Efficient Provably Secure ID-based Blind Signature with Message Recovery

Wei Cui\(^1\), Qian Jia\(^2\)

\(^1\) Information Center of Ministry of Science and Technology, Beijing, 100862, China
\(^2\) Center of Neurology, Beijing Tiantan Hospital, Capital Medical University, Beijing, 100050, China
dacui635@163.com*

**Keywords:** ID-based Blind Signature; Message Recovery; Provably Secure

**Abstract:** Due to the rapid growth in popularity of electronic cash, electronic voting and location-based mobile, the design of secure schemes with low-bandwidth and blocking attacks capability is an important research issue. In this paper, we propose an efficient provably secure ID-based blind signature with message recovery scheme based on bilinear pairings. In the scheme, the original message is not required to be transmitted together with the signature and it can be recovered during the signature verification process. Assuming the intractability of the \(q\)-Strong Diffie-Hellman problem, our scheme is unforgeable under adaptive chosen-message and ID attack. The proof of correctness and blindness property analysis of the proposed scheme are presented. The scheme can offer advantages in runtime over the schemes available.

1. Introduction

Blind signature is interactive signature scheme, which provides anonymity of users to get a signature without giving the signer any information about the actual message. ID-based blind signature is attractive since one’s public key is simply his/her identity. The first ID-based blind signature (IBBS) schemes based on bilinear pairings was proposed by Zhang [1]. Recently, Kumar [2] proposed a new blind signature scheme using identity-based technique in 2017. The concept of general signatures with message recovery (MRS) was introduced by Nyberg [3]. In this scheme, the message is not sent with the signature and it is recovered from the verification process. Tso [4] proposed two new ID-based signature schemes with message recovery.

A blind signature with message recovery is important for many applications which requires the smaller bandwidth for signed messages than signatures without message-recovery. In 2005, Han [5] first proposed a pairing-based blind signature scheme with message recovery. Later, Hassan [6] and James[7] respectively proposed a new identity-based blind signature scheme with message recovery(ID-MR-BS) based on bilinear. Recently, Verma[8] presented an efficient ID-MR-BS from pairings which achieves bandwidth savings and is suitable for signing short messages in 2018.

In this paper, we propose an efficient provably secure ID-based blind signature with message recovery scheme based on bilinear pairings. Then, we discuss the security and efficiency of our schemes. The proposed scheme is unforgeable with the assumption that the \(q\)-Strong Diffie-Hellman problem (\(q\)-SDHP) is hard in the random oracle. The scheme needs less computing power as compared with others schemes.

Some background on bilinear pairings and \(q\)-SDHP problem that we use in our proposed scheme are introduced in Section 2. In Section 3, we describe our proposed ID-based blind signature scheme with message recovery and analyze its security. The comparison of the performance with other ID-based blind signature scheme with message recovery is shown in Section 4. Finally, we draw our conclusion in section 5.
2. Preliminaries

2.1 Pairings

Let us consider groups $G_1, G_2$ and $G_T$ of the same prime order $p$, where $G_1$ and $G_2$ are additive groups, and $G_T$ is a multiplicative group. Let $P, Q$ be generators of respectively $G_1$ and $G_2$. We say that $(G_1, G_2, G_T)$ are bilinear map groups if there exists a bilinear map $e : G_1 \times G_2 \rightarrow G_T$ satisfying the following properties:

1) Bilinearity: $\forall (P, Q) \in G_1 \times G_2$, $\forall a, b \in \mathbb{Z}$, $e(aP, bQ) = e(P, Q)^{ab}$

2) Non-degeneracy: $\forall S \in G_1$, $e(S, T) = 1$ if $S = O$.

3) Computability: $\forall (P, Q) \in G_1 \times G_2$, $e(P, Q)$ is efficiently computable.

4) There exists an efficient, publicly computable isomorphism $\psi : G_2 \rightarrow G_1$ such that $\psi(Q) = P$.

We can obtain such bilinear map groups with ordinary elliptic curves such as those suggested in [9].

2.2 Intractability Assumption

The computational assumptions for the security of our schemes were previously formalized by Boneh and Boyen [10] and are recalled in the following definition.

**Definition 1([10]):** Let us consider bilinear map groups $(G_1, G_2, G_T)$ and generators $P \in G_1$ and $Q \in G_2$.

