New Certificateless Blind Ring Signature Scheme

Hua Sun*, Yanqiang Ge
School of Computer and Information Engineering, Anyang Normal University
Anyang 455000, China
*Corresponding author, e-mail: sh1227@163.com

Abstract
A new certificateless blind ring signature scheme was proposed in this paper. The scheme could not only avoid the problem of certificate management of public key certificate cryptography, but also overcome the inherent key-escrow problem of identity-based public key cryptography. In the last, by using bilinear pairing technique, it was proved that this scheme satisfied the security of existential unforgeability, blindness and unconditional anonymity.

Keywords: Certificateless cryptography, Blind ring signature, k-collision attack algorithm problem, Modified inverse computational Diffie-Hellman problem

Copyright © 2014 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction
In 1984, ID-based public key cryptography (ID-PKC) was proposed by Shamir [1], which was utilized to solve the certificate management problems in traditional PKC. In 2003, Al-Riyami et al. [2] introduced the concept of certificateless PKC that was used to resolve the inherent key-escrow problem in ID-based cryptography. In 2005, the security model of certificateless signature was firstly formally defined by Huang et al. [3]. In 2009, a certificateless signature scheme was proposed by Wan et al. [4] in the standard model, while it was proved to be not precise. In 2010, another certificateless signature without bilinear pairings was given by He et al. [5], and Zhang et al. [6] analyzed two certificateless signature schemes and pointed out their security weakness.

Blind signature was firstly put forward by Chaum [7], which could achieve the anonymity of users and was widely used in e-cash or e-voting systems. In 1996, the concept of partial blind signature was put forth by Abe et al. [8], such signatures contain the pre-agreed information of signers and users. In 2009, a certificateless partial blind signature scheme was proposed by Su et al. [9], which was inefficient. In 2012, a certificateless partial blind signature scheme and the corresponding security model were put forth by Liu et al. [10], but the scheme could not resist the forgery attack to pre-agreed information.

Ring signature was firstly described by Rivest et al. [11], which makes it possible to specify a set of possible signers without revealing which member actually produced the signature. In 2007, Chow et al. [12] gave the first certificateless ring signature, and Zhang et al. [13] proposed another certificateless ring signature scheme based on different assumptions, while the length of signature is longer. In 2008, two kinds of certificateless distributed ring signature schemes, based on identity-based distributed ring signature, were put forward by Sang et al. [14].

Blind ring signature has not only the blind attribute of blind signature, but also the anonymity of ring signature. In 2005, the first blind ring signature was proposed by Chan et al. [15], but it proved to be not secure. In 2006, another scheme was introduced by Wu et al. [16], while the scheme did not satisfy the unconditional anonymity, Javier et al. [17] put forth a blind ring signature with constant length and gave the security model of it. In this paper, a concrete construction of certificateless blind ring signature is proposed along with its security proofs.

2. Preliminaries
Let $G$ be an additive group of prime order $q$ and $G_T$ be a multiplicative group of the same order. A bilinear pairing is a map $e: G \times G \rightarrow G_T$ that satisfies the following properties:
1. Bilinear: \( e(aP, bQ) = e(P, Q)^a \) for all \( P, Q \in G \), \( a, b \in \mathbb{Z}_q \).
2. Non-degeneracy: there exists \( P, Q \in G \) such that \( e(P, Q) \neq 1 \).
3. Computability: There is an efficient algorithm to compute \( e(P, Q) \) for all \( P, Q \in G \).

**k-Collision Attack Algorithm (k-CAA) problem.** For an integer \( k \), and \( s \in \mathbb{Z}_q, P \in G \),
given \( t_1, \ldots, t_k, P, Q = sP, \frac{1}{t_i + s} P, \ldots, \frac{1}{t_k + s} P \), to compute \( \frac{1}{c + s} P \) for some \( c \in \mathbb{Z}_q^* \backslash \{t_1, \ldots, t_k\} \).

**Modified Inverse Computational Diffie-Hellman (mICDH) problem.** For \( a, b \in \mathbb{Z}_q^* \),
given \( b, P, aP \in G \), to compute \( (a + b)^{-1} P \).

3. A Concrete Certificateless Blind Ring Signature Scheme (CL-BRS)

In this section, we give the concrete construction of my CL-BRS.

