi$ with the same random tape but different choices of $H_2$, $H_3$, $\mathcal{A}dv$ will output another signature $\left(m_i^*, Y_i^{*'}, R_i^*, v_i^{*'}\right)$. This signature satisfies the verification equation.

By $r_i^*, s$, we now denote discrete logarithms of $R_i^*, P_{pub}$, respectively, which is $R_i^* = r_i^*P$, $P_{pub} = sP$.

As the signatures $\left(m_i^*, Y_i^*, R_i^*, v_i^*\right)$, $\left(m_i^*, Y_i^{*'}, R_i^*, v_i^{*'}\right)$ satisfy the verification equations, we get two linearly independent equations as $Y_i^{*(j)} = z_{2i}^{*(j)}P - h_{2i}^{*(j)}\left(R_i^* + h_{1i}^{*(j)}P_{pub}\right)$ for $j = 1, 2$. $\xi$ solves the unknown values $r_i^*, s$, from the above two linearly independent equations and outputs $s$ as the solution of ECDLP. However, the ECDLP is computationally infeasible by any polynomial-time bounded algorithm. Therefore, based on the intractability assumption of ECDLP, our scheme is provably secure in the ROM against the adaptive chosen message and identity attacks. □

### *5.2. Efficiency Analysis of the Proposed Scheme*

In this section, we analyze the performance of our PF-IDBS-MR scheme. We compare our scheme with the relevant schemes in terms of computational and communicational cost. We consider the experimental results (Ren et al. [44], Cao et al. [45], and Tan et al. [46]), to achieve the comparable security with 1024-bit RSA key, where the bilinear pairing (Tate pairing) is defined over the super singular elliptic curve $E_q : y^2 = x^3 + x$ with embedding degree 2 and the 160-bit Solinas prime number $q = 2^{159} + 2^{17} + 1$ with 512-bit prime number $p$ satisfying $p + 1 = 12qr$. The running time is calculated for different cryptographic operations in References [44–46] using MIRACL (Shamus software) [47], a standard cryptographic library and implemented on a hardware platform PIV (Pentium-4) 3GHZ processor with 512-MB memory and a windows XP operating system. Furthermore, Chung et al. [48]

indicated that the time needed to execute the elliptic curve scalar multiplication $(T_{EM})$ is approximately $29T_{ML}$, and the time needed to execute the modular exponentiation $(T_{EX})$ is approximately $240T_{ML}$. It was also mentioned in Reference [45] that the time needed to execute one pairing based scalar multiplication $(T_{EM})$ is approximately 6.38 ms, i.e, $T_{EM} \approx 6.38$ ms, the time needed to execute one bilinear pairing (Tate pairing) operation $(T_{BP})$ is approximately 20.01 ms, i.e.,$T_{BP} \approx 20.01$ ms and the time needed to execute one pairing-based exponentiation $T_{PX}$ is approximately 11.20 ms, i.e., $T_{PX} \approx 11.20$ ms. Now, from the works proposed by Baretto et al. [49] and Tan et al. [46], $1T_{BP} \approx 3T_{EM}$ and $1T_{PX} \approx (1/2)T_{BP}$. We summarize these computational results in Table 4.

**Table 4.** Notations and descriptions of various cryptographic operations and their conversions.

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

### 5.2.1. Computational Efficiency

The comparison of our proposed PF-IDBS-MR scheme with the existing blind signature schemes, in terms of a computational point of view, is presented in Table 5. The total computational cost of our proposed scheme is $156.96T_{ML}$, which is much more efficient than the well-known existing schemes. While the computational cost of our scheme is equal to Islam et al. scheme [33], our proposed scheme achieves message recovery. Hence, our scheme is considered to be more efficient compared to Islam et al. scheme [33]. From Table 5, it is clear that the computation cost of our PF-IDBS-MR scheme is $156.96T_{ML}$, which is 76.37% less than Han et al. scheme [36], 67.98% less than Hassan et al. scheme [37], 70.60% less than Fan et al. scheme [23], 69.95% less than Prasad et al. [21], 32.34% less than He et al. scheme [26], 67.01% less than James et al. [39], and 71.01% less than Verma et al. scheme [40]. Hence, our scheme is computationally more efficient when compared to the well-known related schemes [21,23,26,33,36,37,39,40].

