4th International Conference on Science, Technology and Management
India International Centre, New Delhi (ICSTM-16)
15th May 2016, www.conferenceworld.in ISBN: 978-81-932074-8-2

PRIVACY PRESERVATION AGAINST COLLUDING ATTACK USING GROUP SIGNATURE SCHEME

Aaditya Jain[1], Jitendra Sen[2], Dr. Bala Buksh[3]

[1] *M.Tech Scholar, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India*

[2]*Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India*

[3]*Professor, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India*

ABSTRACT

Group signature is an extension of digital signature, which allows a group member to sign anonymously a document on behalf of the group. Any client can verify the authenticity of the document by using the public parameters of the group. The identity of the group member cannot be revealed from the group signature. In case of a legal dispute, an authorized group member can disclose the identity of the group member from the signed document but some time. In the last few years it is analyze that colluding attack is the most vulnerable type of attack so in this paper, we designed a group signature scheme based upon hard computational assumptions such as, Discrete Logarithm Problem (DLP), Integer Factorization Problem (IFP), and Computational Diffie Hellmann (CDH) problem. The proposed scheme is proved to be resistant against colluding attack. Moreover, the group signature remains valid, if some members leave the group or some new members join the group.

Keywords: Group Signature, Colluding Attack, Discrete Logarithm, Anomility.

I. INTRODUCTION

A digital signature is a mathematical scheme for providing the authenticity of a digital information or document. A valid digital signature gives a recipient reason to believe that the information was given by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. Digital signatures are basically applied for software distribution, financial transactions, and in cases of disputes where it is important to detect forgery or tampering of digital information. Extending the idea of digital signature into the group, a new signature scheme i.e. group signature scheme, first introduced by Chaum and Heyst, allows a group member to sign messages anonymously on behalf of the group [1]. Any client can verify the authenticity of the signature by using only the group's public key and parameters. The identity of the group member cannot be linked from a signed message. In the case of a dispute, the identity of a signer or member can be revealed by a designated entity. The main feature of group signature is the security of the information or the data that makes it more important and attractive for many real time applications, such as e-cash, e-bidding and e-commerce, where the priority of privacy and anonymity of signer is very much high and important for an organization.

After the scheme proposed by Chaum, a number of group signature schemes have been proposed. Chen and Pedersen constructed a scheme, which allows new members to join the group dynamically, and suggested to use group signatures in e-bidding [2]. Camenisch and Stadler proposed the first group signature scheme that can be used for large groups, since in their scheme the group public key and signatures have lengths independent of the group size [3]. Later, Kim et al. extended their scheme to support efficient member revocation [4]. Ateniese and Tsudik pointed out some obstacles that stand in the way of real world applications of group signatures, such as coalition attacks and member deletion [5].

In the literature, we observed that at present these group signature schemes available are mainly classified into two types, a public-key registration type, and a certificate based type. In the former type are constructed by using only known order groups. However, in these schemes, both a group public key and the signature size depend on the number of group members. It yields a serious problem for large groups. In the latter type, give a membership certificate to group members, and the group signature is based on the zero knowledge proof of knowledge (SPK) of membership certificate. Therefore, neither a group public key nor signature size depends on the number of group members.

II. OVERVIEW OF GROUP SIGNATURE SCHEME

A group signature scheme is a technique of signing the documents or any relevant information anonymously on behalf of group, where group consist of manager and various designated members shown in Fig1. The integrity of sign is verified by the designated verifier, where the verifier is aware of the correctness of the sign not the identity of member who signed the documents etc.

According to the Chaum and Heyst in [1] the group signature must include following policies.

- Group members are only role person to sign the messages.
- The integrity of the signature should be checked without revealing the identity of the signer.
- If necessary, the signature can be opened to reveal the identity of signer.

