A New Type of Group Blind Signature Scheme Based on Bilinear Pairings

Jun Zhong Dake He

（School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China）

Abstract: This paper constructs a new group blind signature scheme on the basis of CZK group signature scheme. The security of the new scheme is under the computational Diffie-Hellman problem in the random oracle model. In our scheme, to blind the group signature of CZK only adds the computation of modular addition; while the scheme in LR98 adds the computation of double discreet logarithm, root of the discreet logarithm and random permutation in order to blind the group signature of CS97. As far as the computation complexity is concerned, our scheme is more efficient than LR98.

Key Words: Group Signature　Group Blind Signature　Information Security
CLC: TP309

1 Introduction

Group signature is the traditional extension of multi-signatures. Such a scheme allows a group member to sign a message on the group's behalf such that everybody can verify the signature but no one can find out which group member provided it. However, there is a trusted third party, called the group manager, who can in case of a later dispute reveal the identity of the originator of a signature. In [4] Chaum and van Heyst first proposed the concept of group signature, however, the most popular scheme is the one in [2], whose technique is the state of the art. It satisfies all the security requirements of group signature, and also, the length of group public key is a constant, which is independent of the size of group.

The concept of a Blind Signature was introduced by Chaum [6] to enable spender to be anonymous in Electronic Cash systems. Such signatures require that a signer be able to sign a document without knowing its contents. Moreover, should the signer ever see the document/signature pair, he should not be able to determine when or for whom he signed it (even though he can verify that the signature is indeed valid). In Electronic Cash systems, document is corresponding to electronic cash and signer corresponding to bank. In papers [7,8,9], Blind Signature’s conception, properties, security and applications all have been deeply investigated. As in article[8], the security of the group blind signature in is proved in the random oracle model.

Group blind signature combines the properties of group signature and blind signature. It was first introduced by Lysyanskaya and Ramzan [3]. By means of the property of group blind signature, Lysyanskaya and Ramzan constructs a new kind of Electronic Cash system, Distributed Electronic Banks. Different from the former systems, the electronic cash can be issued by several electronic banks. And this prominent advantage of the new system makes the application of electronic cash more extensive than ever before.

ID-based group signature scheme was firstly proposed by Park, Kim and Won [11]. The scheme is much inefficient: the length of the group public key and signature are proportional to the size of the group; moreover, the identity of each member must be included in the group public key, so the the anonymity of the scheme is not guaranteed. At present, the best ID-based group signature scheme is proposed in paper [1] by Chen, Zhang and Kim(we call it CZK for short). The length of group public key and signature of CZK are a constant, which are independent of the size of group.

The CZK is provable secure. The security of it is on the basis of the ID-based public key encryption system, which is constructed from Bilinear Pairings. In this paper, using CZK, we establish a new kind of group blind signature scheme, ID-based group blind signature scheme.

2 Preliminaries

This section reviews some cryptographic assumptions and introduces the building blocks necessary in the subsequent design of our group blind signature scheme.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q. Let a, b be elements of Z_q^*. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

2.2 Gap Diffie-Hellman Group

Let G_1 be a cyclic additive group generated by P, whose order is a prime q. We first introduce the following problems in G_1:

1. Discrete Logarithm Problem(DLP): Given two elements P, Q, to find an integer $n \in Z_q^*$ such that $Q = nP$;
2. Computation Diffie-Hellman Problem(CDHP): Given P, aP, bP, $a, b \in Z_q^*$ to compute abP;
3. Decision Diffie-Hellman Problem(DDHP): Given P, aP, bP, cP, $a, b, c \in Z_q^*$ to decide whether $c \equiv ab \bmod q$;

We call G_1 a Gap Diffie-Hellman Group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. Such group can be found in supersingular elliptic curve or hyperelliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see[12,13].

2.3 ID-based Public Key Setting from Bilinear Pairings

The ID-based public key systems, introduced by Shamir[14], allow some public information of the user such as name, address and email etc., rather than an arbitrary string to be used as his public key. The private key of the user is calculated by Private Key Generator (PKG) and sent to the user via a secure channel. ID-based public key setting from bilinear pairings can be implemented as follows:

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H_1: \{0,1\}^* \to Z_q, H_2: \{0,1\}^* \to G_1$.