**Table 5.** Comparison of computational efficiency of our proposed scheme with the related schemes.

| Scheme | Signing Cost | Verification Cost | Total Cost |
|---|---|---|---|
| Han et al. (2005) [36] | $6\mathrm{T}_{EM} + 2T_{BP} + 1T_{IN} + 2T_{PA}$ | $3T_{BP} + 1T_{PX}$ | $664.34T_{ML}$ |
| Hassan et al. (2006) [37] | $6\mathrm{T}_{EM} + 1T_{BP} + 1T_{IN} + 2T_{PA}$ | $2T_{BP} + 1T_{PX}$ | $490.34T_{ML}$ |
| Fan et al. (2010) [23] | $7\mathrm{T}_{EM} + 1T_{MTP} + 1T_{IN} + 3T_{PA}$ | $3T_{BP} + 1T_{MTP}$ | $533.96T_{ML}$ |
| Rao, et al. (2010) [21] | $2T_{BP} + 3T_{EM} + 1T_{PX} + 4T_{PA}$ | $2T_{BP} + 1T_{PX}$ | $522.48T_{ML}$ |
| He et al. (2011) [26] | $5T_{EM}$ | $3T_{EM}$ | $232T_{ML}$ |
| Islam et al. (2016) [33] | $4\mathrm{T}_{EM} + 2T_{PA} + 1T_{IN}$ | $1T_{PA} + 1T_{EM}$ | $156.96T_{ML}$ |
| James et al. (2017) [39] | $6\mathrm{T}_{EM} + 1T_{BP} + 1T_{IN} + 2T_{PA}$ | $2T_{BP} + 1T_{EM}$ | $475.84T_{ML}$ |
| Verma et al. (2018) [40] | $3\mathrm{T}_{EM} + 1T_{MTP} + 1T_{BP} + 1T_{IN}$ | $1T_{BP} + 1T_{EX}$ | $541.6T_{ML}$ |
| **Our Proposed Scheme** | $3T_{EM} + 1T_{PA} + 1T_{IN}$ | $2T_{EM} + 2T_{PA}$ | $156.96T_{ML}$ |

### 5.2.2. Communicational Efficiency

The comparison of our proposed PF-IDBS-MR scheme with the existing blind signature schemes, in terms of communicational point of view, is presented in Table 6. The schemes [21,23,36,37,39,40] are established on bilinear pairings. The remaining related schemes [26,33] and our proposed scheme is established on ECC. To achieve a security level of 80 bits, in bilinear pairing, we consider $\hat{e} : G_1 \times G_1 \rightarrow G_T$, where $G_1$ is an additive group that is generated by $\hat{P}$ with the order $\hat{q}$ on the super singular elliptic curve $\hat{E} : y^2 = x^3 + x \bmod \hat{p}$ with embedding degree 2. Here, $\hat{p}$ consists of 512 bit prime number and $\hat{q}$ is of 160 bit solinas prime number. To achieve the same 80 bit security level, in ECC, we consider $G$ as an additive cyclic group generated by a point $P$ on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$ and its order is $q$ where $p, q$ are prime numbers of 160 bit each and $a, b \in Z_q{}^*$. Hence, the size of $\hat{p}$ is 512 bits (i.e., 64 bytes) and the size of $p$ is 160 bits (i.e., 20 bytes). Hence, the size of elements in $G_1$ is $512 \times 2 = 1024$ bits and the size of elements in $G$ is $160 \times 2 = 320$ bits. Additionally, the size of the elements in $Z_q{}^*$ is 160 bits.