The $q$-Strong Diffie-Hellman problem ($q$-SDHP) in the groups $(G_1, G_2)$ consists in, given a $(q + 2)$-tuple $(P, Q, \alpha P, \alpha^2 Q, \ldots, \alpha^q Q)$ as input, finding a pair $(c, \frac{1}{c + \alpha} P)$ with $c \in \mathbb{Z}_p^*$. 

3. New ID-based Blind Signature with Message Recovery

**Setup:** given a security parameter $k$, the PKG chooses bilinear map groups $(G_1, G_2, G_T)$ of prime order $p > 2^k$ and generators $Q \in G_2$, $P = \psi(Q) \in G_1$, $g = e(P, Q)$. The user may compute $g = e(P, Q)$ beforehand outside of the signing protocol. It then selects a master key $s \in \mathbb{Z}_p^*$, $Q_{pub} = sQ \in G_2$ and hash functions $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p$, $H_2 : \mathbb{G} \rightarrow \mathbb{Z}_p^*$. We can select $l_1, l_2$ as positive integers such that $l_1 + l_2 = \lfloor \log_2 p \rfloor$. The public parameters are

$$\text{params} := \{G_1, G_2, G_T, P, Q, g, Q_{pub}, e, \psi, H_1, H_2, F_1, F_2\}$$

**Extract:** Given an identity ID, the private key $S_{ID} = \frac{1}{x + H_1(ID)} P$, Note if $s + H_1(ID) \equiv 0 \mod p$, then abort $s$ and return SETUP to choose another $s$.

**Blind signature issuing protocol:** Suppose that $M \in \{0, 1\}^*$ is the message to be signed.

- The signer randomly chooses a number $x \in \mathbb{Z}_p^*$, computes $r = g^x \in G_T$, and sends $r$ to the user as commitment.

- (Blinding) The user randomly chooses $a, b \in \mathbb{Z}_p^*$ as blinding factors. He computes $r' = r^a g^{ab}$, $U = [F_1(M) \parallel F_2(F_1(M) \oplus M)]$, $w = [H_2(r') \oplus U]$ sends $z = a^{-1}w + b$ to signer.

- (Signing) The signer sends $V$ to user, where $V = (x + z)S_{ID}$.

- (Unblinding) The user computes $V' = aV$. He outputs signature $\text{sig} = (w, V')$ as the blind signature on the message $M$.

**Blind Signature Verification:** Given ID and the signature $(w, V')$, anyone can verify the signature and recover the message as follows:

$$\text{Compute } d = [w]_2 \parallel H_2(e(V', Q_{ID}) \cdot g^{-w}) \text{ and } m = F_2(x) \parallel d \parallel [d]_l \text{, where } Q_{ID} = H_1(ID)Q + Q_{pub}$$

Accept the signature if and only if $[d]_l | w = F_1(m)$.
4. Security Analysis

The verification of the signature is justified by the following equations:

\[ e(V', Q_{id}) \cdot g^{-w} \]
\[ = e(V', H_1(ID)Q + Q_{pub}) \cdot g^{-w} \]
\[ = e(a(x + z)S_{id}, H_1(ID)Q + Q_{pub}) \cdot e(P, Q)^{-w} \]
\[ = e(a(x + z)P, Q) \cdot e(P, Q)^{-w} \]
\[ = e((ax + w + ab)P, Q) \cdot e(P, Q)^{-w} \]
\[ = r^a \cdot g^{ab} = r' \]  

(1)

According to the equation (1), we can get the following equations:

\[ d = [w]_2 \oplus H_2(e(V', Q_{id}) \cdot g^{-w}) \]
\[ = [w]_2 \oplus H_2(r') \]
\[ = U \]  

(2)

\[ m = F_6(\{d\} \oplus \{d\} \oplus \{d\} \oplus \{d\} \oplus \{d\} \oplus \{d\}) \]
\[ = F_6(U \oplus U \oplus U \oplus U \oplus U \oplus U) \]
\[ = F_6(F_6(M)) \oplus F_6(F_6(M) \oplus M) \]
\[ = M \]  

(3)

Theorem 1. The proposed scheme has the blindness property.

