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*

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 $e: G \times G \to G_T$ that satisfies the following properties:

Received June 5, 2013; Revised July 16, 2013; Accepted August 29, 2013

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G$, $a, b \in Z_q$.
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 $s \in Z_q, P \in G$, given $\left(t_1, ..., t_k, P, Q = sP, \frac{1}{t_1 + s} P, ..., \frac{1}{t_k + s} P\right)$, to compute $\frac{1}{c+s} P$ for some $c \in Z_q^* \setminus (t_1, ..., t_k)$.

Modified Inverse Computational Diffie-Hellman (mICDH) problem. For $a, b \in Z_q^*$, 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 $e: G \times G \to G_T$. Given a security parameter k, let P is a generator of G. Choose a random number $s \in_R Z_q^*$ and set $P_{pub} = sP$, $g = e(P, P)$. Define three hash functions $H_1 : \{0,1\}^* \to Z_q^*$, $H_2 : \{0,1\}^* \to Z_q^*$, $H_3 : G \to Z_q^*$. The parameters are $params = (G, G_T, q, e, g, P, P_{pub}, H_1, H_2, H_3)$ and the system public-private key pair is $mpk = p_{pub}$, $msk = s$.

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 $x_{ID} \in Z_q^*$, 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 $L = \{ID_1, ..., ID_n\}$ and the actual signer's identity is $ID_A (A \in 1, ..., n)$. To produce a blind ring signature, the user and actual signer perform the following setps.

1. The signer randomly chooses a number $x \in Z_q$, computes $r = g^x$, $U = x(R_{ID} + y_{ID} Q_{ID})$, and randomly chooses a number $a_i \in Z_q, i \in 1, ..., n, i \neq A$, computes $V_i = a_i P$, $u = e\left(P, \sum_{i \neq A} a_i \left(R_{ID_i} + y_{ID_i} Q_{ID_i}\right)\right)$, then sends $r, U, u, V_i \left(i \in 1, ..., n, i \neq A\right)$ to the user.

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

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

4. (Unblinding) The user computes $V_A = \alpha S$ and outputs $\sigma = \left(m, u, r', U', V_1, ..., V_n\right)$.

Then $\left(u, r', U', V_1, ..., V_n\right)$ is the blind ring signature of the message m .

Verify: To verify a blind ring signature σ, the verifier firstly computes $h^{'} = H_2\left(m, L, r^{'}\right)$, and verify $r^{'} g^{h^{'}} e\left(P, U^{'}\right) u \overset{?}{=} \prod_{i=1}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right)$ 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

$$\prod_{i=1}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right)$$

$$= e\left(V_A, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \prod_{i=1, i \neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right) = e\left(\alpha\left(x+h\right) S_{ID_A} + \alpha x P, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \prod_{i=1, i \neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right)$$

$$= e\left(\alpha\left(x+h\right) S_{ID_A} + \alpha x P, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \prod_{i=1, i \neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right)$$

$$= e\left(\alpha\left(x+h\right) S_{ID_A}, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) e\left(\alpha x P, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \prod_{i=1, i \neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right)$$

$$= e\left(P, P\right)^{\left(\alpha x + \alpha\beta + H_2\left(m, L, r^{'}\right)\right)} \cdot e\left(P, U^{'}\right) \prod_{i=1, i \neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right) = r^{'} g^{h^{'}} e\left(P, U^{'}\right) u$$

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 $\sigma = \left(m, u, r^{'}, U^{'}, V_1, ..., V_n\right)$ 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 $u = e\left(P, \sum_{i \neq A} a_i \left(R_{ID_i} + y_{ID_i} Q_{ID_i}\right)\right)$ and all $V_i = a_i P\left(i \in 1, ..., n, i \neq A\right)$ are also uniformly distributed. Also since $x \in Z_q$ and $\alpha, \beta \in Z_q$ are randomly generated, so $r^{'} = r^{\alpha} g^{\alpha\beta}$, $U^{'} = \alpha U$ and $V_A = \alpha S$ are uniformly distributed. This fact shows that the signature σ 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 $(t_1, ..., t_k, P, Q = sP, \frac{1}{t_1 + s} P, ..., \frac{1}{t_k + s} P)$ where $k \geq q_{H_1}$ (we suppose A_I makes at most q_{H_1} queries to H_1 oracle). Its goal is to compute $\frac{1}{t+s} P$ for some $t \notin \left(t_1, ..., t_k\right)$ and ID^* denotes an arbitrary signer associated with the forgery.

