An Efficient and Secure ID Based Group Signature Scheme from Bilinear Pairings

Pankaj Sarde
Dept. of Mathematics, Rungta College of Engineering and Technology, Raipur, CG, India
Email: pnsarde@gmail.com
Amitabh Banerjee
Dept. of Mathematics, Govt. D. B. Girls PG College, Raipur, CG, India
Email: amitabh_61@yahoo.com

ABSTRACT

We propose an efficient and secure identity based group signature scheme from bilinear pairings. Group signature allows group member to sign arbitrary number of messages on behalf of the group without revealing their identity. Under certain circumstances the group manger holding a tracing key can reveal the identities of the signer from the signature. Our scheme is based on the Computation Diffie-Hellman Problem (CDHP) assumption and bilinear pairings. In the scheme, the size of the group public key and length of the signature are independent on the numbers of the group members

Keywords: **Group Signature, Bilinear Pairings, ID based Cryptography**

Date of Submission: January 30, 2015 Date of Acceptance: May 01, 2015

1. Introduction:

Group signature introduced by Chaum and E. Van Heyst [1], allows any member of a group to sign messages on behalf of the group. Anyone can verify the signature with a group public key while no one can know the identity of signer except the group manager. Further it is computationally hard to decide whether two different signatures were issued by the same member. Plenty of the group signature schemes [2, 3, 4, 5, 6] have been presented after the Chaum and Van Heyst's initial works. However, most of them are much inefficient for large groups because the group public key and length of the signature depend on the size of the group. In 1997 J. Camenisch and M. Stadler [7] proposed the first efficient group signature scheme for which the group public key and group signature are both of constant size. Atenese et al. [8] proposed a practical and provably coalition-resistant secure group signature scheme. Recently, M. Bellare, D.Micciancio and B. Warinschi [9] provides theoretical foundations for the group signature primitive. The concept of ID based cryptography was introduced by Shamir [10] to simplify key managements procedure of certified based public key infrastructure. An identity based crypto-system [10, 11] is a system that allows a publicly known identifier (email address, IP address, name) to be used as the public key component of a public/private key pair in a crypto-system. An ID-based group signature scheme is firstly proposed by S. Park, S. Kim and D. Won [12]. However, it is inefficient the size of the group public key and length of a group signature depend on the size of the group. Another ID based group signature scheme is proposed by Tseng and Jan [13], unfortunately it is universally forgeable. X Chen et al [14] proposed a new ID based group signature scheme from bilinear pairings. The scheme presented an approach to solve the key escrow problem. Several ID based signature schemes have been proposed in the last years [15, 16, 17]. Some of the schemes use Elliptic curve algorithms and are therefore particularly efficient.

The rest of the paper is organized as follows. Basic definition and properties is presented in section 2. Some preliminary works in section 3. Our new ID based group signature scheme from bilinear pairings is given in section 4. The security and efficiency analysis of our scheme are given in section 5. Finally concluding remarks will be made in section 6.

2. Group Signatures

In this section we introduce the definition and security properties of group signatures [14].

Definition 2.1 A group signature scheme is a digital signature scheme consisted of the following four procedures:

- **Setup:** On input a security k, the probabilistic algorithm outputs the initial group public key Y and the secret key s of the group manager.
- **Join:** A protocol between the group manager and a user that result in the user becoming a new group member. The user's output is a membership certificate and a membership secret.
- **Sign:** A probabilistic algorithm that an input a group public key, a membership certificate, a membership secret and a message m. Output is the group signature of m.
- **Verify:** An algorithm takes as input the group public key Y, the signature, the message m to output 1 or 0.
- **Open:** The deterministic algorithm takes as input the messages m, the signature, the group manager's secret key s to return " Identity or failure"

A secure group signature must satisfy the following properties:

- **Correctness:** Signature produced by a group member using **Sign** must be accepted by **Verify.**
- **Unforgeability:** Only the group members can sign messages on behalf of the group.
- **Anonymity:** Given a valid signature, it is computationally hard to identify the signer for any-one except the group manager.
- **Unlinkability:** Deciding whether two different valid signatures were computed by the same group member is computationally hard for any-one except the group manager.
- **Traceability:** The group manager is always able to open a valid signature & identify the signer.
- **Exculpability:** Neither the group manager nor a group member can sign messages on behalf of other group members. Also, the group manager or colludes with some group members can misattribute a valid group signature to frame a certain members.
- **Coalition-resistance:** A colluding subset of group members (even if comprised of the whole group) cannot produce a valid signature that the group manager cannot open.
- **Efficiency:** The efficiency of group signature is based on the parameters: the size of the group public key, the length of the group signature and the efficiency of the algorithms and protocols of the group signatures

3. Preliminary Works:

In this section, we will briefly describe the basic definition and properties of bilinear pairing and Gap Diffie-Hellman Group. We also presented ID-based public key setting from pairing.