**Proof:** For \( i = 0, 1 \), let \((r_i, x_i, z_i, V_i)\) be data appearing in the view of the signer during the execution of the signature issuing protocol with the user on message \( M_i \), and let \((w_i, V_i)\) be the corresponding message-signature pair. It is sufficient to show that there exists factors \((a, b)\) that maps \((r_i, x_i, z_i, V_i)\) to \((w_j, V_j)\) for each \( i, j \in \{0, 1\} \). The following equations must hold for \( a, b \in \mathbb{R} \) \( Z_p^* \).

\[ V_j = a \cdot V_i \]
\[ z_i = a^{-1} w_j + b \]

(4)

(5)

So we can get \( a = \log_{r_j} V_j \) and \( b = z_i - a^{-1} w_j \). Because \((w_j, V_j)\) is a valid signature, we can show that \( a \) and \( b \) satisfy equation \( e(V_j, Q_{id}) \cdot g^{-w} = r^a \cdot g^{ab} \). According to equations (4) and (5), we have:

\[ e(V_j, Q_{id}) \cdot g^{-w} \]
\[ = e(aV_j, H_1(ID)Q + Q_{pub}) \cdot g^{-w} \]
\[ = e(a(x + z)S_{id}, H_1(ID)Q + Q_{pub}) \cdot e(P, Q)^{-w} \]
\[ = e(a(x + a^{-1}w_j + b)P, Q) \cdot g^{-w} \]
\[ = e((P, Q)^{a(x + a^{-1}w_j + b)}, e(P, Q)^{-w} \]
\[ = e(P, Q)^{a(x + a^{-1}w_j + b)} = r^a \cdot g^{ab} \]

Thus the blinding factors always exist which lead to the same relation defined in the signature issuing protocol.

**Lemma 1 ([16]):** If there is a forger \( F_0 \) for an adaptively chosen message and identity attack having advantage \( \varepsilon_0 \) against our scheme when running in a time \( t_0 \) and making \( q_h \) queries to random oracle \( h_1 \), then there exists an algorithm \( F_i \) for an adaptively chosen message and given identity attack which has advantage \( \varepsilon_i \geq \varepsilon_0(1 - 1/p)/q_h \) within a running time \( t_i \leq t_0 \) Moreover, \( F_i \) asks the same number key extraction queries, signature queries and \( H_2 \)-queries as \( F_0 \) does.

**Lemma 2.** In the random oracle model, if an algorithm \( F \) \((t, q_h, q, q_E, q_S, \varepsilon)\)-breaks the proposed scheme with probability \( \varepsilon \) and time \( t \) under the adaptive chosen message and given
identity attack, with making $q_h$ queries to random oracle $h_1, q_f$ queries to random oracle $F_1$, $q_s$ queries to Extract Query and $q_e$ queries to signature issuing protocol. Then there is another $(t', \varepsilon')$ algorithm $B$ which can solve the $q$-SDHP for $q = q_h$ and $q_e \leq q_h$, where $t' \leq 120686q_h \cdot t / \varepsilon$ and $\varepsilon' \geq (1 - \frac{1}{n}) (1 - \frac{\varepsilon}{q_0}) \varepsilon (1 - \frac{\varepsilon}{q_0}) \varepsilon$.

**Proof:** Suppose that an algorithm $F$ run by an adversary $(t, q_h, q_f, q_e, q_s, \varepsilon)$ breaks the proposed scheme by the adaptive chosen message and given identity attacks. We can construct an algorithm $B$ to solve the $q$-SDHP through interacting with $F$.

Algorithm $B$ takes as input $(P, \alpha, \gamma, \ldots, \gamma)$ and aims to find a pair $(\gamma, \gamma_e)$. In the setup phase, it builds a generator $G \in G_1$, and does the following steps:

1) It picks $w_1, w_2, \ldots, w_{q-1} \in \mathbf{Z}^*$ and $f(z) = \prod_{i=1}^{q-1} (z + w_i)$ is expanded to obtain $c_0, c_1, \ldots, c_{q-1} \in \mathbf{Z}^*$ so that

$$ f(z) = \sum_{i=0}^{q-1} c_i z^i $$

2) $G = \gamma(H) = f(\alpha)P \in G_1$. The public key $H_{pub} \in G_2$ is fixed to $H_{pub} = \sum_{i=1}^{q-1} c_i (\alpha')Q$ so that $H_{pub} = \alpha H$, although $B$ does not know $\alpha$.