B sets $g = e\left(P, P\right)$ 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_1 query, and Private-Key and Sign queries are preceded by Public-Key query. B maintains four lists L_1, L_2, L_3 and $L_4 = \left(ID, R_{ID}, x_{ID}, c \in \left(0,1\right)\right)$, where all of them are initially empty. When the attacker A_I issues a number of queries, B responses as follows :

H_1 *Queries*: When A_I queries $H_1\left(ID_i\right)$ where $1 \le i \le q_{H_1}$, if such query has already been made, B checks the list L_1 and outputs the corresponding q_{ID_i}. Otherwise, B picks $j \in \left(1, q_{H_1}\right)$ at random. If $i = j$ (we let $ID_i = ID^*$ at this point), B randomly chooses $t_x \in Z_q^*$ and returns $q_{ID^*} = t_x$, otherwise B returns $q_{ID_i} = t_i, t_i \in \left(t_1, ..., t_k\right)$. B then computes $Q_{ID_i} = P_{pub} + q_{ID_i}P$ and adds $\left(ID_i, Q_{ID_i}, q_{ID_i}\right)$ to L_1.

H_2 *Queries*: When A_I queries $H_2\left(m, L, r^{'}\right)$, if such query has already been made, B checks the list L_2 and outputs the corresponding h_i. Otherwise, B randomly chooses $h_i \in Z_q^*$ and adds $\left(m, L, r^{'}, h_i\right)$ to L_2, then returns h_i.

H_3 *Queries*: When A_I queries $H_3\left(R_{ID_i}\right)$, if such query has already been made, B checks the list L_3 and outputs the corresponding y_{ID_i}. Otherwise, B randomly chooses $y_{ID_i} \in Z_q^*$ and adds $\left(R_{ID_i}, y_{ID_i}\right)$ to list L_3, then returns y_{ID_i}.

Partial-Private-Key Queries: When A_I makes a query on the partial private key of input ID_i, if $ID_i = ID^*$, B output FALL and aborts the simulation; else if $ID_i \ne ID^*$, B returns $D_{ID_i} = \left(t_i + s\right)^{-1}P$.

Public-Key Queries: When A_I makes a query on the public key of input ID_i, if the list L_4 contains $\left(ID_i, R_{ID_i}, x_{ID_i}, c\right)$, B returns R_{ID_i}. Otherwise, B finds $\left(ID_i, Q_{ID_i}, q_{ID_i}\right)$ in L_1, and randomly chooses $x_{ID_i} \in Z_q^*$. B then returns $R_{ID_i} = x_{ID_i}Q_{ID_i}$ and adds $\left(ID_i, R_{ID_i}, x_{ID_i}, 1\right)$ to L_4.

Private-Key Queries: When A_I makes a query on the private key of input ID_i, if $ID_i = ID^*$, B output FALL and aborts the simulation; else if $ID_i \ne ID^*$, B finds $\left(ID_i, R_{ID_i}, x_{ID_i}, c\right)$ in L_4. If $c = 1$ and the list L_3 contains $\left(R_{ID_i}, y_{ID_i}\right)$, B returns $S_{ID_i} = \left(x_{ID_i} + y_{ID_i}\right)^{-1}D_{ID_i}$; if $c = 1$ and the list L_3 does not contain $\left(R_{ID_i}, y_{ID_i}\right)$, B queries $H_3\left(R_{ID_i}\right)$ and returns $S_{ID_i} = \left(x_{ID_i} + y_{ID_i}\right)^{-1}D_{ID_i}$; if $c = 0$, B gets additionally information $x_{ID_i}^{'}$ from A_I and simulates as in the above case ($c = 1$).