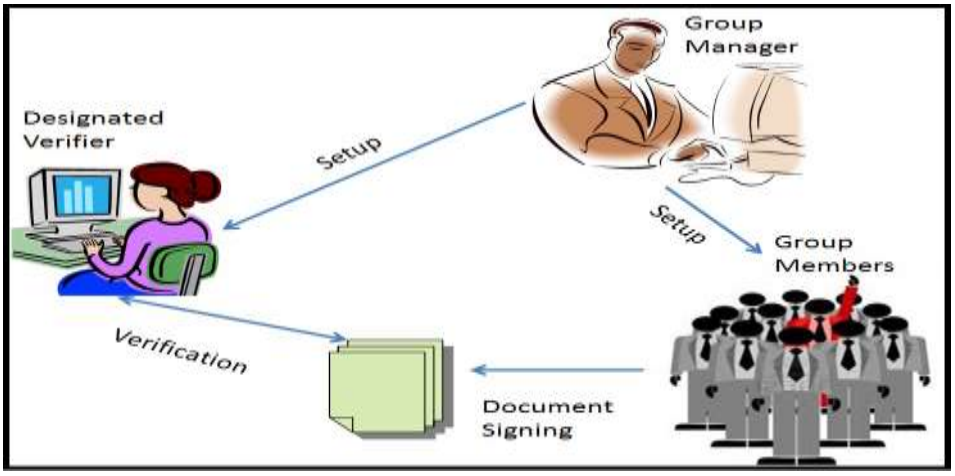

Fig. 1 Standard Group Signature System

In group signature schemes, group manager is the only person capable of addition of the members and removing of the members from the group. In case of legal disputes, if any, then manager is responsible in revealing the

identity of the signer or member who signed. However, a standard group signature scheme has following five phases [6], [7]:

- System setup: the setup includes key generation mechanism, where the group manager's key and group public key and secret keys for members with some essential parameters is necessary.
- Join: this phase includes joining of members in the group where the user or member receives the membership certificate and secret key from the group manager.
- Sign: this phase performs the signature generation on behalf of the group.
- Verify: this phase includes verification of signature via group's public key on behalf of the group
- Open: this phase is additional vital phase where the identity of signer can be revealed by the group manager, if necessary.

In literature, we found that the responsibility of adding members and revoking signature anonymity are separated and assigned to two distinguished persons namely, membership manager and revocation manager. The basic security requirements of a standard group signature are given below:

- Soundness or correctness: Valid signatures by group members always verify correctly, and invalid signatures always fail verification.
- Anonymity: for a message and its signature, the identity of the individual signer cannot be revealed without the group manager's secret key.
- Unforgeablility: Only members of the group can create valid group signatures and otherwise signature is considered to be invalid.
- Unlinkability: for certain messages and their signatures, we cannot determine if the signatures were from the same signer or not.
- Exculpability: If group members collude, then it must be impossible to forge a signature for a non-participating group member.

III. SCENARIO OF COLLUDING ATTACK

Collusion as the name suggest is an act of cooperation between two person or set of person for the sake of achieving mainly the illegal benefits. Collusion is a very common and risky problem to be faced in every field which cannot be controlled easily as the unpredictable nature of attack can observe in Fig2. So if we generalize the nature, we can state the collusion, as a agreement between two or more parties, sometimes illegal and therefore secretive, to limit open competition by deceiving, misleading, or defrauding others of their legal rights, or to obtain an objective forbidden by law typically by defrauding or gaining an unfair advantage. It is an agreement among firms or individuals to divide a market, set prices, limit production or limit opportunities. In other words collusion attack can be described as an action carried out by a given set of malicious users in possession of a copy of protected content that join together in order to obtain at the end of the attack procedure an unprotected asset. The attack is carried out by properly combining the protected copies of the multimedia documents collected by the collude, according to the type of content and the kind of adopted protection system.

