Advances in Engineering Research, volume 173
4th Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2018)

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 $e: G_1 \times G_2 \to G_T$ satisfying the following properties:

1) Bilinearity: $\forall (P,Q) \in G_1 \times G_2$, $\forall a,b \in Z$, $e(aP,bQ) = e(P,Q)^{ab}$
2) Non-degeneracy: $\forall S \in G_1$, $e(S,T) = 1$, $T \in G_2$, 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 $\psi : G_2 \to G_1$ 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 $(P, Q, \alpha Q, \alpha^2 Q, \cdots, \alpha^q Q)$ as input, finding a pair $(c, \frac{1}{c+\alpha} P)$ with $c \in Z_p^*$.

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 computes $g = e(P,Q)$ beforehand outside of the signing protocol. It then selects a master key $s \in_R Z_p^*$, $Q_{pub} = sQ \in G_2$ and hash functions $H_1 : \{0,1\}^* \to Z_p^*$ $H_2 : G_T^* \to Z_{l_1+l_2}^*$. We can selects l_1, l_2 as positive integers such that $l_1+l_1=|p|$, $F_1 : \{0,1\}^{l_2} \to \{0,1\}^{l_1}$, $F_2 : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$ The public parameters are

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

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

Blind signature issuing protocol: Suppose that $M \in \{0,1\}^{l_2}$ is the message to be signed.

-The signer randomly chooses a number $x \in_R Z_p^*$, computes $r = g^x \in G_T$, and sends r to the user as commitment.

-(Blinding) The user randomly chooses $a, b \in_R Z_p^*$ as blinding factors. He computes $r' = r^{\alpha} g^{\alpha b}$, $U = [F_1(M) \| F_2 \ (F_1(M)) \oplus M]$, $w = [H_2(r') \oplus U]$ 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 $sig = (w, V')$ 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:

Compute $d = [w]_2 \oplus H_2(e(V', Q_{ID}) \cdot g^{-w})$ and $m = F_2({}_{l_1}|d|) \quad \oplus |d|_{l_2}$, where $Q_{ID} = H_1(ID)Q + Q_{pub}$

Accept the signature if and only if ${}_{l_1}|w| = F_1(m)$.

4. Security Analysis

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

$$\begin{aligned}
& e(V', Q_{ID}) \cdot g^{-w} \\
&= e(V', H_1(ID)Q + Q_{pub}) \cdot g^{-w} \\
&= e(a((x+z)S_{ID}), H_1(ID)Q + Q_{pub}) \cdot e(P,Q)^{-w} \\
&= e(a(x+z)P, Q) \cdot e(P,Q)^{-w} \\
&= e((ax+w+ab)P, Q) \cdot e(P,Q)^{-w} \\
&= r^a \cdot g^{ab} = r'
\end{aligned} \tag{1}$$

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

$$\begin{aligned}
d &= [w]_2 \oplus H_2(e(V', Q_{ID}) \cdot g^{-w}) \\
&= [w]_2 \oplus H_2(r') \\
&= U
\end{aligned} \tag{2}$$

$$\begin{aligned}
m &= F_2({}_{l_1}| d |) \oplus | d |_{l_2} \\
&= F_2({}_{l_1}| U |) \oplus | U |_{l_2} \\
&= F_2(F_1(M)) \oplus F_2(F_1(M) \oplus M \\
&= M
\end{aligned} \tag{3}$$

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, $b \in_R Z_p^*$.

$$V_j^{'} = a\, V_i \tag{4}$$

$$z_i = a^{-1} w_j + b \tag{5}$$

So we can get $a = \log_{V_i} V_j^{'}$ 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 $e(V_j', Q_{ID}) \cdot g^{-w_j} = r_i^a \cdot g^{ab}$ .According to equations (4) and (5), we have:

$$\begin{aligned}
& e(V_j^{'}, Q_{ID}) \cdot g^{-w_j} \\
&= e(aV_i, H_1(ID)Q + Q_{pub}) \cdot g^{-w_j} \\
&= e(a(x_i + z_i)S_{ID}, H_1(ID)Q + Q_{pub}) \cdot g^{-w_j} \\
&= e(a(x_i + a^{-1}w_j + b)P, Q) \cdot g^{-w_j} \\
&= e(P,Q)^{(ax_i + w_j + ab)} \cdot e(P,Q)^{-w_j} \\
&= e(P,Q)^{(ax_i + ab)} = r_i^x g^{ab}
\end{aligned}$$