**Setup:** Let \( G, G \) be groups of the same order \( q \), the bilinear pairing is given as \( e : G \times G \rightarrow G_f \). Given a security parameter \( k \), let \( P \) is a generator of \( G \). Choose a random number \( s \in \mathbb{Z}_q^* \), and set \( pub = sP, g = e(P, P) \). Define three hash functions \( H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^* \), \( H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^* \), \( H_3 : G \rightarrow \mathbb{Z}_q^* \). The parameters are \( \text{params} = (G, G_f, q, e, g, P, pub, H_1, H_2, H_3) \) and the system public-private key pair is \( mpk = pub, msk = s \).

**Partial-Private-Key-Extract:** A user submits his identity information \( ID \) to KGC. KGC computes \( q_{ID} = H_1(ID) \) and returns \( D_{ID} = (s + q_{ID})^{-1} P \) to user as his partial private key.

**Set-Public-Private-Key:** After obtaining his partial private key \( D_{ID} \), the user chooses a random number \( x_{ID} \in \mathbb{Z}_q^* \), computes \( Q_{ID} = P_{pub} + H_1(ID)P \), \( R_{ID} = x_{ID}Q_{ID} \), \( y_{ID} = H_3(R_{ID}) \), \( S_{ID} = (x_{ID} + y_{ID})^{-1}D_{ID} \) and output \( (R_{ID}, S_{ID}) \) as his public-private key pair.

**Blind-Ring-Sign:** Given the message \( m \), there is a group of \( n \) users whose identities from the set \( L = \{ID_1, \ldots, ID_n\} \) and the actual signer’s identity is \( AID = \{A \in 1, \ldots, n\} \). To produce a blind ring signature, the user and actual signer perform the following steps.

1. The signer randomly chooses a number \( \alpha \in \mathbb{Z}_q^* \), computes \( U = x(R_{ID} + y_{ID}Q_{ID}) \), and randomly chooses a number \( \alpha_i \in \mathbb{Z}_q, i \in 1, \ldots, n, i \neq A \), computes \( V_j = a_iP, u = e(P, \sum_{i \neq A} (R_{ID} + y_{ID}Q_{ID})) \), then sends \( R, U, U, V_j (i \in 1, \ldots, n, i \neq A) \) to the user.

2. (Blinding) The user randomly chooses \( \beta, g \in \mathbb{Z}_q^* \) as blinding factors. He computes \( r = \gamma^\alpha, U' = \alpha U, h = \alpha^{-1}H_2(m, L, r) + \beta \), sends \( h \) to the signer.

3. (Signing) The signer sends back \( S \), where \( S = (x + h)S_{ID} + xP \).

4. (Unblinding) The user computes \( V_j = \alpha S \) and outputs \( \sigma = (m, u, r', U', V_1, \ldots, V_n) \).

Then \( (u, r', U', V_1, \ldots, V_n) \) is the blind ring signature of the message \( m \).
Verify: To verify a blind ring signature $\sigma$, the verifier firstly computes $h = H_2(m,L,r)$, and verify $r'g^h e(P,U)^u = \prod_{i=1}^{n} e(V_i,R_{ID} + y_{ID_i}Q_{ID_i})$ holds with equality. then accept the blind ring signature as valid and output True if the above equation holds, otherwise, output False.

4. Analysis of the Proposed CLBRS Scheme

4.1. Correctness

$\prod_{i=1}^{n} e(V_i,R_{ID} + y_{ID_i}Q_{ID_i}) = e(V_i,R_{ID} + y_{ID_i}Q_{ID_i}) \prod_{i=1, j \neq i}^{n} e(V_j,R_{ID} + y_{ID_j}Q_{ID_j})$

$= e(\alpha(x+h)S_{ID_i},aP,R_{ID_j} + y_{ID_j}Q_{ID_j}) \prod_{i=1, j \neq i}^{n} e(V_j,R_{ID} + y_{ID_j}Q_{ID_i})$

$= e(\alpha(x+h)S_{ID_i},aP,R_{ID_j} + y_{ID_j}Q_{ID_j}) \prod_{i=1, j \neq i}^{n} e(V_j,R_{ID} + y_{ID_j}Q_{ID_i})$

$= e(P,P)^{ax+by+cy} \prod_{i=1}^{n} e(V_i,R_{ID_i} + y_{ID_i}Q_{ID_i}) = r'g^h e(P,U)^u$

4.2. Security Proofs

Theorem 1. Our CLBRS scheme has the blindness property.
Proof. As it can be easily proved, so we omit it here.