1. Setup: PKG chooses a random number $s \in Z_q^*$, and set $P_{pub} = sP$ .The center publishes systems parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and keeps s as the master-key, which is known only himself.
2. Extract: A user submits his/her identity information ID to PKG. PKG computes the user's public key as $Q_{ID} = H_2(ID)$, and returns $S_{ID} = sH_2(ID)$ to the user as his/her private key.

2.4 CZK ID-based Group Signature Scheme

In this Section, we briefly describes the CZK ID-based group signature scheme. Let G_1 be a Gap Diffie-Hellman group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$. We define two ideal hash functions $H_1: \{0,1\}^* \times G_1 \to Z_q, H_2: \{0,1\}^* \times G_1 \to G_1$.

The group manager(GM) chooses a random number $s \in Z_q^*$, and sets $P_{pub} = sP$. GM keeps s as his master-key and publishes group public key $Y = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$. User chooses a random number $r \in Z_q^*$ as his long-term private key and sends rP to GM. GM computes $S_{ID} = sH_2(ID \| T, rP)$, where T is the life of user's long-term private key r, and sends S_{ID} to user. The user's private key pair are $\langle r, S_{ID} \rangle$,the public key is ID. It is worthy of noting that user's private key pair $\langle r, S_{ID} \rangle$ and the public key ID are used to construct CZK ID-based public key setting, on which the CZK ID-based group signature is based. For more details, please refer to paper[1]. CZK ID-based group signature scheme can be characterized into four parts:

1. Join

- The user randomly chooses $x_i \in Z_q^*$, $i = 1, 2, \cdots, k$. He then sends $rx_iP, x_iP, rP, ID, S_{ID}$ to GM.
- If $S_{ID} = sH_2(ID \| T, rP)$, $e(rx_iP, P) = e(rP, x_iP)$,GM sends the user $S_i = sH_2(T, rx_iP)$, $i = 1, 2, \cdots, k$.
- The user's member certificates are (S_i, rx_iP) ,and his private signing keys are rx_i .Here $i = 1, 2, \cdots, k$.
- GM adds rx_iP, x_iP, rP, ID to the member list.

2. Sign

- The signer randomly chooses $a \in Z_q^*$ and computes $U = aH_2(T, rx_iP)$.
- computes $V = rx_iH_2(m, U)$
- computes $h = H_1(m, U + V)$
- computes $W = (a + h)S_i$

Then (U, V, W, T, rx_iP) is the signature of the message of m .

3. Verify

If T is a valid period, the verifier computes $H_2(T, rx_iP)$, $H_2(m, U)$, $h = H_1(m, U + V)$ and tests if the following equation holds:

$$e(W, P) = e(U + hH_2(T, rx_iP), P_{pub})$$

4. Open

Given a valid group signature, GM can easily identify the signer from the following two equations:

$$e(rx_iP, P) = e(x_iP, rP)$$
$$e(S_{ID}, P) = e(H_2(ID \| T, rP), P_{pub})$$

3 ID-based Group Blind Signature Scheme

In our ID-based group blind signature scheme, we first transform noninteractive signing part of CZK ID-based group signature scheme into interactive signing, and then blind the interactive version of the signing:

User Round 0: User wants message m signed and sends a signature request to the signer.

Signer Round 1: Chooses randomly $a \in Z_q^*$, then computes and sends $U = aH_2(T, rx_iP)$ to the user;

User Round 2: User Chooses randomly $b \in Z_q^*$, after that he computes and sends $U' = U + bP$ and $H_2(m, U')$ to the signer;

Signer Round 3: Signer computes $V = rx_iH_2(m, U')$, and sends it to the user;

User Round 4: User computes $V' = V + bP$ and $h' = H_1(m, U' + V')$, then sends h' to the signer;

Signer Round 5: Signer computes $W = (a + h')S_i$, then sends it to the user;

User Round 6: User computes $W' = W + bP_{pub}$.

Thus, (U', V', W', T, rx_iP) is the ID-based group blind signature of m. Next, we show the correctness and blindness of the ID-based group blind signature with theorem 1 and 2.