**Table 6.** Comparison of communicational efficiency of our proposed scheme with the related schemes.

| Scheme | Message Recovery | Signature Length | In Bytes |
|---|---|---|---|
| Han et al. (2005) [36] | ✓ | $2\|G_1\|$ | 256 *bytes* |
| Hassan et al. (2006) [37] | ✓ | $\|q\| + \|G_1\|$ | 148 *bytes* |
| Fan et al. (2010) [23] | ✗ | $\|m\| + 2\|G_1\|$ | 256 *bytes* + $\|m\|$ |
| Rao et al. (2010) [21] | ✗ | $\|q\| + \|G_1\|$ | 148 *bytes* + $\|m\|$ |
| He et al. (2011) [26] | ✗ | $\|q\| + 2\|G\|$ | 100 *bytes* + $\|m\|$ |
| Islam et al. (2016) [33] | ✗ | $\|q\| + 2\|G\|$ | 276 *bytes* + $\|m\|$ |
| James et al. (2017) [39] | ✓ | $\|q\| + \|G_1\|$ | 148 *bytes* + $\|m\|$ |
| Verma et al. (2018) [40] | ✓ | $\|q\| + \|G_1\|$ | 148 *bytes* |
| **Our Proposed Scheme** | ✓ | $\|q\| + 2\|G\|$ | 100 *bytes* |

Since our proposed scheme is with message recovery, the original message of the signature is not required to be transmitted together with the signature, and hence the signature length of our proposed scheme is $|q| + 2|G|$ and the communication cost is $160 + 2 \times 320 = 800$ bits = 100 bytes.

From Table 6, it is clear that our PF-IDBS-MR scheme is more efficient compared to the existing blind signature schemes [21,23,26,33,36,37,39,40], in a communicational point of view.

The following bar graphs (Figures 1 and 2) clearly show that our scheme is much more efficient than the existing schemes. Hence, our PF-IDBS-MR scheme is much more efficient than the existing blind signature schemes, both from a computational and communicational cost point of view.