Public-key-Replacement Queries: When A_I makes a query on public key replacement of input $\left(ID_i, R_{ID_i}\right)$, if the list L_4 contains $\left(ID_i, R_{ID_i}, x_{ID_i}, c\right)$, B sets $R_{ID_i} = R_{ID_i}^{'}$ and $c = 0$. Otherwise, B makes a public-key-replacement query on ID_i, then sets $R_{ID_i} = R_{ID_i}^{'}$ and $c = 0$.

Blind-Ring-Sign Queries: When A_I queries a blind ring signature on message m and a group of n users whose identities from the set $L = \left\{ID_1, ..., ID_n\right\}$, B performs as following:

(a) B first finds $\left(ID_i, Q_{ID_i}, q_{ID_i}\right)$, $\left(ID_i, R_{ID_i}, x_{ID_i}, c\right)$ in the list L_1 and L_4 for all $i \in \left(1, ..., n\right)$.

(b) If $c = 1$, B chooses an index $A \in \left(1, ..., n\right)$, and finds $\left(R_{ID_i}, y_{ID_i}\right)$ for $i \in \left(1, ..., n\right)$ in the list L_3; if it does not contain R_{ID_i}, B randomly chooses $y_{ID_i} \in Z_q^*$, and adds $\left(R_{ID_i}, y_{ID_i}\right)$ to L_3. B then randomly chooses $a_i \in Z_q^*$ and computes $V_i = a_iP$, for all $i \in \left(1, ..., n\right), i \ne A$; B then randomly chooses $V_A, U^{'} \in G$, $h_A \in Z_q^*$, computes $u = e\left(P, \sum_{i \ne A} a_i\left(R_{ID_i} + y_{ID_i}Q_{ID_i}\right)\right)$,

$r^{'} = g^{-h_A} e\left(-U^{'}, P\right) e\left(V_A, R_{ID_A} + y_{ID_A} Q_{ID_A}\right)$ and set $h_A = H_2\left(m, L, r^{'}\right)$. If the list L_2 has already contained $H_2\left(m, L, r^{'}\right)$, B output FALL and aborts the simulation. Otherwise, B returns $\sigma = \left(m, u, r^{'}, U^{'}, V_1, ..., V_n\right)$ and adds $\left(m, L, r^{'}, h_A\right)$ 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 $\left(L^*, h_1, \sigma = \left(m^*, u, r^{'}, U^{'}, \cup_{i=1, i\neq A}^{n} \left\{V_i\right\}, V_A\right)\right)$ which means σ is a blind ring signature on message m^* on behalf of the group specified by identities in $L^* = \left\{ID_1^*, ..., ID_n^*\right\}$, where suppose the actual signer's identity is ID_A and $h_1 = H_2\left(m^*, L^*, r^{'}\right)$. According to the forking lemma, B then replays A_I with the same random tape but different H_2. Suppose H_2 outputs $h_1 \neq h_2$ in the first round and the second round respectively. We can get another different valid forge $\left(L^*, h_2, \sigma = \left(m^*, u, r^{'}, U^{'}, \cup_{i=1, i\neq A}^{n} \left\{V_i\right\}, V_A^{'}\right)\right)$. According to the equations as follows:

$$r^{'} g^{h_1} e\left(P, U^{'}\right) u = e\left(V_A, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \cdot \prod_{i=1, i\neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right) \qquad (1)$$

$$r^{'} g^{h_2} e\left(P, U^{'}\right) u = e\left(V_A^{'}, R_{ID_A} + y_{ID_A} Q_{ID_A}\right) \cdot \prod_{i=1, i\neq A}^{n} e\left(V_i, R_{ID_i} + y_{ID_i} Q_{ID_i}\right) \qquad (2)$$