Theorem 1: *ID-based group blind signature described above is correct.*

$Proof.$ Given a signature (U', V', W', T, rx_iP), the verifier first computes $h' = H_1(m, U' + V')$ and $H_2(T, rx_iP)$. And then he verifies whether the equation $e(W', P) = e(U' + h'H_2(T, rx_iP), P_{pub})$ is valid. The details is as follows:

$$
\begin{aligned}
& e(W', P) = e(W + bP_{pub}, P) \\
& = e(W, P)e(bP, P_{pub}) \\
& = e((a + h')S_i, P)e(bP, P_{pub}) \\
& = e(asH_2(T, rx_iP) + h'sH_2(T, rx_iP), P)e(bP, P_{pub}) \\
& = e(U + h'H_2(T, rx_iP) + bP, P_{pub}) \\
& = e(U' + h'H_2(T, rx_iP), P_{pub})
\end{aligned}
$$

Thus we prove it.

Theorem 2: *CZK ID-based group signature is correctly blinded.*

$Proof.$ From User round 2, we know that the user utilizes random number b to blind U coming from signer and transform it into U'. At the same time, the user blinds message m with the help of hash function H_2. Thus, in Signer round 3, the signer makes a signature to message m and U without knowing them. From User round 4, random number b blinds V and changes it to be V'. So, in Signer round 5, the signer uses his certificate S_i to make a signature

without knowing its content. At last, in User round 6, the user utilizes random number b to blind the W coming from the signer.

4 Security Analysis

This section gives a security analysis to the ID-based group signature scheme. The details is as follows:

Lemma3[1]: *ID-based group blind signature scheme is secure against an existential adaptively chosen message attack under the assumption of CDHP(computational Diffie-Hellman problem) in the random oracle model.*

Lemma4: *If there exists an adversary A_0 can forge a member certificate with time t and a non-negligible probability ε, then we can solve CDHP in G_1 with time t and a non-negligible probability ε.*

Proof. Consider the following game: the adversary A_0 may query H_2 adaptively at most k times. Suppose the i th input of query is (T, rx_iP) and he gets the corresponding certificate S_i. Finally, he outputs a new pair (rxP, S). A_0 wins the game if rxP is not queried and $e(S,P) = e(H_2(T, rxP), P_{pub})$ is valid.

Assume there is an adversary A_0 can forge a member certificate with time t and a non-negligible probability ε, we can construct another adversary A_1 as follows:

- A_1 randomly chooses integer $u \in \{1, 2, \cdots, k\}$, and defines $Cer(H_2(T, rx_iP)) = S_i$;
- For $i = 1, \cdots, k$, let A_1 replace A_0 answering the queries of H_2 and Cer. When $i = u$, A_1 replaces x_u as x;
- A_0 outputs $(rx_{out}P, S_{out})$;
- If $x_{out} = x$ and S_{out} is a valid certificate, A_1 outputs (rxP, S).

Since the integer u is randomly selected, as for A_0, the query result given by A_1 is indistinguishable from the one given by challenger in the real environment. At the same time, due to the randomness of H_2, if the certificate S_{out} output by A_0 is valid, then $H_2(T, rxP)$ must be queried.

Let $H_2(T, rxP) = aP$, $P_{pub} = bP$, since $e(S,P) = e(H_2(T, rxP), P_{pub})$, we have solved

the CDHP in group G_1.

Lemma5: *The interactive protocol underlying the ID-based group blind signature scheme is an honest-verifier zero-knowledge proof of knowledge of a member certificate and corresponding identity.*

Proof. The process of proof utilize the techniques of paper[2], we restrict our attention on the proof of knowledge part. We show that the knowledge extractor can recover the member certificate once it has found two accepting tuples.

Let (U',V',W',T,rx_iP) and (U',V'',W'',T,rx_iP) be two accepting tuples. Define $h' = H_1(m,U'+V')$. Because $e(W',P) = e(U'+h'H_2(T,rx_iP),P_{pub})$, thus we can get equation

$$W' = s(U'+h'H_2(T,rx_iP)) \qquad (1)$$

Let $h'' = H_1(m,U'+V'')$, likewise , we can obtain $e(W'',P) = e(U'+h''H_2(T,rx_iP),P_{pub})$

Thus, we get

$$W'' = s(U'+h''H_2(T,rx_iP)) \qquad (2)$$

From equations (1) and (2), we obtain $W'-W'' = sh'H_2(T,rx_iP) - sh''H_2(T,rx_iP)$, and then we get the result $S_i = sH_2(T,rx_iP) = (h'-h'')^{-1}(W'-W'')$. Thus, we have recovered the member certificate.

