RESEARCH ARTICLE OPEN ACCESS

A New Group Signature Scheme using IBE

Girish[1] , Dr.Phaneendra H.D.[2]

[1]Department of Master of computer application, National Institute of Engineering, Mysore, Karnataka – 570008
[2]Department of Computer Science and Engineering, National Institute of Engineering, Mysore, Karnataka – 570008

---------- ********** ----------

Abstract:

Group signature is a method which allows any genuine group member to sign many number of messages on behalf of the group without giving his identity. Whenever dispute arises, the manager of the group can reveal the identity of the signer. If quantum computer comes in to picture group signatures which are based on the traditional cryptography can be broken easily. In this paper, we propose a new identity based group signature. Our signature scheme is based on bilinear maps. This identity based scheme has the security properties of group signatures. In this scheme the size of the group pubic key and the length of signatures are independent on the size of the group. This scheme can be used for very large groups. Same key pair can be used by the group member to sign many messages.

Keywords — **Group Signature, Digital Signature, Identity based Group signature, Bilinear Map.**

---------- ********** ----------

Digital signatures have been used extensively to offer different type of security services such as data integrity, entity authentication, non-repudiation, and data origin authentication. An anonymous digital signature is a special type of digital signature scheme, in which any unauthorized person even the verifier, cannot find out the signer's identity. A group members can do sign on behalf of the group using the Group signature. 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 cannot misattribute a valid group signature to frame a certain member, i.e., the member should responsible for a valid signature that he did not produce. Using a single group public key, the signatures can be verified. It is not possible to trace weather the two signatures originated from the same member or the different member of the group. In the case of dispute the authorized group manager can disclose the identity of the member of the group who has made the signature by opening the signature, Group signatures can be publicly verifiable and can also verified with respect to a single group public key. Group signatures can be used in many areas of applications in privacy protection [1,2,3]. In the electronic transaction environment the personal privacy is a big challenge, like the right of the individual is much less or the right to find out the amount of personal information which should be available to others is more. Privacy is important for many reasons, such as impersonation and fraud. It becomes easier for criminals to commit fraud as more identity information is collected, correlated, and sold. But privacy is more than that, it also concerns about the secrecy of which websites we visited, the candidates we voted for, etc. Anonymity is one important form of privacy protection. For some application high level of anonymity can do more damage. For example, in some situation one

would like to have a trusted third party to have the capability to trace users after the fact that users have misbehaved, such as tracing double-spenders in an electronic cash system. Designing secure cryptographic schemes with unconditional anonymity is undoubtedly challenging. Most of the group signatures are based on traditional cryptography, such as RSA and discrete logarithm [2]. But it is proved that finding discrete logarithms and factoring integers can be accomplished in polynomial time on a quantum computer. When the quantum computers arrive, the traditional public key cryptosystems based on these problem, such as RSA and ECC [4], may be broken. Many group signature schemes have been proposed but all of them are not very efficient. Designing an highly efficient group signature scheme is still an open

research problem in cryptography. We show an efficient group signature can be produced using the identity based encryption.. This makes our proposal very attractive since this is probably most efficient group signature scheme.

Applications of Group Signature

A group signature scheme let a signer to produce a signature on behalf of a group of signers. Everyone in the group can be sure that the signature is produced by one of the group members, but no one can let know who the real signer is except the group manager. Because of this features, group signature attracts many researchers' attentions. The group signature can be used in many applications in practice Here are a few examples of such applications:

Membership Authentication: For different social networking sites a user is required to confirm that user is a valid member, but does not have to show user identity.

Vehicle to Vehicle communications: In the Vehicular Adhoc Network, to participate in the network, it is essential for a driver is to prove that his vehicle is properly registered, but is not required to show with which registration authority.

Electronic Voting: In the electronic voting system, the voters can vote only one time. If there is a vote by more than once by a person, the tallying authority must be able to distinguish the duplicate votes without opening the ballots. Moreover, there usually exists supervision authority to limit the privileges of the tallying authority and guarantee the justice of the voting in a voting system.