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 ε_0 against our scheme when running in a time t_0 and making q_{h_1} queries to random oracle h_1, then there exists an algorithm F_1 for an adaptively chosen message and given identity attack which has advantage $\varepsilon_1 \geq \varepsilon_0(1-1/p)/q_{h_1}$ within a running time $t_1 \leq t_0$. Moreover, F_1 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_1}, q_{h_2}, q_E, q_S, ε)-breaks the proposed scheme with probability ε and time t under the adaptive chosen message and given identity attack, with making q_{h_i} queries to random oracle h_i, q_{F_i} queries to random oracle F_i, q_e queries to Extract Query and q_s queries to signature issuing protocol. Then there is another (t', ε') algorithm B which can solve the *q-SDHP* for $q = q_{h_1}$ and $q_E \le q_{h_1}$, where $t' \le 120686 q_{h_2} \cdot t/\varepsilon$ and $\varepsilon' \ge (1-\frac{q}{p})(1-\frac{q_S}{q_{F_1}})^{q_S}(1-\frac{q_S}{q_{F_2}})^{q_S}\varepsilon$

Proof: Suppose that an algorithm F run by an adversary (t, q_{h_1}, q_{h_2}, q_E, q_S, ε) -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 $(P, \alpha Q, \alpha^2 Q, \cdots, \alpha^q Q)$ and aims to find a pair $(c, \frac{1}{c+\alpha}P)$. In the ***setup phase***, it builds a generator $G \in G_1$, and does the following steps:

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

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

3) For $1 \le i \le q-1$, B expands $f_i(z) = f(z)/(z+w_i)$ $= \sum_{i=0}^{q-2} d_{i-1} z^i$, $\sum_{i=0}^{q-2} d_{i-1}\psi(\alpha^i Q) = f_i(\alpha)P = \frac{f(\alpha)}{\alpha+w_i}P = \frac{1}{\alpha+w_i}G$, so $(w_i, \frac{1}{\alpha+w_i}G)$ 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,…,ID_{q1}) and the messages (M_1, M_2, …, M_{qS}). 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 $ID_i(1 \le i \le q_{H_1})$, if $ID_i = ID^*$,B answers $w = w^*$. Otherwise, answers $w = w_1 \in Z_p^*$. 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' ($1 \le j \le q_{h_2}$), 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 $h_j' \in_R Z_p^*$ which is different from other elements, and stores tuple <r_j', h_j'> in the L_2, where $h_i' \ne h_j'$, ($i \ne j$). 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_j ($1 \le j \le q_s$), B first checks W_1, if an entry < M_j, s_{1j}> for the query is found, then B checks W_1 and returns the stored value < M_j, s_{1j}>. Otherwise, B selects $s_{1i} \in_R \{0,1\}^{l_1}$ which is different from other elements, and stores tuple < M_j, s_{1j}>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_j ($1 \le j \le q_s$), B first checks W_2, if an entry < M_j, s_{2j}> for the query is found, then B checks W_2 and returns the stored value < M_j, s_{2j}>. Otherwise, B selects $s_{2i} \in_R \{0,1\}^{l_1}$ which is different from other elements, and stores tuple < M_j, s_{2j}>in the W_1.

5) **Extract Query on** $ID \ne ID^*$: For any given $ID_i(1 \le i \le q_{h_1})$, 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_i, M_i), if ID_i=ID^*, then B aborts and reports failure. Otherwise, B randomly picks $V_i' \in G_1$, $t_i \in_R Z_p^*$ and computes $r_i = e(V_i', Q_{ID}) \cdot\ e(G,H)^{-t_i}$ where $Q_{ID} = H_1(ID)H + H_{pub}$. Then B defines the value $H_2(r_i)$ as h_i and computes $d_i = [t_i]_2 \oplus h_i$. B

checks hash table L_1 for M_i. If M_i is already defined, then B aborts. Otherwise, B stores tuple $< M_i, {}_{l_1}|t_i| >$ in the L_1. B also checks table L_2 for ${}_{l_1}|d_i|$, if ${}_{l_1}|d_i|$ is already defined, then B aborts. Otherwise, B stores tuple $<{}_{l_1}|d_i|,\ M_i \oplus |d|_{l_2}>$ in the L_2.