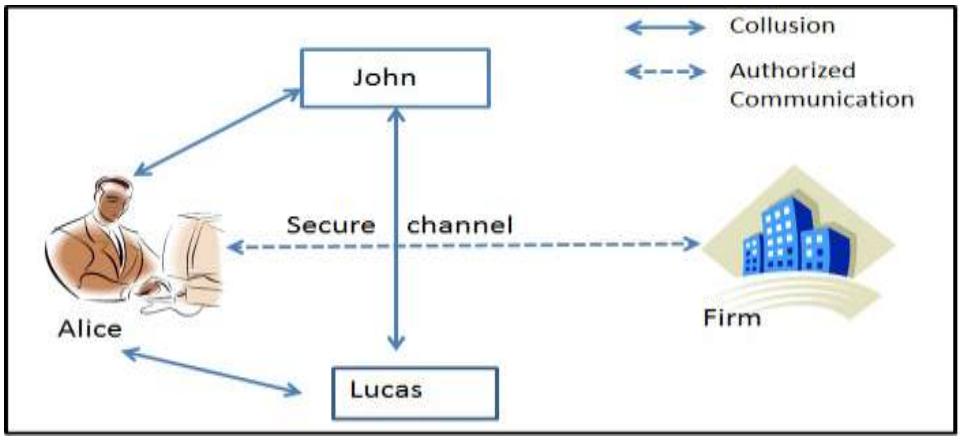

Fig. 2 Scenario of Colluding Attack

The Colluding attack has another flavor with small variation stated as coalition. The coalition can be thought of subpart of collusion where a set of member collide to achieve the respective objective.

IV. PRELIMINARIES FOR GROUP SIGNATURE SCHEME

4.1 Discrete Logarithm Problem (DLP)

Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups [8]. If G is a multiplicative cyclic group and g is a generator of G, then from the definition of cyclic groups, we know every element h in G can be written as g^x for some x. The discrete logarithm to the base g of h in the group G is defined to be x. The discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups. Mathematically DLP can be given as: Let a, b, n be positive real numbers, such that

$$\log_b(a) = n, if\ and\ only\ if\ a = b^n$$

The $\log b$ function solves the following problem: Given a base b and a power a of b, find an exponent n such that $a = b^n$ .That is, given b^n and b, find n .

4.2 Cryptographic Hash Function

A cryptographic hash function is hash function that converts arbitrary block of information and provides a fixed size string where each data is mapped such that any change would vary the value of hash with very high probability [9]. The information to be encoded is known to be the message and the hash value obtained is called the message digest or digest. Ideally the hash function must follow certain properties, firstly should be easy to compute the hash value for given message and at the same time must be infeasible to generate a message with a random hash and also be resistant against modify a message without the hash. We may come across a long list of cryptographic hash functions, although many have been found to be vulnerable and should not be used. Considering the integrity of information we may use hash function such as SHA 1, MD2, MD4 and MD5 where each scheme can be used to provide a digest of respective bits depending on the requirement of message or information integrity.

4.3 Random Number Generator

A random number generator is a computational device designed to generate a sequence of numbers that lack any pattern, i.e. appear random [10]. The many applications of randomness have led to the development of several different methods for generating random data. Random number generators are very useful in developing Monte Carlo-method simulations, as debugging is facilitated by the ability to run the same sequence of random numbers again by starting from the same random seed. They are also used in cryptography so long as the seed is secret. Sender and receiver can generate the same set of numbers automatically to use as keys. There are two principal methods used to generate random numbers. One measures some physical phenomenon that is expected to be random and then compensates for possible biases in the measurement process. The other uses computational algorithms that can produce long sequences of apparently random results, which are in fact completely determined by a shorter initial value, known as a seed or key. The latter type is often called pseudorandom number generators.

4.4 Prime Numbers and Primality Test

A primality test is an algorithm for determining whether an input number is prime. Amongst other fields of mathematics, it is used for cryptography [11]. Unlike integer factorization, primality tests do not generally give prime factors, only stating whether the input number is prime or not. Factorization is thought to be a computationally difficult problem, whereas primality testing is comparatively easy. Primality tests can be classified in two varieties: deterministic and probabilistic.

Deterministic Algorithm: A deterministic primality testing algorithm accepts an integer and always outputs a prime or a composite. Deterministic tests determine with absolutecertainty whether a number is prime. Until recently, all deterministic algorithms were so insufficient at finding larger primes that they were considered infeasible. In 2002, Agrawal, Kayal and Saxena announced that that they had found an algorithm for primality testing with polynomial time complexity of O((log 12n)) .