Exchange of Messages: When two companies, say *A* and *B*, work on a sensitive contract, neither *A* nor *B* wants the other company to be able to tell a third party that *A* or *B* has signed the contract before both the companies exchange their signatures to each other, and neither of them wants to reveal which individual employee signs the contract on behalf of the company.

2 Group Signature

In this section we introduce the definition and security properties of group sig-natures.

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 results 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 on input a group public key, a membership certificate, a membership secret and a message m. Outputs is the group signature Sig of m.

Verify: An algorithm takes as input the group public key mathcal Y , the signature Sig, the message m to output 1 or 0.

Open: The deterministic algorithm takes as input the message m, the signa-ture Sig, the group manager's secret key S to return "Identity" or "failure".

A secure group signature must satisfy the following properties:

Correctness : Signatures produced by a group member using Sign must be accepted by Verify.

Unforgability : 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 anyone except the group manager.

Unlinkability : Deciding whether two different valid signatures were computed by the same group member is computationally hard for anyone except the group manager.

Traceability: The group manager is always able to open a valid signature and 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 not

misattribute a valid group signature to frame a certain member, i.e., the member should responsible for a valid signature that he did not produce.

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.

Effciency : The effciency of group signature is based on the parameters such as the size of the group public key, the length of the group signatures and the effciency of the algorithms and protocols of the group signatures.

Related work

Group signature, introduced by Chaum and van Heijst [15], allows any member of a group to sign on behalf of the group. Anyone can verify the signature with a group public key while no one can know the identity of the signer except the Group Manager. Further, it is computational hard to decide whether two different signatures were issued by the same member. Plenty of group signature schemes [16, 12, 16, 17, 26] have been presented after the Chaum and van Heijst's initial works. However, most of them are much inefficient for large groups because the group public key and the length of the signature depend on the size of the group. Also, new member addition and revocation require re-issuing all members' keys and changing the the group public key. Camenisch [13] presented the first efficient group signature schemes for large groups in which the group public key and the length of signature are both of constant size. Ateniese et al [5] proposed a practical and provably coalition-resistant secure group signature scheme. ID-based group signature scheme is firstly proposed by Park, Kim and Won [25]. The scheme is much inefficient: the length of the group public key and signature are proportional to the size of the group; more precisely, the identity of each member must be included in the group public key. Furthermore, Mao and Lim [24] showed that the anonymity of the scheme was not guaranteed. Tseng and Jan [31] presented a novel ID-based group scheme. However, it is universally forgeable [21] and not coalition-resistant [20]. Recently, the bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, have initiated some completely new fields in cryptography, making it possible to realize cryptographic primitives that were previously un-known or impractical [10, 11]. More precisely, they are important tools for construction of ID-based cryptographic schemes [8, 10, 19, 28, 32]. However, It is still an open problem to design an ID-based group signature scheme from bilinear pairings. The reasons are as follows: Firstly, the problem of key escrow is a fatal

disadvantage for ID-based systems, i.e., the trusted third party, called KGC, knows the private key of each member. Therefore dishonest KGC can forge the signature of any member. Secondly, the public key ID of a user should not re- veal his/her real identity information otherwise anonymity of the group signature scheme is not guaranteed. However, if we use an arbitrary string as the public key [7], an inherent problem is that KGC can misattribute a valid group signature to frame an honest member. Similarly, a member can deny his signature because KGC can also generate a public key and computes the corresponding private key. No one knows who indeed generates the certain public key because it does not reveal any information of the identity. For example, given a public key "h80fef6je59", who can provide a proof that the public key is generated by KGC or the members? So, It seems that the traditional ID-based systems from bilinear pairings are unsuitable for designing ID-based group signature. In this paper we firstly propose new ID-based systems from pairings to solve the key-escrow problem. Contrasting with previous schemes, we never assume that KGC is a trustful party or distribute the trust onto multiply KGCs. In our systems, if the dishonest KGC impersonation an honest user to sign a document, the user can provide a proof that the KGC is dishonest, which is similar to CA- based systems. We then propose a group signature scheme from bilinear pairings under the new ID-based system . The rest of the paper is organized as follows: The formal model of a secure group signature scheme is presented in Section 2. Some preliminary works are given in Section 3. Our new ID-based systems from bilinear pairings are given in Section 4. In Section 5, we propose a new ID-based group signature scheme under the new systems. The security and efficiency analysis of our scheme are given in section 6. Finally, concluding remarks will be made in Section