F outputs a pair $< t_1, V_1' >$ for the user ID^*, and it can pass the verify algorithm.

F can forge a signature $< t_1, V_1' >$ 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 $h_1 \neq h_2$ by applying the forking lemma. The simulator B run F' to obtain $< t_1, V_1' >$, $< t_2, V_2' >$ and recovers the pairs (ID^*, w^*) from list L_1. If both forgeries satisfy the verification equation, we obtain the relations $e(V_1', Q_{ID}^*) e(G,H)^{-t_1} = e(V_2', Q_{ID}^*) \cdot e(G,H)^{-t_2}$, with $Q_{ID^*} = H_1(ID^*)H + H_{pub} = (w^* + \alpha)H$ .Then we can get $e((t_1 - t_2)^{-1}(V_1' - V_2'), Q_{ID^*}) = e(G,H)$ 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 $\sigma^* = \frac{1}{\gamma_{-1}}[T^* - \sum_{i=0}^{q-2} \gamma_i \psi(\alpha^i Q)] = \frac{1}{w^* + \alpha} P$

In the step of ***Issue Query***, B stops the simulation when $< M_i, {}_{l_1}|t_i| >$ is in the W_1 or $<{}_{l_1}|d_i|,\ M_i \oplus |d|_{l_2}>$ is in the W_2. The probability that those events does not happen is $(1 - \frac{q_S}{q_{F_1}})$ and $(1 - \frac{q_S}{q_{F_2}})$ 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 ε' of B is $\varepsilon' \geq (1 - \frac{q}{p})(1 - \frac{q_S}{q_{F_1}})^{q_S}(1 - \frac{q_S}{q_{F_2}})^{q_S}\varepsilon$. According to the forking lemma, the time t' is $t' \leq 120686 q_{h_2} \cdot t/\varepsilon$

The combination of the above lemmas yields the following theorem

Theorem 2. In the random oracle model, if an algorithm F $(t, q_{h_1}, q_{h_2}, q_{F_1}, q_{F_2}, q_E, q_S, \varepsilon)$-breaks the proposed scheme with probability $\varepsilon \geq 10(q_s + 1)(q_{h_2} + q_s)/p$ under the adaptive chosen message and identity attack, then there is another (t', ε') algorithm B which can solve the q-$SDHP$ for $q = q_{h_1}$ and $q_E \leq q_{h_1}$, where $t' \leq 120686 q_{h_2} \cdot q_{h_1}/\varepsilon$ and $\varepsilon' \geq (1 - \frac{q}{p})(1 - \frac{q_S}{q_{F_1}})^{q_S} \cdot (1 - \frac{q_S}{q_{F_2}})^{q_S} q_{h_1} \varepsilon$

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_{nv} a modular inversion operations, and by P a computation of the pairing.

Table 1. Calculations of Five ID-MR-BS Schemes

Scheme	our scheme	Verma[11]	James[10]	Hassan[9]	Han [8]
Extract	1M+ 1I_{nv}	2M+ 1I_{nv}	1M	1M+1 H_M	1M+1 H_M
Issue	3E+1Mt +1I_{nv}	1P+4M +1I_{nv}+1A	1P+6M +1I_{nv}+3A	1P+2M+1A	2P+6M+2E +4A
Verify	1P+1Mt+1E +1M+1A	2P+1E+1A +1Mt	2P+1M	2P+1E+1Mt +1 H_M	3P+E +2Mt
Total	1P+2Mt +4E+2M +2I_{nv}+1A	3P+6M +1E+1A +2I_{nv}+1Mt	2P+7M +1I_{nv}+3A	3P+3M +1E+1Mt +2H_M+1A	5P+7M +3E+2Mt +1H_M+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 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	5.55*ms*	7.76 *ms*	2.21 *ms*	5.25 *ms*	5.25 *ms*
Issue	21.59 *ms*	32.22 *ms*	36.64 *ms*	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 Asiacrpt 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] [12] 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.