3.1 Bilinear Pairings:

Let G_1 be a cyclic additive group generated by P, whose order is prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a, b be elements of $Z^*{}_q$. We assume that the DLP in both G_1 and G_2 are hard. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:

I. **Bilinear:** $e(aP,bQ)=(P,Q)^{ab}$

II. **Non-degenerate:** There exist $P,Q \in G_1$ such that $e(P,Q) \neq 1$

III. **Computable:** There is an efficient algorithm to compute e(P, Q) for all $P,\, Q \in G_1$

3.2 Gap Diffie-Hellman Group

Let G_1 be a cyclic additive group generated by P whose order is prime q, assume that the inversion and multiplication in G_1 can be computed efficiently. We first introduce the following problem in G_1

- **Discrete Logarithm Problem(DLP):** Given two elements P and Q, to find an integer $n \in Z^*{}_q$ such that Q=nP

whenever such an integer exist.

- **Computation Diffie-Hellman Problem(CDHP):** Given P, aP, bP for $a,b,\, c \in Z^*{}_q$ to compute abP.
- **Decision Diffie Hellman Problem (DDHP):** Given P, aP, bP, cP for $a,\, b,\, c \in Z^*{}_q$ to decide whether $c \equiv ab \bmod q$.

We call G1 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 pairing can be derived from the Weil or Tate pairings.

4. Proposed ID based group signature scheme from bilinear pairings

We propose an ID-based group signature scheme from bilinear pairing. We only need to consider that Key generation centre (KGC) is the group manager. We can't adopt the usual ID-based system. Since key escrow is fatal drawback for traditional ID-based system. So it assumed that that KGC must be trusted unconditionally. Otherwise, the system will be collapsed. If KGC act as the group manager of a group, he can forge the signature of any users. Therefore, the most important thing to design an ID-based group signature scheme is to solve the problem of key-escrow.

Proposed scheme consists of six procedures: **Set-up, Extract, Join, Sign, Verify**, and **Open.** In our scheme, KGC is assumed no longer to be a trusted party.

Let G_1 be a Gap DH cyclic additive group generated by P, whose order is prime order q and G_2 be a cyclic multiplicative group of same order q. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$. Define Cryptographic hash function $H_1: \{0,1\}^* \times G_1 \rightarrow G_1$, $H_2: \{0,1\}^* \rightarrow Z^*{}_q$ and $H_3: G_1 \rightarrow Z^*{}_q$

- **Setup:** KGC chooses a generator P of G_1 and picks a random number $s \in Z^*{}_q$ and set $P_{pub} = sP$. Thus system Parameters are $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$ and keep s as the master secret key, which is known only him-self.
- **Extract:** A user U_i submit his (or her) identity information ID_i and rP to KGC, where $r \in Z^*{}_q$ long-term private key. Then KGC computes the user's public key $Q_{IDi} = H_1(ID_i \| T,\, rP)$. Here T is life Span of r and sends $S_{IDi} = sQ_{IDi}$ to the user via a secure channel. Thus user's private key pair is (r, S_{IDi}). The user should update his key pair after period of T. We call S_{IDi}, rP pseudo

secret, since KGC is no longer trustful , it may expose them to other members.

- **Join:** Suppose that a user U$_i$ wants to join the group. For this, he and KGC perform Join protocol as follows:
  1. The user U$_i$ chooses a random number $x_i \in Z^*{}_q$, then sends $\{rx_i,\ \ rP,\ ID_i,\ x_i P\}$to KGC
  2. If KGC is convinced that the user know $S_{IDi} = sH_1(ID_i \parallel T, rP)$ and $e(rx_iP,\ P)=e(x_i,\ rP)$, KGC sends secretly $s_i = sH_1(ID_i,\ rx_iP)$ to the user U$_i$

Thus user's member certificates are $(s_i,\ rx_iP)$ and his private signing key is rx_i. KGC adds $(rx_iP,\ x_iP,\ rP,\ ID_i)$ to the member list.