Bilinear Pairings

Let G_1 be a cyclic additive group generated by P , whose order is a 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 discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairings is a map e : $G_1 \times G_1 \rightarrow G_2$ with the following properties:

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

Gap Diffe-Hellman Group

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

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 exists.
2. Computation Diffe-Hellman Problem (CDHP): Given P, aP, bP for a, b $\in Z_q^*$, to compute abP.
3. Decision Diffe-Hellman Problem (DDHP): Given P, aP, bP, cP for a, b, c $\in Z_q^*$, to decide whether c ≡ ab mod q.

We call G_1 a Gap Diffe-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 super singular elliptic curve or hyper elliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [6, 10, 15].

3.3 ID-based Setting from Bilinear Pairings

The ID-based public key systems, introduced by Shamir [23], allow some public information of the user such as name, address and email etc., rather than an arbitrary string to be used his public key. The private key of the user is calculated by KGC 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, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairings is a map e : $G_1 \times G_1 \rightarrow G_2$. Define two cryptographic hash functions H_1 : $\{0, 1\}^* \rightarrow Z_q$ and $H_2 : \{0, 1\}^* \rightarrow G_1$.

Setup: KGC 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 keep s as the masterkey, which is known only himself.

Selects two groups G1 and G2 of order q, a bilinear
map e from G1×G1→ G2

- Selects generator P from G1
- picks a master secret key ms where s ∈ Z*q
- selects two Cryptographic hash functions H1 and H2
- selects H1 : {0,1}* ∈ G1*
- selects H2 : G2 ∈ {0,1}n
- calculates Ppub =s • P. The operator • is multiplication of integers with points on elliptic curve.
- publishes the system parameter {G1, G2, e, q, P, Ppub , H1, H2} to all the users and keeps the key s secret. In this step calculating s•P is easy, but for a given P finding the value of ms is practically impossible.

Extract

If a Group member wants to generate secrect member key uses a interactive session with the KCG. The communication between the group manager and member is secure.

- The user with identity information ID picks a random number r ∈ Z*qas her private key,

- computes rP,
- Sends rP together with ID to KGC.
- KGC computes D_{ID} = sH2(ID||rP)
- sends it to the user as the user's private key associated to ID via a secure channel.
- Thus the user has a private key pair (r , S_{ID}).
- S_{ID} and rP pseudo-secret, since KGC is no longer trustful and it may expose them to other members.
- the user has an associated public key Q_{ID} = H2(ID||rP).

3. Join

A user wants to join the group performs the following procedure and becomes the member

- chooses a random ∈ Z*q
- sends (rxP, rP, ID, xP) to KGC and proves to KCG that he knows S_{ID}
- If KGC is convinced that the user knows S_{ID} and e(rxP, P) =e(xP, rP),
- KGC sends secretly S = sH2(ID||rxP).
- User has secret keys x and rx, and member key xP, and the member certificates (rxP; S). The member key and the member certificates are pseudo-secret.

4. Sign

To sign a message m,

- user chooses a random k ∈ Z*q and uses her two secret keys andcertificates to compute the following values:
- U = k1rxP, k1∈
- W = (q -k1)xP;
- R = k2H2(ID||U +W + R), k2 ∈ $_R$Z*q
- h = H1(m||U +W);
- V = hk2S + k1rxH2(m||U +W + R).
- The resulting signature on the message m is (U,W,R,V).