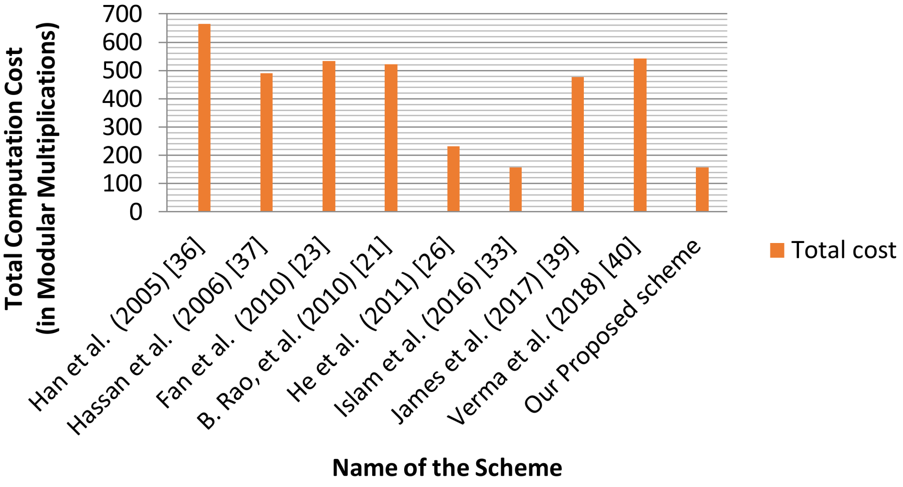

**Figure 1.** Graphical representation of Total Computation Cost.

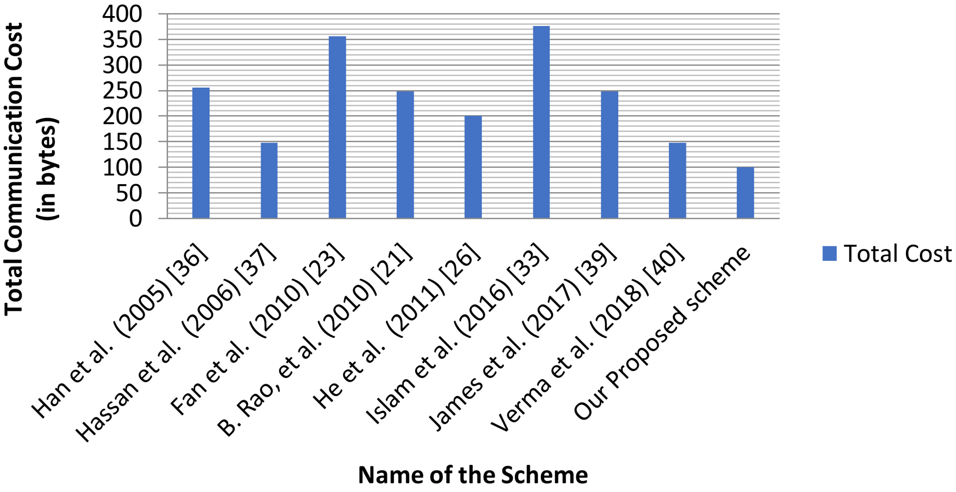

**Figure 2.** Graphical representation of Total Communication Cost.

## 6. Conclusions

In this paper, we have presented a pairing-free Identity-based blind signature scheme with message recovery. This PF-IDBS-MR scheme combines the advantages of blind signature, message recovery property in ID-based setting. Moreover, it is designed in pairing-free environment. The correctness of the proposed scheme has been validated. The proposed scheme is secure and existential unforgeable against the adaptive chosen message and identity attacks under the assumption that ECDLP intractable. The blindness property of the proposed scheme provides the anonymity of the user and the message recovery property of the proposed scheme enhances the bandwidth efficiency. To the best of our knowledge, this is the first blind signature scheme with message recovery in pairing free environment. The comparison of our PF-IDBS-MR scheme with the existing schemes shows that the proposed scheme is efficient in terms of computational and communicational point of view. The proposed scheme is very useful in practical applications such as mobile communications, wireless sensor networks etc., where bandwidth is the main constrain. Due to the blindness and message recovery property, computational, and communicational efficiency, the proposed PF-IDBS-MR scheme can be applied efficiently in the design of e-voting and e-payment applications.

**Author Contributions:** Conceptualization, S.J.; Investigating, S.J.; Problem Designing, P.V.R.; Formal Analysis and Writing, N.B.G.; Review and Editing, N.B.G.; Supervision, P.V.R.

**Funding:** This research is received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
2. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 20–24 August 2000; pp. 47–53.
3. Chang, C.C.; Lee, J.S. An anonymous voting mechanism based on the key exchange protocol. *Comput. Secur.* **2006**, *25*, 307–314. [CrossRef]
4. Fan, C.I.; Sun, W.Z. An efficient multi-receipt mechanism for uncoercible anonymous electronic voting. *Math. Comput. Model.* **2008**, *48*, 1611–1627. [CrossRef]
5. Liaw, H.T. A secure electronic voting protocol for general elections. *Comput. Secur.* **2004**, *23*, 107–119. [CrossRef]