Probabilistic Algorithm: Probabilistic tests can potentially (although with very small probability) falsely identify a composite number as prime. However, they are in general much faster than deterministic tests. Numbers that have passed a probabilistic prime test are therefore properly referred to as probable primes until their primality can be demonstrated deterministically.

V. CLASSIFICATION OF GROUP SIGNATURE SCHEME

5.1 Static Group Signature Scheme

Static group signatures as in [12] consist of four polynomial time algorithm namely key generation where system generates group public key with the secret key generation for signing of document, Signature generation algorithm where it takes the secret key and the information for signing and returns the signed document, Signature verification algorithm where it takes the group public key, the signature with the message and returns the value as accepted or rejected, finally the opening algorithm where it takes group managers secret key, message and the signature and reveals the identity of group member who signed. In general, the static group signature determines all the parameters initially with the group member in the group and also revocation is possible only through removing of member but no addition of member allowed.

5.2 Dynamic Group Signature Scheme

Dynamic group signature as the name suggests the randomness and non deterministic nature of scheme [13]. The dynamic group signature consist of five polynomial algorithm namely signature key parameter generation where public parameters and secret of member is determined with a new list generated which keeps the track of group member registration, join protocol where it computes the two algorithm, firstly registering the member into the registration list and secondly generating the member parameters for signing, Signature generation algorithm where it takes the message with the group members secret key and generates sig- nature, Signature verification algorithm which is a deterministic algorithm where it takes message ,group public key and signature generated from group and outputs the validity of signature. Finally the opening algorithm of signature where it takes message, signature from group and registration list which will reveal the identity of member in case of dispute. The difference between the static and dynamic group signature is the addition of join phase where it provides the full revocation as member can be added or removed depending on the choice of member in a group.

5.3 Group Signature with Verifiable Opening

The distinguished property of signature is to preserve signer's anonymity, yet allow the manager to reveal the identity in legal dispute through the open procedure. The group signature with verifiable opening has five polynomial algorithms as the dynamic group signature but the difference here comes in the open procedure, where the algorithm is divided into two procedures i.e. opening procedure and the judging procedure. The basic functionality of group signature does not allow the manager to falsely accuse the member in case of dispute, thus to assure the validity of managers decision, manager has to provide additional proof against the member. The opening algorithm can be given as; opening procedure that takes the managers secret key with the message and the signature from the group and out puts the identity if accused with proof. In judgment procedure, algorithm takes the proof and signature and reveals the validity of manager's signature proving to be verifiably open procedure.

5.4 Group Signature with Verifiable Opening

Group signature includes the group manager, who is responsible for many roles in the signature procedure. The manager is concerned with mainly two tasks i.e. the member ship in group and the opening of signature, these two tasks can be distributed among two authorities as the issuer and the opener as distributed roles of manager. The group signature scheme consist of basic polynomial algorithm except the change in key generation where the algorithm provides secret key for issuer and secret key for opener with group public parameters, join procedure is carried out by the issuer where the registration list is updated after every successful join operation and the opening procedure where the new role i.e. opener is responsible for opening the signature in case of any disputes. These can be modified into the verifiable opening group signature by including the proof and validity of proof in the opening procedure. An alternative approach would be to require some third trusted party to generate both types of private keys in advance and then hand the keys to the issuer and the opener respectively using secure channels.

VI. LITERATURE SEARCH

6.1 Group Signature Based on DLP

Chaum and Heyst introduced the group signature scheme based on DLP. In 1997, Park, Kim and Won proposed an ID-based group signature [14]. The main contribution of their scheme is that signer's public key is identification (ID) that does not need to be verified, so there is no need to set up a trusted center to verify a huge number of public keys. Nevertheless, an ID-based group signature must use a set of group member identities in the signing phase. When group member changes either add or remove, the group signature is inactive and moreover the length of its signature increases with the number of members.

In 1998, Lee and Chang proposed an efficient group signature based on the discrete logarithm [15]. The scheme was more efficient in terms of computational, communication and storage costs, while allowing the group to be changed without having the members choosing the new keys. However, when the signer has been identified, the authority must redistribute the keys of this signer and send the keys to him/her.