Theorem6: *The ID-based group blind signature scheme is provably secure under the assumption of CDHP in the random oracle model.*

Proof. Our scheme satisfies all the properties of group blind signature scheme:

- Correctness: Theorem1;
- Blindness: Theorem2;
- Unforgeability: Lemma4;
- Anonymity: Since x_i is randomly chosen, rx_iP reveals no information about the signer's identity to anyone except GM;
- Unlinkability: Given rx_iP and rx_jP, without knowing x_iP, x_jP, it is hard to compute rP;
- Traceablity: GM can open any valid group blind signature because he is able to provide a zero-knowledge proof that the signer indeed produces the signature;
- Exculpability: From lemma3, we know that whether GM or group member cannot sign a message on behalf of other group members;
- Coalition-resistance: From lemma4 and lemma5, we know that a colluding subset of group members cannot produce a valid signature that the group manager cannot open.

5 Efficiency Analysis

The size of the group public key and the group blind signature is independent on the numbers of group members. The algorithms and protocols of the group blind signatures are efficient. In our scheme, to blind the group signature of CZK only adds the computation of modular addition; while the scheme in LR98 adds the computation of double discreet logarithm, root of the discreet logarithm and random permutation in order to blind the group signature of CS97. As far as the computation complexity is concerned, our scheme is more efficient than LR98.

6 Conclusion

In this paper, we construct a provably secure ID-based group blind signature on the basis of CZK scheme. The size of the group public key and the group blind signature is independent on the numbers of group members. Compared with LR98 scheme, our scheme is more efficient. The drawback of our scheme is that for different message m , signer will need a new private key pair to make a signature.

References

[1]X. Chen, F. Zhang and K. Kim. A new ID-based group signature scheme from bilinear pairings. http://eprint.iacr.org/2003/116. 2003.

[2] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In: Advances in Cryptology- CRYPTO 2000. LNCS 1880, Heidelberg: Springer-Verlag, 2000. 255～270.

[3] A. Lysyanskaya, Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In: Proc of the Int'l Conf on Financial Cryptography. New York: Springer-Verlag, 1998, 184～197

[4] D. Chaum, E. v. Heyst. Group signatures. In: Proc of EUROCRYPT 91. New York: Springer-Verlag, 1991. 257～265

[5] J. Camenisch, M. Stadler. Efficient group signature for large groups. In: Proc of CRYPTO 97. New York: Springer-Verlag, 1997. 410～ 424.

[6] D. Chaum. Blind signatures for untraceable payments. In R. L. Rivest, A. Sherman, and D. Chaum, editors, Proc. CRYPTO 82, pages 199～203, New York, 1983. Plenum Press.

[7] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, Proc CRYPTO 88, pages 319-327. Springer-Verlag, 1988. Lecture Notes in Computer Science No. 403.

[8] D. Pointcheval and J. Stern. Provably secure blind signature schemes. In M. Y. Rhee and K. Kim, editor, Advances in Cryptology-ASIACRYPT'96, pages 252-265. Springer-Verlag, 1996. Lecture Notes in Computer Science No. 1163.

[9] A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In Proc CRYPTO 97, pages 150-164. Springer-Verlag, 1997. Lecture Notes in Computer Science No. 1294.

[10] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In First ACM Conference on Computer and Communications Security, pages 62-73, Fairfax, 1993. ACM.

[11]S.Park, S.Kim and D.Won. ID-based group signature. Electronics Letters. 33(19), pp.1616-1617, 1997.

[12]D. Boneh and M. Franklin. Identity-based encryption from the Weil pairings. Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[13]F. Hess. Efficient identity based signature schemes based on pairings. Proc.9th Workshop on Selected Areas in Cryptography–SAC 2002,LNCS 2595,Springer-Verlag, pp.310-324, 2002.

[14]A. Shamir. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.