- **Sign:** To sign a message m, the user U$_i$ randomly chooses number $\alpha,\ \beta,\ k \in Z^*{}_q$ and uses her signing key and corresponding member certificate and then computes the following values:

$$R = kP \qquad ....(1)$$

$$S_1 = rx_i Q_{IDi} \qquad ....(2)$$

$$S_2 = rx_i\alpha H_1(ID_i,\ rx_iP) + H_3(R)P \ ....(3)$$

$$S_3 = rx_i\beta H_1(ID_i,\ rx_iP) + H_2(m)P \ ....(4)$$

$$S_4 = [H_2(m)\alpha + \beta H_3(R)]s_i \qquad ....(5)$$

Thus ID-based group signature on the message m is $(R,\ S_1,\ S_2,\ S_3,\ S_4,\ rx_iP)$

- **Verify:** To verify a group signature $(R,\ S_1,\ S_2,\ S_3,\ S_4,\ rx_iP)$ on the message m. Verifier accept the signature if following equation holds

$$e(S_4,\ \ rx_iP) = e(S_2,\ P_{pub})^{H_2(m)} \times e(S_3,\ P_{pub})^{H_3(R)} \quad ....(6)$$

$$e(S_1,\ P) = e(Q_{IDi},\ \ rx_iP) \quad ....(7)$$

If it is true then $[R,\ S_1,\ S_2,\ S_3,\ S_4,\ rx_iP]$ is valid ID based group signature on the message m

- **Open:** In case of dispute, the KGC can easily identify the user. The signer can't deny the signature after KGC present a proof. KGC check the following equation:

$$e(S_{IDi},\ \ P) = e(H_1(ID_i \parallel T,\ rP),\ \ P_{pub})$$

$$e(s_i,\ P) = e(H_1(ID_i,\ rx_iP),\ \ P_{pub})$$

$$e(S_1,\ \ P_{pub}) = e(S_{IDi},\ \ rx_iP)$$

$$e(S_2,\ S_{IDi})^{H_2(m)} e(S_3,\ S_{IDi})^{H_3(R)} = e(S_4,\ S_1) \quad ....(8)$$

5. Analysis of Our Scheme

In this section, we prove that security of our group signature scheme on the assumption that G$_1$ is gap DH group.

Theorem 5.1. If there is an adversary A$_1$ (without colluding with KGC) can forge a member certificate with time t and a non-negligible probability ε, then we can solve CDHP in G$_1$ at most with time t and a non-negligible probability ε

Proof: The adversary A$_1$ forge a valid pseudo-secret key and member certificate with non-negligible probability ε, through the following process. First adversary A$_1$ queries the random oracle H$_1$(:) at most t times. Then he outputs a tuple $(ID_i,\ rP,\ rx_iP,\ S_{IDi},\ s_i)$ in which (ID, rP, rxP) were not queried. If the tuple is valid, it must satisfy the open function.

$$e(S_{IDi},\ P) = e(H_1(ID_i \parallel T,\ rP),\ \ P_{pub})$$

$$(s_i,\ P) = e(H_1(ID_i,\ rx_iP),\ \ P_{pub})$$

Let $H_1(ID \parallel rP)$ OR $H_1(ID \parallel rxP) = aP$, $P_{pub} = bP$. Then adversary can solve CDHP in G$_1$ for S$_{ID}$=abP with negligible probability ε.

Theorem 5.2. Proposed ID-based group signature from bilinear pairings is secure under the assumption of CDHP is hard in the oracle.

Proof: A secure group signature scheme should satisfy several security properties, we examine the security of our scheme according to the requirements.

Correctness: To prove (6)

$$\begin{aligned}
& e(S_2,\ P_{pub})^{H_2(m)} e(S_3,\ P_{pub})^{H_3(R)} \\
&= e(rx_i\alpha H_1(ID_i,\ rx_iP)H_2(m) + H_2(m)H_3(R)P, P_{pub}) \\
&\quad \times e(rx_i\beta H_1(ID_i,\ rx_iP)H_3(R) - H_2(m)H_3(R)P, P_{pub}) \\
&= e(rx_i\alpha H_1(ID_i,\ rx_iP)H_2(m) + rx_i\beta H_1(ID_i,\ rx_iP)H_3(R) \\
&\qquad ,\ P_{pub}) \\
&= e(\alpha H_2(m)s_i + \beta H_3(R)s_i,\ rx_iP) \\
&= e(S_4,\ rx_iP)
\end{aligned}$$

and

$$e(s_i,\ P) = e(rx_iQ_{IDi},\ P) = e(Q_{IDi},\ rx_iP)$$

To prove (8)

$$
\begin{aligned}
& e(S_2, S_{IDi})^{H_2(m)} e(S_3, S_{IDi})^{H_3(R)} \\
& = e(rx_i \alpha H_1(ID_i, rx_i P) H_2(m) + H_2(m) H_3(R) P, S_{IDi}) \\
& \times e(rx_i \beta H_1(ID_i, rx_i P) H_3(R) - H_2(m) H_3(R) P, S_{IDi}) \\
& = e(\alpha H_1(ID_i, rx_i P) H_2(m) + \beta H_1(ID_i, rx_i P) H_3(R) \\
& \quad , \ rx_i S_{IDi}) \\
& = e(\alpha H_2(m) s_i + \beta H_3(R) s_i, \ rx_i Q_{IDi}) \\
& = e(S_4, S_1)
\end{aligned}
$$