In 1999, Tseng and Jan aimed to improve the aforementioned problem to propose an improved group signature that is based on the Lee and Chang scheme [15]. In the same year, Sun showed in that the Tseng-Jan scheme is still not unlinkable. After that, Bellare and Miner in [16] proposed to improve their scheme.

In 2000, Li et al. [17] demonstrated that two schemes of the paper [16], which are called TJ1 and TJ2 both could be attacked. The threshold group signature is an important kind of signature. Many threshold group signatures are proposed but many suffered from conspiracy attack and are insecure.

6.2 Group Signature with Anonymity and Separability

We have group signature based on strong separability Shundong Xia, where author proposed secure scheme based on discrete logarithm problem, such that group manager can be split into membership manager and revocation manager. Previously proposed group signature scheme were not having identity with respect to the public keys, thus requiring the manger to maintain data to map the identity information. The scheme suggested that previous schemes may have weak form of separability if proper communication is not available between revocation and membership manager thus justifying strong separability.

In the paper [18] by Fucai Zhou, 2008 anonymity of signature was compared to the group signature where they discussed an important problem, that is the signatures are produced on behalf of group or group member and concluding that the signature should be produced on behalf of group and also pointed the convict of authenticated content. In 2009, a new improved group signature was introduced by Cheng Lee et al. where the problem of unlinkability and unforgeablility was enhanced based on the discrete logarithm.

6.3 Group Signature Based on Threshold Scheme

The group signature based on threshold scheme can be classified group oriented (t, n) traceable signers and group oriented anonymous signers. The signature was proven to be under forgery attack in paper proposed by Z.C. Li, 2001.Threshold based signature was under revision by many authors and also being used in proxy and blind signatures. In the paper Yuan-Lung Yu, 2005 in [19] the author integrates the short secret key characteristic of the elliptic curve cryptosystem and the (t, n) threshold method to create a signature scheme with simultaneous signing. The distinguishing feature of the proposed scheme is that the threshold value denotes the

minimum number of members required to produce a valid group signature. All message recipients then can verify the signature. Many threshold group signature schemes have been proposed, but most of them suffer from conspiracy attack and are insecure.

In this paper Fengyin Li, 2007 in [20], based on the discrete logarithm problem, a secure threshold group signature scheme is proposed. The scheme is not only threshold signing, but also threshold verifying. In the paper, Fucai Zhou presented the requirement of real group signature and gave a new scheme to realize a real group signature, which is based on pivot threshold scheme [20]. In 2011, Improvement of threshold group signature scheme was introduced by Tong lu and Baoyuankang where the scheme proposes to be more secure as providing the strong unforgeability based on discrete logarithm problem.

6.4 Short Group Signature Scheme

The Group signature schemes are revised with respect to many security factors where size of the signature was considered to be main issue by some authors as compared to the complexities of signature generation schemes. In 2004 a short signature scheme was proposed where they gave a scheme that has approximately the size of RSA signature standard with same security. The scheme was based on bilinear groups with Strong Diffie Hellman assumptions (SDH) [21].

Many schemes were developed that would be efficient and short in size but considering the security of the signature in 2006, the author considered the formal security model which has been proposed by Bellare et al. in [13], including both dynamic groups, concurrent join and proposed extremely dynamic short signature scheme with strong security under random oracle assumption. The signature scheme was based on strong Diffie Hellman assumptions (SDH) and external Diffie Hellman assumptions.

Recently a paper on Short group signature with control linkability is proposed by Cecile et al. aims at providing dynamic membership where the controllable link ability enables an entity who possesses linking key to check if two signatures are from the same signer while preserving anonymity [22]. The scheme is sufficiently efficient and well-suited for real-time applications even with restricted resources, such as vehicular adhoc network and Trusted Platform Module at the same time scheme supporting controllable link ability provides a signature that is shorter than the standard normal group signature.