5. Verify

- To verify a group signature (U,W,R,V) of the message m, the receiver of the signature first computes
- h = H1(m||U +W)

checks whether

- e(V,P) = e(R,Ppub)^h .e(H2(m||U +W + R),U). (1)

6. Open

- Given a valid group signature, KGC can easily identify the user. The signer cannot deny the signature after KGC presents a zero knowledge proof:
- e(U,P) . e(W,rP) = e(rxP, P)
- e(S, P) = e(H2(ID||rxP), Ppub).
- e(SID, P) = e(H2(ID||rP), Ppub).

4. **Cryptanalysis**

In this section, we prove the security of our group signature scheme on the assumptionthat G1 is a Gap DH group.

Theorem 1

If there is an adversary A (without colluding with KGC) who can forge a valid tuple (ID; rP; rxP; SID; S) with non-negligible probability ², then we can solve CDHP in G1 with non-negligible probability ².

Theorem 2

A group member cannot impersonate other group members to sign the message m with non-negligible probability.

Theorem 3

Under the assumption of hardness of DLP in G1, KGC cannot impersonate a group member to sign the message m with non-negligible probability.

From the three theorems above, it is easy to deduce that our scheme satisfies the security properties of group signatures unforgeability, anonymity, unlink-ability, traceability, exculpability and coalition-resistance.

Our group signature scheme overcomes the drawback that a user(signer) should have a new key pair for each message if he wants to sign many message. To some extent, we solve the open problem of designing an ID-based group signature scheme from bilinear pairings with one key pair.

CONCLUSION

We proposed an efficient identity-based group signature scheme. The group signature is based on the CDHP assumption. In addition, the size of the group public key and the length of the signature are independent on the number of the group members. Once a user joins the group, they can sign many messages using the same key pair. However, the standard identity based cryptosystem has a weakness in that the entities' keys are completely controlled by Centralized key generator. The proposed identity-based group signature scheme supports a set of attractive properties, correctness, signer anonymity, signer traceability. This group signature solution will benefit any application, in which group identies are sensitive