we can get $g^{h_1 - h_2} = e\left(V_A - V_A^{'}, R_{ID_A} + y_{ID_A} Q_{ID_A}\right)$, that is $e\left(P, P\right)^{h_1 - h_2} = e\left(V_A - V_A^{'}, \left(x_{ID_A} + y_{ID_A}\right)\left(s + q_{ID_A}\right) P\right)$, then we have $e\left(\frac{1}{s + q_{ID_A}} P, P\right) = e\left(\frac{x_{ID_A} + y_{ID_A}}{h_1 - h_2}\left(V_A - V_A^{'}\right), P\right)$. So the solution of the problem k-CAA is $\frac{1}{s + q_{ID_A}} P = \frac{x_{ID_A} + y_{ID_A}}{h_1 - h_2}\left(V_A - V_A^{'}\right)$.

Theorem 4. *Our CLBRS scheme is existential unforgeable against the Type II adversary in the random oracle model assuming the mICDH 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 $g = e\left(P, P\right)$. 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

[1] Shamir A. *Identity-Based Cryptosystems and Signature schemes*. In CRYPTO 84. 1984; 196: 47-53.

[2] Al-Riyami SS and Patersony KG*. Certificateless Public Key Cryptography.* In ASIACRYPT 2003. 2003; 2894: 452-473.

[3] Huang XY, Susilo W, Mu Y, and Zhang FT. *On the Security of Certificateless Signature Schemes from Asiacrypt 2003*. In CANS 2005. 2005; 3810: 13-25.

[4] Wan ZM, Lai XJ, Weng J, Liu SL, Long Y and Hong X. Certificateless Key-Insulated Signature without Random Oracles. *Journal of Zhejing University Science A*. 2009; 10(12): 1790-1800.

[5] He DB, Chen JH and Zhang R. Efficient and Provably-Secure Certificateless Signature Scheme without Bilinear Pairings. http://eprint.iacr.org/2010/632.pdf.

[6] Zhang FT, Li SJ, Miao SQ, Mu Y, Susilo W and Huang XY. Cryptanalysis on Two Certificateless Signature Schemes. *International Journal of Computers, Communications & Control*. 2010; 5(4): 586-591.

[7] Chaum D. *Blind Signature for Untraceable Payments*. In CRYPTO 1982. 1982: 199-203.

[8] Masayuki Abe and Eiichiro Fujisaki. *How to Date Blind Signatures*. In ASIACRYPT 1996. 1996; 1163: 244-251.

[9] Wanli Su, Shichong Tan, Yanping Li and Yumin Wang. Certificateless Partially Blind Signatures. *Journal of Jilin University (Engineering and Technology Edition)*. 2009; 39(4): 1094-1098.

[10] Liu JW, Zhang ZH, Sun R and Kwak KS. *Certificateless Partially Blind Signature*. Proceedings of WAINA 2012, IEEE Press. 2012: 128-133.

[11] Rivest RL, Shamir A and Tauman Y. *How to Leak a Secret. In ASIACRYPT 2001*. 2001; 2248: 552-565.

[12] Chow SSM and Yap WS. Certificateless Ring Signatures. http://eprint.iacr.org/2007/236.pdf.

[13] Zhang L, Zhang FT, and Wu W. *A Provably Secure Ring Signature Scheme in Certificateless Cryptography*. In ProvSec 2007. 2007; 4784: 103-121.

[14] Sang YX and Zeng JW. *Two Certificateless Distributed Ring Signature Scheme*. ACTA Electronica Sinica. 2008; 36(7): 1468-1472.

[15] Chan TK, Fung K, Liu JK, and Wei VK. *Blind Spontaneous Anonymous Group Signatures for Ad Hoc Groups*. In ESAS 2004. 2005; 3313: 82-84.

[16] Wu QH, Zhang FG, Susilo W, and Mu Y. *An Efficient Static Blind Ring Signature Scheme*. In ICISC 2005. 2006; 3935: 410-423.

[17] Herranz J and Laguillaumie F. *Blind Ring Signatures Secure Under the Chosen-Target-CDH Assumption*. In ISC 2006. 2006; 4176: 117-130.