VII. GROUP SIGNATURE AGAINST COLLUDING ATTACK

We proposed a group signature scheme which provides full anonymity of signer, full traceability of the signature, resistant to colluding attack and forgery attack. The proposed group signature scheme consists of four participants namely, group manager, group members, designated verifier, and trusted third party. The scheme consists of following five phases. The system model of proposed scheme is shown in Figure 3. A trusted third party (TTP) is an entity involved in this scheme who manages all critical communications among the group members and group manager.

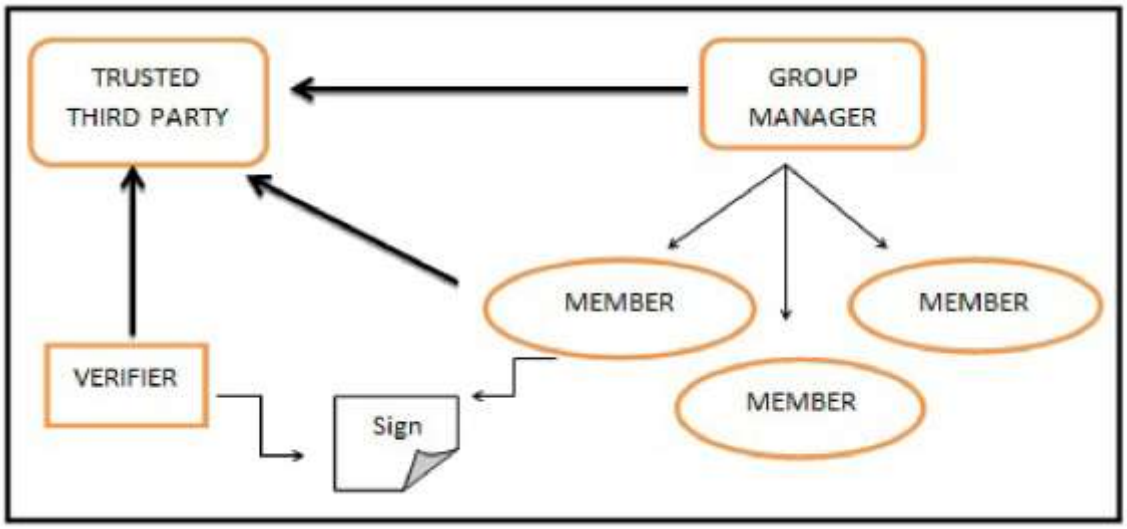

Fig.3 Simple view of proposed scheme

7.1 Setup Phase

Manager selects a prime p as public key which is large enough that the discrete log problem is intractable in Z_{p*}. He selects another public key q such that (q - 1) = 0 mod p and also chooses a random private key Y. Manager also computes group key as $g_k = (y-1)^{\delta}$, where the δ is a randomly chosen parameter.

7.2 Join Phase

Any member who wants to join the group gets registered through the certificate authority and authority ensures the registration of member to the manager. Manager computes the secret d for the member such that $d = y^{\alpha} \, mod \, p$ where α is randomly chosen by the group manager. Then the manager splits the secret key d into two parts as d1 and d2. The key division can be done through any method which is appropriate to the manager. Here the manager has a exibility to decide the splitting method but one important concern regarding the splitting is that the division should be lossless. The secret keys d and d1 are sent to each member in encrypted form using the member0s public key. The key d2 is send to the trusted third party (TTP) which manages keys of each member. Each member chooses a primitive element e_0 in z_p, and computes $e_1 = e_0{}^{p-1/q} mod \, p$. The Member chooses a secret key x and compute $e_2 = e_1{}^{xd} \, mod \, p$.

Members are organized according to a structure as shown in Figure 4. Here we have two structures namely QA, QB which are divided into many slots with respect to the member who will sign the document. Each member is assigned with the binary counter (0/1), where 0 represents that the member is not signing any document and 1 represents that the member is reserved with the signing of document. We have members organized initially in QA and when a member completes the signing of the document then the member is send to the QB similarly a member completing signing of document or message in QB is send back to the QA. The trusted third party has database maintained for the member according to the slot and structure defined.