[1] D. Chaum and E. van Heyst, "Group signatures", in
EUROCRYPT'91, LNCS 547, pp. 257-265, Springer-Verlag, 1991.
[2] J. Camenisch and M. Michels, "A group signature scheme based on an RSA-variant", in *Technical Report RS-98-27. BRICS,* ASIACRYPT'98Springer-Verlag, November 1998.
.[3] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups", in *CT-RSA'05*, LNCS 3376, pp. 136-153, Springer-Verlag, 2005.
[4] S. Han, J. Wang, and W. Liu, "An efficient identitybased group signature scheme over elliptic curves", in *ECUMN'04*, LNCS 3262, pp. 417- 429, Springer-Verlag, 2004.
[5]G. Ateniese, J. Camenisch, M. Joye, G. Tsudik, A practical and provably secure coalition-resistant group signature scheme, Advances in Cryptology-Crypto 2000, LNCS 1880, pp.255-270, Springer-Verlag, 2000.
[6]G. Ateniese, G. Tsudik, Some open issues and new directions in group signatures, Financial Cryptography 1999, LNCS 1648, pp.196-211, Springer-Verlag, 1999.
[7]D. Balfanz, G. Durfee, N. Shankar, D. Smentters, J. Staddon, H. Wong, Secret handshakes from pairing based agreements, Proceeding of the 2003 IEEE Sympo-siumon Security and Privacy, pp. 180–196, 2003.
[8]P. Barreto, H.Y. Kim, B.Lynn, and M.Scott, E□cient algorithms for pairings-based cryptosystems, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
[9]M. Bellare, D. Micciancio and B. Warinschi, Foundations of group signatures: formal definations, simplified requirements, and a construction based on generalassumptions, Advances in Cryptology-Eurocrypt 2003, LNCS 2656, pp.614-629, Springer-Verlag, 2003.
[10]D. Boneh and M. Franklin, Identity-based encryption from the Weil pairings, Ad-vances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
[11]D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairings, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
[12]J. Camenisch, Efficient and generalized group signatures, Advances in Cryptology-Eurocrypt 1997, LNCS 1233, pp.465-479, Springer-Verlag, 1997.
[13]J. Camenisch and M. Stadler, Efficient group signatures schemes for large groups, Advances in Cryptology-Crypto 1997, LNCS 1294, pp.410-424, Springer-Verlag, 1997.
[14]J. Cha and J.H. Cheon, An identity-based signature
from gap Di□e-Hellman groups, Public Key Cryptography-PKC 2003, LNCS 2567, pp.18-30, Springer-Verlag, 2003.
[15]D. Chaum and E. van Heijst, Group signatures, Advances in Cryptology-Eurocrypt 1991, LNCS 547, pp.257-265, Springer-Verlag, 1991.
[16]L. Chen and T. Pedersen, New group signature schemes, Advances in Cryptology-Eurocrypt 1994, LNCS 950, pp.171-181, Springer-Verlag, 1994.
[17]L. Chen and T. Pedersen, On the efficiency of group signatures providing information-theoretic anonymityenisch, Advances in Cryptology-Eurocrypt 1995, LNCS 1233, pp.465-479, Springer-Verlag, 1997.
[18]C. Gentry and A. Siverberg, Hierarchical ID-Based Cryptography, Advances in Cryptology-Asiacrypt 2002, LNCS 2501, pp.548–566, Springer-Verlag, 2002.
[19]F. Hess, E□cient identity based signature schemes based on pairingss, Proc. 9th Workshop on Selected Areas in Cryptography – SAC 2002, LNCS 2595, Springer-Verlag, pp.310-324, 2002.
[20]M. Joye, On the difficulty coalition-resistance in group signature schemes (II), Technique Report, LCIS 99-6B, 1999.
[21]M. Joye, S. Kim and N. Lee, Cryptanalysis of two
group signature schemes, Infor-mation Security 1999, LNCS 1729, pp.271-275, Springer-Verlag, 1999.
[22]A. Juels, Trustee Tokens: simple and practical anonymous digital coin tracing, Financial Cryptography 1999, LNCS 1648, pp.33-43, Springer-Verlag, 1999.
[23]A.Lysyanskays, Z.Ramzan, Group blind signatures: A scalable solution to electronic cash, Financial Cryptography 1998, LNCS 1465, pp.184-197, Springer Verlag, 1998.
[24]W. Mao and C.H. Lim, Cryptanalysis in prime order subgroup of Zn , Advances in Cryptology-Asiacrypt 1998, LNCS 1514, pp.214-226, Springer-Verlag, 1998.
[25]S. Park, S. Kim and D.Won, ID-based group signature, Electronics Letters, 33(19), pp.16163-1617,
1997.

[26]H. Petersen, How to conver any digital signature scheme into a group signaure sheme, In Security Protocols Workshop 1997, pp.177-190, Springer-Verlag, 1997.
[27]A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 1984, LNCS 196, pp.47-53, Springer-Verlag, 1984.
[28]N.P. Smart, An identity based authenticated key agreement protocol based on the Weil pairings, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.
[29]K. Sakurai, S. Miyazaki, An Anonymous Electronic Bidding Protocol Based on New Convertible Group Signature Scheme, ACISP 2000, LNCS 1841, pp.10-12, Springer-Verlag, 2000.
[30] J. Traor, Group signatures and their relevance to privacy protecting o□ine electronic cash systems, ACISP 1999, LNCS 1587, pp. 228-243, Springer Verlag,199
[31]Y. Tseng and J. Jan, A novel ID-based group signature, International computer symposium, workshop on cryptology and information security, pp.159-164, 1998.
[32]F. Zhang and K. Kim, ID-based blind signature and ring signature from pairings, Advances in Cryptology Asiacrypt 2002, LNCS 2501, pp. 533-547, Springer Verlag,2002