3) For $1 \leq i \leq q-1$, $B$ expands $f(z) = f(z) / (z + w_i)$

$$ f(z) = \sum_{i=0}^{q-1} d_i \gamma_i(\alpha')Q = \frac{f(\alpha)P}{\alpha + w_i} = \frac{1}{\alpha + w_i} G \left( w_i, \frac{1}{\alpha + w_i} G \right) $$

can be computed from this equation. Then, $B$ sent the public key to $F$, and take the $(H_{pub}, ID)$ as the input of $F$. $F$ issues the following queries for the identities (ID$_1, ID_2, \ldots, ID_{q_1}$) and the messages $(M_1, M_2, \ldots, M_{q_5})$. $B$ simulates queries as follows:

1) **ID Hash Query**: $B$ constructs hash table $L_1$ to store the answers of ID hash query, and returns the same answer for the same query. For any given $ID_1(1 \leq i \leq q_{id})$, if $ID_1 = ID^*$, $B$ answers $w = w^*$. Otherwise, answers $w = w_1 \in \mathbf{Z}^*$. In both cases $B$ stores $(ID, w)$ in a list $L_1$.

2) **H$_2$ Hash Query**: $B$ constructs hash table $L_2$ to store the answers of H$_2$ hash query, returns the same answer for the same query. For any given $r_j^*$, $1 \leq j \leq q_{id}$, $B$ first checks $L_2$, if an entry $<r_j, h_j>$ for the query is found, $B$ returns the stored value $h_j$; otherwise, $B$ selects $h_j \in \mathbf{Z}^*$ which is different from other elements, and stores tuple $<r_j, h_j>$ in the $L_2$, where $h_j \neq h_j^*$, $(i 
eq j)$. $B$ returns the value $h_j$ to $F$.

3) **F$_1$ Query**: $B$ constructs hash table $W_1$ to store the answers of F$_1$ hash query, and returns the same answer for the same query. For any given $M_1(1 \leq j \leq q_{id})$, $B$ first checks $W_1$, if an entry $<M_j, s_j>$ for the query is found, then $B$ checks $W_1$ and returns the stored value $<M_j, s_j>$. Otherwise, $B$ selects $s_j \in \mathbf{Z}^*$ which is different from other elements, and stores tuple $<M_j, s_j>$ in the $W_1$.

4) **F$_2$ Query**: $B$ constructs hash table $W_2$ to store the answers of F$_2$ hash query, and returns the same answer for the same query. For any given $M_1(1 \leq j \leq q_{id})$, $B$ first checks $W_2$, if an entry $<M_j, s_j>$ for the query is found, then $B$ checks $W_2$ and returns the stored value $<M_j, s_j>$. Otherwise, $B$ selects $s_j \in \mathbf{Z}^*$ which is different from other elements, and stores tuple $<M_j, s_j>$ in the $W_1$.

5) **Extract Query on ID $\neq ID^*$**: For any given $ID_1(1 \leq i \leq q_{id})$, $B$ recovers the matching pair $(ID, w)$ from $L_1$. $B$ computes $\frac{1}{\alpha + w} G$ and returns it.

6) **Issue Query**: For any given identity-message pair $(ID_1, M_1)$, if $ID_1 = ID^*$, $B$ aborts and reports failure. Otherwise, $B$ randomly picks $V_i \in G_1, r_i \in \mathbf{Z}^*$ and computes $r_i = e(V_i, Q_{id}) - e(G, H)^{\epsilon_i}$, where $Q_{id} = H_1(ID)H + H_{pub}$. Then $B$ defines the value $H_2(r_i)$ as $h_i$, and computes $d_i = [r_i]_2 \oplus h_i$. $B$
checks hash table \( L_1 \) for \( M_i \). If \( M_i \) is already defined, then \( B \) aborts. Otherwise, \( B \) stores tuple \(< M_i, q_i | l_i > \) in the \( L_1 \). \( B \) also checks table \( L_2 \) for \( i | d_i > \) if \( i | d_i > \) is already defined, then \( B \) aborts. Otherwise, \( B \) stores tuple \(< i | d_i >, M_i \oplus | d_i > \) in the \( L_2 \).

\( F \) outputs a pair \( < t_i, V_i' > \) for the user \( ID^* \), and it can pass the verify algorithm.