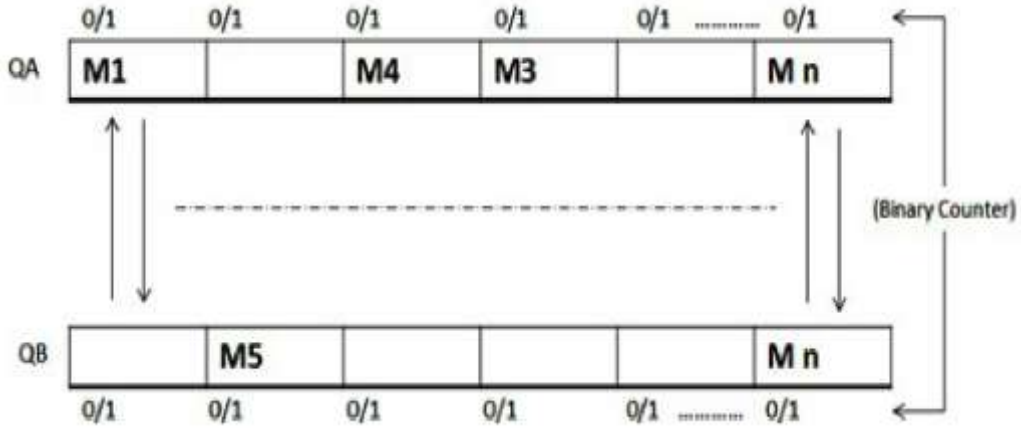

Fig 4 Join Phase of the Scheme

7.3 Signature Generation Phase

In this phase, a member Xi chooses a random number β from 1 to q and computes the signature as:

$$s1 = h(M|e1^{\beta} \, mod \, P)$$

$$s2 = \beta + x \times (id + d2) \times s1 mod q$$

Where M is the required message to be signed, h represents the hash for the signature and id represents the slot id that maps the key from trusted third party with the respective member. The parameter e1, e2 are encrypted using verifiers public key and finally the message, signature with hash M, s1, s2 along with the hash of key h(d2) encrypted via manager's public key are finally encrypted using group key and send to the verifier. The value of β will vary with respect to each message.

7.4 Verification Phase

The verifier gets the encrypted data which he decrypts using the group key and verifier's private key accordingly. And now computes the following to check the validity of signature.

$$s' = h(M|e1^{s2} \times e2^{-s1} \, mod \, p)$$

If the value of s' satisfies the following, $s1 = S' mod \, p$, then signature is accepted otherwise rejected.

7.5 Open Phase

The encrypted signature can be decrypted by manager with the group key and can check the hash value that is encrypted with the manager's key. As manager has the key hashed with respect to each member so can say who has generated the signature.

VIII. SECURITY ANALYSIS OF THE PROPOSED SCHEME

We analyze the security feature of the proposed scheme including computational efficiency. It is proved that the proposed scheme satisfies the unforgeability, anonymity, verifiability, and exculpability. This scheme is safe and secure against colluding attack and also safe from many active attacks.

Correctness: The group signature s1, s2 for a message M is indeed a valid signature.

Proof: The correctness of the group signature is given as follows.

$$S' = h(M|e1^{s2}.e2^{-s1} mod\ p)$$

$$S' = h(M|e1^{\beta+x(id+d2)s1 mod\ q}.e2^{-s1} mod\ p)$$

$$S' = h(M|e1^{\beta+(id+d2)s1\ mod\ q}.e2^{-x.d.s1\ mod\ q} modp)$$

$$S' = h(M|e^{\beta\ mod q})$$

As the above signature is congruent, thus proofs the correctness of signature.

IX. CONCLUSION

The group signature is extended idea of digital signature with some stringent condition from which the resistance against colluding attack is one of the critical issues in group signature. Idea of setting a secure group system became very challenging as the condition were very stringent as compared to digital signature but if this is achieved can be effective in this fast developing digital era. The proposed group signature scheme is secure scheme based on discrete logarithm problem assumption. The proposed scheme is member independent such that any member leaving or joining would not affect the signature generation scheme. The size of signature is still needed to be considered. Though the cost of signature verification is more as compared to other standard signature scheme but on the security aspect this would be efficient scheme where this scheme is very much safe against many active attacks can be very much useful in an organization, where the group manager can be equivalent to the chief executive officer, the signers can be employees of the organization and the verifier may be a specific customer. This scheme can also be applicable in e-voting system, e-cash system and e-commerce applications.