Theorem 2. Our CLBRS scheme has the unconditional anonymity property.
Proof. Let $\sigma = (m,u,r',U,V_1,...,V_n)$ be a valid blind ring signature of a message $m$ on behalf of a group of $n$ members specified by identities in $L$. Since all $a_i \in Z_q, i \in 1,...,n,i \neq A$ are randomly generated, hence $u = e(P,\sum_{i \neq A} a_i(R_{ID_i} + y_{ID_i}Q_{ID_i}))$ and all $V_i = a_iP (i \in 1,...,n,i \neq A)$ are also uniformly distributed. Also since $x \in Z_q$ and $\alpha,\beta \in Z_q$ are randomly generated, so $r' = r g^\alpha$, $U' = aU$ and $V_i = aS$ are uniformly distributed. This fact shows that the signature $\sigma$ does not leak any information about the identity of the actual signer.

Theorem 3. Our CLBRS scheme is existential unforgeable against the Type I adversary in the random oracle model assuming the $k$-CAA is hard.
Proof. Let $A_i$ be a forger that breaks the proposed signature scheme under adaptive chosen message and identity attack. There will exists an algorithm $B$ that can use $A_i$ to solve the k-CAA instance $(t_1,...,t_k,P,Q = sP, \frac{1}{t_1+s}, \frac{1}{t_k+s})$ where $k \geq q_{H_i}$ (we suppose $A_i$ makes at most $q_{H_i}$ queries to $H_i$ oracle). Its goal is to compute $\frac{1}{t+s}P$ for some $t \notin (t_1,...,t_k)$ and $ID^*$ denotes an arbitrary signer associated with the forgery.

$B$ sets $g = e(P,P)$ and $P_{pub} = Q = sP$ where $msk = s$ is the master key, which is unknown to $B$. $B$ then gives the system public parameters $params$ to $A_i$. Without loss of generality, we assume that any extraction (Partial-Private-Key-Extract, Public-Private-Key) and Sign queries are preceded by $H_i$ query, and Private-Key and Sign queries are preceded by Public-Key query. $B$ maintains four lists $L_1, L_2, L_3$ and $L_4 = (ID,R_{ID},x_{ID},\epsilon \in (0,1))$, where all of them are initially empty. When the attacker $A_i$ issues a number of queries, $B$ responds as follows:
H1 Queries: When Ai queries H1(IDi) where 1 ≤ i ≤ qK, if such query has already been made, B checks the list L1 and outputs the corresponding qID1. Otherwise, B picks j ∈ (1, qK) at random. If i = j (we let IDi = IDj at this point), B randomly chooses t∗ ∈ Z∗p and returns qID1 = t∗, otherwise B returns qID1 = t1,...,tk. B then computes QID1 = Ppub + qID1P and adds (ID1, QID1, qID1) to L1.

H2 Queries: When A1 queries H2(m, L1, r), if such query has already been made, B checks the list L2 and returns the corresponding h1. Otherwise, B randomly chooses h1 ∈ Z∗q and adds (m, L1, h1) to L2, then returns h1.

H3 Queries: When A1 queries H3(RID1), if such query has already been made, B checks the list L3 and outputs the corresponding yID1. Otherwise, B randomly chooses yID1 ∈ Z∗q and adds (RID1, yID1) to list L3, then returns yID1.

Partial-Private-Key Queries: When A1 makes a query on the partial private key of input ID1, if ID1 = ID∗, B outputs FALL and aborts the simulation; else if ID1 = ID∗, B returns DID1 = (t1 + s)−1 P.

Public-Key Queries: When A1 makes a query on the public key of input ID1, if the list L4 contains (ID1, RID1, xID1, c), B returns RID1. Otherwise, B finds (ID1, QID1, qID1) in L5, and randomly chooses xID1 ∈ Z∗p. B then returns RID1 = xID1QID1 and adds (ID1, RID1, xID1, 1) to L4.

Private-Key Queries: When A1 makes a query on the private key of input ID1, if ID1 = ID∗, B outputs FALL and aborts the simulation; else if ID1 = ID∗, B finds (ID1, RID1, xID1, c) in L4. If c = 1 and the list L3 contains (RID1, yID1), B returns SISID1 = (xID1 + yID1)−1 DID1; if c = 1 and the list L3 does not contain (RID1, yID1), B queries H3(RID1) and returns SISID1 = (xID1 + yID1)−1 DID1; if c = 0, B gets additionally information x∗ ID1 from A1 and simulates as in the above case (c = 1).

Public-key-Replacement Queries: When A1 makes a query on public key replacement of input (ID1, RID1), if the list L4 contains (ID1, RID1, xID1, c), B sets RID1 = R∗D1 and c = 0. Otherwise, B makes a public-key-replacement query on ID1, then sets RID1 = R∗D1 and c = 0.