\( F \) can forge a signature \( < t_i, V_i' > \) without knowing the private key for \( ID^* \), so we can build \( F' \) that replays \( F \) on input \((H_{pub}, ID') \) to obtain forgeries \( t_{2}, V_{2}' > \), with \( h_i \neq h_{i'} \) by applying the forking lemma. The simulator \( B \) run \( F' \) to obtain \( < t_i, V_i' >, < t_2, V_2' > \) and recovers the pairs \( (ID', w') \) from list \( L_1 \). If both forgeries satisfy the verification equation, we obtain the relations \( e(V_1', Q_{m1}) e(G,H)^{x} = e(V_2', Q_{m2}) e(G,H)^{x} \), with \( Q_{m1} = H_{i}(ID')H + H_{pub} = (w + \alpha)H \). Then we can get \( e((t_1 - t_2)^{-1}(V_1' - V_2'), Q_{m3}) = e(G,H) \) and \( T' = (t_1 - t_2)^{-1}(V_1' - V_2') = \frac{1}{w + \alpha}G \). From \( T' \), \( B \) can do following steps as in [10] to extract \( \sigma' = \frac{1}{w + \alpha}P \):

1) We can obtain \( \gamma_{-1}, \gamma_0, \cdots, \gamma_{q-2} \in Z_p^* \) from \( f(z)/(z+w') \)

\[ \gamma_{-1}/(z+w') + \sum_{i=0}^{q-2} \gamma_i z^i \]

2) We can compute \( \sigma' = \frac{1}{\gamma_{-1}}(T' - \sum_{i=0}^{q-2} \gamma_i/\alpha(Q)) = \frac{1}{w + \alpha}P \)

In the step of Issue Query, \( B \) stops the simulation when \( < M_i, q_i | l_i > \) is in the \( W_1 \) or \( < i | d_i >, M_i \oplus | d_i > \) is in the \( W_2 \). The probability that those events does not happen is \((1 - \frac{q}{q_0}) \) and \((1 - \frac{q}{q_0}) \) respectively. And we note that \( w' \neq w_1, \cdots, w_{q-1} \) with probability at least \( 1-q/p \). For all the \( q_S \) issue queries, the success probability \( \varepsilon \) of \( B \) is \( \varepsilon \geq (1 - \frac{q}{q_0}) \varepsilon \) \((1 - \frac{q}{q_0}) \varepsilon \) \( \varepsilon \).

According to the forking lemma, the time \( t' \) is \( t' \leq 126068q_{h_a} \times t'/\varepsilon \)

The combination of the above lemmas yields the following theorem

**Theorem 2.** In the random oracle model, if an algorithm \( F(t, q_h, q_s, q_E, q_S, \varepsilon) \) breaks the proposed scheme with probability \( \varepsilon \geq 10(q_1 + 1)(q_h + q_s)/p \) under the adaptive chosen message and identity attack, then there is another \((t', \varepsilon')\) algorithm \( B' \) which can solve the \( q-SDHP \) for \( q = q_h \) and \( q_s \leq q_h \), where \( t' \leq 12608q_{h_a} \times q_h /\varepsilon \) and \( \varepsilon' \geq (1 - \frac{q}{p})(1 - \frac{q_1 + 1}{q_0}) \varepsilon \).

### 5. Efficiency

In this section, we compare our schemes to other available identity-based blind signature with message recovery based on bilinear pairings. In the following, we denote by \( M \) a scalar multiplication in \( G_1 \) and \( G_2 \), by \( A \) a addition in \( G_1 \) and \( G_2 \), by \( M_t \) the multiplication on \( G_t \), \( E \) an exponentiation in \( G_t \), \( H_M \) the MapToPoint function, \( I_{pq} \) a modular inversion operations, and by \( P \) a computation of the pairing.

| Scheme | our scheme | Verma[11] | James[10] | Hassan[9] | Han[8] |
|--------|------------|-----------|-----------|-----------|-------|
| Extract | 1M+1H_w | 2M+1H_w | 1M | 1M+1H_M | 1M+1H_M |
| Issue  | 1E+1Mt+ | 1P+4M+1L_a+ | 1P+6M+1L_a+3A | 1P+2M+1A | 2P+6M+2E+4A |
| Verify | 1P+1M+1E+1M | 2P+1E+1A+1Mt | 2P+1M | 2P+1E+1Mt+1H_M | 3P+E+2Mt |
| Total  | 1P+2Mt+2E+2M+2L_a+1A | 3P+6M+1E+1A+1L_a+3A | 2P+7M | 3P+3M+1E+1Mt+2H_a+1A | 5P+7M+3E+2Mt+H_a+4A |

According to Cao [12], we can get the time needed to execute related mathematical operations. To achieve 1024-bit RSA level security for pairing-based cryptosystem, we assume the Tate pairing.