6. Delaune, S.; Kremer, S.; Ryan, M. Coercion-resistance and receipt-freeness in electronic voting. In Proceedings of the 19th IEEE Computer Security Foundations Workshop, Venice, Italy, 5–7 July 2006; pp. 28–42.
7. Chaum, D. Blind Signatures for Untraceable Payments. Available online: https://link.springer.com/chapter/10.1007%2F978-1-4757-0602-4_18#citeas (accessed on 3 October 2018).
8. Chaum, D.; Fiat, A.; Naor, M. Untraceable electronic cash. *Adv. Cryptol.* **1990**, *403*, 319–327.
9. Nyberg, K.; Rueppel, R.A. A New Signature Scheme Based on the DSA Giving Message Recovery. In Proceedings of the 1st ACM Conference on Communication and Computer Security, Fairfax, VA, USA, 3–5 November 1993.
10. Jeng, F.G.; Chen, T.L.; Chen, T.S. An ECC-based blind signature scheme. *J. Netw.* **2010**, *5*, 921–928. [CrossRef]
11. Shen, V.R.L.; Chung, Y.F.; Chen, T.S.; Lin, Y.A. A Blind Signature Based on Discrete Logarithm Problem. *Int. J. Innov. Comput. Inf. Control* **2011**, *7*, 5403–5416.
12. Garcia, L.L.; Perez, L.J.D.; Henriquez, F.R. A pairing-based blind signature e-voting scheme. *Comput. J.* **2014**, *57*, 1460–1471. [CrossRef]
13. Verma, G.K.; Singh, B.B. New ID based fair blind signatures. *Int. J. Current Eng. Sci. Res.* **2016**, *3*, 41–47.
14. Darwish, A.; Gendy, M.M.E. A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. *Int. J. Swarm Intel. Evol. Comput.* **2017**, *6*, 2. [CrossRef]
15. Sahu, R.A.; Padhye, S. ID-based signature scheme from bilinear pairings: A survey. *Front. Electr. Electron. Eng.* **2011**, *6*, 487–500. [CrossRef]
16. Zhang, F.; Kim, K. ID-based blind signature and ring signature from pairings. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002.
17. Zhang, F.; Kim, K. Efficient ID-based blind signature and proxy signature. In Proceedings of the Australasian Conference on Information Security and Privacy, Sydney, NSW, Australia, 9–11 July 2003.
18. Huang, Z.; Chen, K.; Wang, Y. Efficient identity-based signatures and blind signatures. In Proceedings of the International Conference on Cryptology and Network Security, Xiamen, China, 14–16 December 2005.
19. Zhao, Z.; Zhao, Z.; Tang, X.; Liu, Y. A New ID-Based Blind Signature from Bilinear Pairings. In Proceedings of the 2006 IET International Conference on Wireless, Mobile and Multimedia Networks, Hangzhou, China, 6–9 November 2006.
20. Kalkan, S.; Kaya, K.; Selcuk, A.A. Generalized ID-Based Blind Signatures from Bilinear Pairings. In Proceedings of the 23rd International Symposium on Computer and Information Sciences, Istanbul, Turkey, 27–29 October 2008.
21. Rao, B.U.; Ajmath, K.A.; Reddy, P.V.; Gowri, T. An ID-Based Blind Signature Scheme from Bilinear Pairings. *Int. J. Comput. Sci. Secur.* **2010**, *4*, 98–106.
22. Hess, F. Efficient identity-based signature schemes based on pairings. In Proceedings of the International Workshop on Selected Areas in Cryptography, St. John's, NF, Canada, 15–16 August 2002.
23. Fan, C.I.; Sun, W.Z.; Huang, V.S.M. Provably secure randomized blind signature scheme based on bilinear pairing. *Comput. Math. Appl.* **2010**, *60*, 285–293. [CrossRef]
24. Zhang, L.; Hu, Y.; Tian, X.; Yang, Y. Novel identity-based blind signature for electronic voting system. In Proceedings of the 2010 Second International Workshop on Education Technology and Computer Science, Wuhan, China, 6–7 March 2010; pp. 122–125.
25. Shakerian, R.; Pour, T.M.; Kamali, S.H. An identity based public key cryptography blind signature scheme from bilinear pairings. In Proceedings of the 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; pp. 28–32.
26. He, D.; Chen, J.; Zhang, R. An efficient identity-based blind signature scheme without bilinear pairings. *Comput. Electr. Eng.* **2011**, *37*, 444–450. [CrossRef]
27. Hu, X.; Wang, J.; Yang, Y. Secure ID-based blind signature scheme without random oracle. In Proceedings of the 2011 International Conference on Network Computing and Information Security, Guilin, China, 14–15 May 2011; pp. 245–249.
28. Xu, G.; Xu, G. An ID-based Blind Signature from Bilinear Pairing with Unlinkability. In Proceedings of the 3rd International Conference on Consumer Electronics, Communications and Networks, Xianning, China, 20–22 November 2013.