- **Unforgeability:** In our scheme, only group members can sign messages on behalf of the group. Since membership certificate for user U_i is (S_i, rx_iP) which are made by KGC.
- **Anonymity:** In our scheme, only KGC is able to open the signature and to recover who signed it. Since x_i is randomly chosen and rx_iP reveals no identity information of user to anyone except KGC.
- **Unlinkability:** Given rx_iP and rx_jP. It is computationally hard to decide that they are correspondence to same rP without knowing the x_iP and x_jP
- **Exculpability:** In our scheme, a group member can't sign on behalf of other members because it does not know the other members private keys. The KGC knows each user's private key s_i but he doesn't know user's private key rx_i. Since one period T corresponds only one unique rP
- **Coalition-resistance:**Membership certificate of each group member is unique which is generated by KGC. Thus colluding subset of group members cannot produce a valid signature that the group manager cannot open

6. Conclusion

In this paper we describe an efficient and secure ID based group signature scheme from bilinear pairing. In this signature scheme the group public key and parameters are constant don't depend on the group members. Thus generated group signature can handle large groups and the security of such a group sig-nature scheme is strong as compare to other ID based group signature scheme.

References

[1] D. Chaum and E. Van Heyst, Group Signatures, Advances in Cryptology-Eurocrypt-1991, LNCS 547, PP. 257 - 265, Springer-Verlag, 1991

[2] G. Ateniese, G. Tsudik, Some open issues and new direction in group signatures, Financial Cryptography 1999, LNCS 1648, PP. 196-211, Springer-Verlag, 1999

[3] J. Camenisch, Efficient and generlized group signatures, Advances in Cryptology-Eurocrypt 1997, LNCS 1233, PP. 465 - 479, Springer-Verlag, 1997

[4] L. Chen and T. Pedersen, New group signatures schemes, Advances in cryptology-Eurocrypt 1994 , LNCS 950, PP. 171-181, Springer-Verlag, 1994

[5] L. Chen, T. Pedersen, On the efficiency of group signatures providing information-theoretic anonymity. In Advances in Cryptology-CRYPTO'91, Springer-Verlag, 1991, pp.196-198.

[6] H. Petersen, How to convert any digital signature scheme into group signature scheme. In security protocols workshop 1997, PP. 177 -190, Springer-Verlag, 1997.

[7] J. Camenisch and M. Stadler, Efficient group signature schemes for large groups. Advances in Cryptology-Eurocrypt'97, LNCS 1294, Springer-Verlag, 1997, PP. 410 - 424.

[8] G. Ateniese, J. Camenisch, M. Joye, G. T-sudik. A practical and provably secure coalition-resistant group signature scheme. Advances in Cryptology-Crypto'2000, LNCS 1880, Springer-Verlag, 2000, PP. 255 – 270

[9] M. Bellare, D. Micciancio, B. Warinschi, Foundation of group signatures: formal definition, simplified requirements and a construction based on general assumption. Advances in Cryptology-Eurocrypt'2003, LNCS 2656, Springer-Verlag, 2003, 614-629

[10] A.Shamir. Identity based cryptosystems and signature schemes, Proceedings of CRYPTO'84, LNCS 196, Springer-Verlag, 1985, PP. 47 -53.

[11] D. Boneh and M. Frauklin, Identity based Encryption from Weil pairing, Advances in cryptology-CRYPTO'2001, Springer-Verlag, LNCS, Vol. 2139, PP. 213 - 229, 2001.

[12] S. Park, S. Kim and D. Won, ID-based group signature, Electronics Letters, 33(19), 1997, PP. 1613 – 1617.

[13] Y. Tseng and J. Jan, A novel ID based group signature, International computer symposium, workshop on cryptology and information security, 1998, PP. 159 -164.

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

[15] K. Paterson, Id-based signatures from pairings on elliptic curves, Tech. Rep., IACR Cryptology e print Archieve: Report 2002/004, http://eprint.iacr/2002/004/, 2002.

[16] C. Popescu, Group signature schemes based on the difficulty of computations of approximate eth roots, Proceedings of protocols for multimedia systems (PROMS 2000), Polond, PP.325- 331, 2000.

[17] R.Sakai,K.Ohgishi, and M. kasahara, Cryptosystems based on pairing, Proceedings of symposium on cryptography and information security, Japan, Okinawa, PP. 26 - 28, 2000.