REFERENCES

[1] D. Chaum and E. van Heyst, “Group signatures”, Lecture Notes On Computer Science, 547(8):257-265, 1991.

[2] L. Chen and T. P. Pedersen, “New group signature schemes”, In A. De Santis, editor, Advances in Cryptology- EUROCRYPT'94, pages 171-181. Springer, Berlin, 1994.

[3] Jan Camenisch and Markus Stadler, “Efficient group signature schemes for large groups”, In Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '97, pages 410-424, Springer-Verlag, 1997.

[4] Hyun-Jeong Kim, Jong In Lim, and Dong Hoon Lee, “Efficient and secure member deletion in group signature schemes”, In Proceedings of the Third International Conference on Information Security and Cryptology, ICISC '00, pages 150-161, Springer-Verlag, 2001.

[5] Giuseppe Ateniese and Gene Tsudik, “Some open issues and new directions in group signatures”, International Journal of Information Science pages 196-211, 1999.

[6] J. Zhang, J. Zou, and Y. Wang, “An improved group signature scheme”, In Lecture Notes in Computer Science, volume 3592, pages 185-194, 2005.

[7] Y. He, "New dynamic group signature scheme", Wuhan University Journal of Natural Sciences, 11(6):1693-1696, 2006.

[8] Steven D, Galbraith and Mark Holmes, "A non-uniform birthday problem with applications to discrete logarithms", Discrete Applied Mathematics, 160(10-11):1547-1560, 2012.

[9] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance", second preimage resistance, and collision resistance, 2004.

[10] David M'Raihi, David Naccache, David Pointcheval, and Serge Vaudenay, "Computational alternatives to random number generators", In Fifth Annual Workshop on Selected Areas in Cryptography SAC098, volume 1556 of LNCS, pages 72-80, Kingston, Ontario, Canada, 1998. Springer.

[11] Henk C. A. van Tilborg and Sushil Jajodia, editors, "Encyclopedia of Cryptography and Security", 2nd Ed. Springer, 2011.

[12] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi, "Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions", In Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, EUROCRYPT'03, pages 614-629, 2003.

[13] Mihir Bellare, Haixia Shi, and Chong Zhang, "Foundations of group signatures: The case of dynamic groups", In CT-RSA, pages 136-153, 2005.

[14] S.J. Park S.J. Kim and D.H Won, "Convertible group signatures", volume 1163, pages 311-321. Springer-Verlag, 1996.

[15] W.B. Lee and C.C. Chang, "Efficient group signature scheme based on the discrete logarithm. volume 145, pages 15-18. IEEE, 1998.

[16] Mihir Bellare and Sara K. Miner, "A forward-secure digital signature scheme. pages 431-448, Springer-Verlag, 1999.

[17] N. Lee, T. Hwang, and C. Li., "(t, n) threshold untraceable signatures", Journal of Information Science and Engineering, 16(6):835-846, 2000.

[18] Fucai Zhou, Jun Zhang, and Jian Xu, "Research on anonymous signatures and group signatures", Computation Communication, 31(17):4199-4205, November 2008.

[19] Yuan-Lung Yu and Tzer Shyong Chen, "An efficient threshold group signature scheme", Applied Mathematics and Computation, 167(1):362-371, 2005.

[20] Fengyin Li, Jiguo Yu, and Hongwei Ju, "A new threshold group signature scheme based on discrete logarithm problem", In Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, volume 03, SNPD '07, pages 1176-1182, Washington, DC, USA, 2007. IEEE Computer Society.

[21] Dan Boneh and Hovav Shacham, "Group signatures with verifier local revocation", In ACM Conference on Computer and Communications Security, pages 168-177, 2004.

[22] Cecile Delerablee and David Pointcheval, "Dynamic fully anonymous short group signatures", In VIETCRYPT, pages 193-210, 2006.0