29. Jain, R.T.; Patel, A.A. Computationally Efficient ID-Based Blind Signature Scheme in E-Voting. *Int. J. Sci. Res. Dev.* **2013**, *1*. Available online: https://s3.amazonaws.com/academia.edu.documents/33502839/IJSRDV1I3034.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1539744028&Signature=o5N7XWZ%2BVlfugIaaf%2FESsqJzfCc%3D&response-content-disposition=inline%3B%20filename%3DComputationally_Efficient_ID-Based_Blind.pdf (accessed on 26 September 2018).
30. Li, F.; Zhang, M.; Takagi, T. Identity-based partially blind signature in the standard model for electronic cash. *Math. Comput. Model.* **2013**, *58*, 196–203. [CrossRef]
31. Pance, R.; Ljupcho, A. Comparison of ID-Based Blind Signatures from Pairings for E-Voting Protocols. In Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 26–30 May 2014; pp. 26–30.
32. Girish; Krupa, K.T.; Phaneendra, H.D. Survey on Identity Based Blind Signature. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *6*, 2678–2681.
33. Islam, S.H.; Amin, R.; Biswas, G.P.; Obaidat, M.S.; Khan, M.K. Provably Secure Pairing-Free Identity-Based Partially Blind Signature Scheme and Its Application in Online E-Cash System. *Arab. J. Sci. Eng.* **2016**, *41*, 3163–3176. [CrossRef]
34. Kumar, M.; Katti, C.P.; Saxena, P.C. An Identity-Based Blind Signature Approach for E-Voting System. *Int. J. Modern Educ. Comput. Sci.* **2017**, *10*, 47–54. [CrossRef]
35. Sarde, P.; Banerjee, A. A Secure ID-Based Blind and Proxy Blind Signature Scheme from Bilinear Pairings. *J. Appl. Secur. Res.* **2017**, *12*, 2. [CrossRef]
36. Han, S.; Chang, E. A Pairing-Based Blind Signature Scheme with Message Recovery. *Int. J. Inf. Technol.* **2007**, *1*, 2602–2607.
37. Hassan, E.; Yasmine, A. A New Blind Identity-Based Signature Scheme with Message Recovery. *Online J. Electron. Electr. Eng.* **2008**, *2*, 2.
38. Diao, L.; Gu, J.; Yen, I.L. A New Proxy Blind Signature Scheme with Message Recovery. *Inf. Technol. J.* **2013**, *12*, 6159–6163.
39. James, S.; Gowri, T.; Babu, G.R.; Reddy, P.V. Identity-Based Blind Signature Scheme with Message Recovery. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 2674–2682.
40. Verma, G.K.; Singh, B.B. Efficient identity-based blind message recovery signature scheme from pairings. *Inst. Eng. Technol. J.* **2018**, *12*, 150–156. [CrossRef]
41. Koblitz, N. Elliptic curve cryptosystem. *J. Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
42. Miller, V.S. Use of elliptic curves in cryptography. *Proc. Adv. Cryptol.* **1985**, *218*, 417–426.
43. Pointcheval, D.; Stern, J. Security arguments for digital signatures and blind signatures. *J. Cryptol.* **2000**, *13*, 361–396. [CrossRef]
44. Ren, K.; Lou, W.; Zeng, K.; Moran, P.J. On broadcast authentication in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 4136–4144. [CrossRef]
45. Cao, X.; Kou, W.; Du, X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Inf. Sci.* **2010**, *180*, 2895–2903. [CrossRef]
46. Tan, S.Y.; Heng, S.H.; Goi, B.M. Java Implementation for Pairing-Based Cryptosystems. *Proc. Int. Conf. Comput. Sci. Appl.* **2010**, *6019*, 188–198.
47. Shamus Software Ltd. Miracl Library. Available online: https://www.miracl.com (accessed on 3 October 2018).
48. Chung, Y.F.; Huang, K.H.; Lai, F.; Chen, T.S. ID-based digital signature scheme on the elliptic curve cryptosystem. *Comput. Stand. Interfaces* **2007**, *29*, 601–604. [CrossRef]
49. Barreto, P.S.L.M.; Libert, B.; McCullagh, N.; Quisquater, J.J. Efficient and provably secure identity-based signatures and signcryption from bilinear maps. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, 4–8 December 2005; Volume 3788, pp. 515–532.