Table 1. Calculations of Five ID-MR-BS Schemes
defined over super-singular elliptic curve on a finite field $F_q$, where $|q| = 512$ bits. Same security level for ECC based scheme, we have to use secure elliptic curve on a finite field $F_p$, where $|p| = 160$ bits. To compute the computation cost, we consider the time of computing $M$ is $T_M = 2.21ms$, the time of computing $M_t$ is $T_{M_t} = 2.32ms$, the time of computing $E$ is $T_E = 5.31ms$, the time of computing $H_M$ is $T_{H_M} = 3.04ms$, the time of computing $I_{nv}$ is $T_{I_{nv}} = 3.34ms$, the time of computing $P$ is $T_P = 20.04ms$. And remaining operations such as modular multiplications, modular addition, simple hash functions $H$, $F_1$, $F_2$ and elliptic, point addition are so efficient that no need to consider (for example, the time of computing modular multiplications is only 0.23ms).

Table 2. Efficiency comparison of Five ID-MR-BS Schemes

| Scheme | Our scheme | Verma[11] | James[10] | Hassan[9] | Han [8] |
|--------|------------|-----------|-----------|-----------|---------|
| Extract | 5.55ms     | 7.76ms    | 2.21ms    | 5.25ms    | 5.25ms  |
| Issue  | 21.59 ms   | 32.22 ms  | 36.64ms   | 24.46 ms  | 63.96 ms|
| Verify | 29.88 ms   | 47.71 ms  | 42.29 ms  | 50.75 ms  | 70.07 ms|
| Total  | 57.02 ms   | 87.69 ms  | 81.14 ms  | 80.46 ms  | 139.28 ms|

6. Conclusions

In this paper, we propose a new efficient ID-based blind signature scheme with message recovery based on bilinear parings and prove them as secure as the $q$-SDHP problem in the random oracle model. The Blindness property of our scheme provides the anonymity of the user and message recovery property provides to work with low band width applications. This scheme improves the efficiency of extracting secret key, issuing and verifying of ID-based blind signature scheme with message recovery.

References

[1] F. Zhang, and K. Kim, “ID-based blind signature and ring signature from pairings,” Advances in Cryptology Asiacrypt 2002, Springer-Verlag, Nov. 2002, pp.533-547.

[2] M. Kumar, C.P. Katti, and P. C. Saxena, “A New Blind Signature Scheme Using Identity-Based Technique,” International Journal of control Theory and applicationa vol. 10, Number 15, pp.115-124, 2017.

[3] K. Nyberg, Rainer A. Rueppel, “A new signature scheme based on the DSA giving message recovery,” Proceedings of ACM Conference on Computer and Communications Security, ACM Press, 1993, pp.58-61.

[4] R. Tso, C. Gu, T. Okamoto, and E. Okamoto, “Efficient ID-Based Digital Signatures with Message Recovery,” International Conference on Cryptology and Network Security, Springer-Verlag, 2007, pp. 47-59.

[5] S. Han, and E. Chang, “A Pairing-Based Blind Signature Scheme with Message Recovery,” International Journal of Information Technology. Singapore, vol. 2, Number 4, pp.187-192, 2005.

[6] E. Hassan, and A. Yasmine, “A New Blind Identity- Based Signature Scheme with Message Recovery,” The Online Journal of Electronics and Electrical Engineering. vol.2, Number 15, pp.200-205, Jan. 2008.

[7] S. James, T. Gowri, G.V. R. Babu and P. V. Reddy, “Identity-Based Blind Signature Scheme with Message Recovery,” International Journal of Electrical and Computer Engineering. San Bernardino Vol. 7, No. 5, Oct. 2017.

[8] G. K. Verma and B. B. Singh, “Efficient identity-based blind message recovery signature scheme from pairings,” IET Information Security. Hertford, Vol. 12, Iss. 2, pp.150-156, Mar. 2018.
[9] P. S. L. M. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order”, Selected Areas in Cryptography, Springer-Verlag, 2005, pp. 319-331.

[10] D. Boneh, and X. Boyen, “Short signatures without random oracles”, International Conference on the Theory and Applications of Cryptographic Techniques, Springer-Verlag, 2004, pp. 56-73.

[11] J. C. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman Groups”, International workshop on public key cryptography, Springer-Verlag, 2003, pp. 18-30.

[12] X. Cao, W. Kou and X. Du, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges,” Information Sciences. New York, vol. 180, pp. 2895–2903, August 2010.