Blind-Ring-Sign Queries: When A1 queries a blind ring signature on message m and a group of n users whose identities from the set L = {ID1,...,IDn}, B performs as following:

(a) B first finds (ID1, QID1, qID1), (ID1, RID1, xID1, c) in the list L4 and L4 for all i ∈ (1,...,n).

(b) If c = 1. B chooses an index Ai ∈ (1,...,n), and finds (RID1, yID1) for i ∈ (1,...,n) in the list L4; if it does not contain RID1, B randomly chooses yID1 ∈ Z∗p, and adds (RID1, yID1) to L4. B then randomly chooses a∗ ∈ Z∗p and computes V∗ i = a∗Pi, for all i ∈ (1,...,n), i ≠ A; B then randomly chooses V∗ i, U∗ ∈ G, h∗ i ∈ Z∗q, computes u = e(P, ∑i≠A a∗ j (RID1 + yID1QID1)),
New Certificateless Blind Ring Signature Scheme (Hua Sun)

\[ r^* = g^{-h}e(-U', P)e(V_{i}, R_{D_{i}} + y_{ID_{i}}Q_{D_{i}}) \] and set \( h_i = H_2(m, L, r^*) \). If the list \( L_2 \) has already contained \( H_2(m, L, r^*) \), \( B \) output FALL and aborts the simulation. Otherwise, \( B \) returns \( \sigma = (m, u, r^*, U', V_1, \ldots, V_n) \) and adds \( (m, L, r^*, h_i) \) to \( L_2 \).

(c) If \( c = 0 \), \( B \) gets additionally information \( x_{ID_i} \) from \( A_i \) and simulates as in the above case \( (c = 1) \).

Forgery: Finally, \( A_i \) outputs the a tuple \( (L^*, h_2, \sigma = (m^*, u, r^*, U', \cup_{i=1,i \neq d} V_i, V_A)) \) which means \( \sigma \) is a blind ring signature on message \( m^* \) on behalf of the group specified by identities in \( L^* = \{ID_1^*, \ldots, ID_n^*\} \), where suppose the actual signer’s identity is \( ID_d \) and \( h_i = H_2(m^*, L, r^*) \). According to the forking lemma, \( B \) then replays \( A_i \) with the same random tape but different \( 2^*H \). Suppose \( 2^*H \) outputs \( 1^2h \neq 1^2h \) in the first round and the second round respectively. We can get another different valid forge \( (L^*, h_2, \sigma = (m^*, u, r^*, U', \cup_{i=1,i \neq d} V_i, V_A')) \). According to the equations as follows:

\[ r^*g^h e(P, U') u = e(V^*, R_{m^*} + y_{ID_{m}}, Q_{ID_{m}}) \prod_{i=1,i \neq d}^n e(V^*, R_{m^*} + y_{ID_{m}}, Q_{ID_{m}}) \]

\[ r^*g^{h_2} e(P, U') u = e(V_{A^*}, R_{m^*} + y_{ID_{m}}, Q_{ID_{m}}) \prod_{i=1,i \neq d}^n e(V_{A^*}, R_{m^*} + y_{ID_{m}}, Q_{ID_{m}}) \]

we can get \( g^{h-h_2} = e(V_{A^*}, R_{D_{d}} + y_{ID_{d}}, Q_{D_{d}}) \), that is \( e(P, P)^{h-h_2} = e(V_{A^*}, R_{D_{d}} + y_{ID_{d}}, Q_{D_{d}}, s + q_{D_{d}}) \). Then we have

\[ e \left( \frac{1}{s + q_{D_{d}}}, P, P \right) = e \left( x_{ID_{d}} + y_{ID_{d}}, \frac{V_{A^*} - V_{A}}{h_i - h_2}, P \right). \]

So the solution of the problem k-CAA is

\[ \frac{1}{s + q_{D_{d}}} P = x_{ID_{d}} + y_{ID_{d}}, \frac{V_{A^*} - V_{A}}{h_i - h_2}. \]

**Theorem 4.** Our CLBRS scheme is existential unforgeable against the Type II adversary in the random oracle model assuming the mCDH is hard.

**Proof.** As the proof is quite straightforward, so we omit it here.

4. Conclusion

In this paper, we propose a concrete construction of certificateless blind ring signature scheme based on bilinear pairings in the random oracle model, which is more efficient by pre-computing the pairing \( g = e(P, P) \). Note that CLBRS schemes may be more efficient than blind ring signature schemes in traditional PKC since they avoid the costly computation for verification of the public key certificates. Also, it is impossible for the KGC to forge valid ring signatures because of no key-escrow in the certificateless public key setting.

**References**


