ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 10, April 2013

A Survey of Group Signature Technique, its Applications and Attacks

Aayush Agarwal, Rekha Saraswat

Abstract*— Group Signature scheme allows members of a group to sign messages on behalf of the group, such that the resulting signature does not reveal the identity of the signer. Signatures can be verified with respect to a single group public key. In case of dispute, only a designated group manager, because of their special property, is able to open signatures, and thus reveal the signer's identity. Its applications are widespread used, especially in e-commerce such as e-cash, e-voting and e-auction. This paper incorporate the detailed study of group signature definition, concept and the main contributions in this field such as applications of group signature that tells where we can use this technique. It starts with overview, concept, properties, keys used, application, challenges, and attack of group signature and a comparative analysis of some group signature techniques.

***Index Terms*—Applications, Attacks, Properties, Signature, Techniques.**

I. INTRODUCTION

A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of a later dispute, open signatures, i.e., reveal the identity of the signer. Group signatures could for instance be used by a company for authenticating price lists, press releases, or digital contracts. The customers need to know only a single company public key to verify signatures. The company can hide any internal organizational structures and responsibilities, but still can find out which employee (i.e., group member) has signed a particular document. The concept of group signatures was introduced by Chaum and van Heyst and they also proposed the first realizations. Improved solutions were later presented by Chen and Pedersen, Camenisch, and Petersen. However, all previously proposed solutions have the following undesirable properties: the length of the group's public key and/or the size of a signature depend on the size of the group. This is very problematic for large groups to add new group members, it is necessary to modify at least the public key. Jan Camenisch and Markus Stadler present the first efficient group signature schemes which overcome these problems. The lengths of the public key and of the signatures are, as well as the computational effort for signing and verifying, independent of the number of group members. Furthermore, the public key remains unchanged if new members are added to the group. The schemes even conceal the size of the group. For realizing such schemes we employ novel techniques of independent interest, such as efficient proofs of (or signatures of) knowledge of double discrete logarithms, of e-th roots of discrete logarithms, and of e-th roots of components of representations.

The paper is organized as follows:

- Section 2 describes the concept of digital signature, their properties and requirements. It also presents how digital signature works in communication or in transferring the message. Finally it mentions various techniques and algorithms based on digital signature technique.
- Section 3 describes the concept of group signature technique with their properties and various keys which are used in this scheme. It also presents the previous work done on group signature and finally the requirements of this technique.
- Section 4 describes the group signature applications.
- Section 5 describes the various possible attacks on the group signature scheme.
- Section 6 describes the various challenges and efficiency of group signature.

II. DIGITAL SIGNATURE TECHNOLOGY

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. It combines a hash with a digital signature algorithm. The digital signature is analogous to the handwritten signature.

A. It must have the following properties:

- It must verify the author and the date and time of the signature.
- It must to authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

B. On the basis of these properties, we can formulate the following requirements for a digital signature:

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.

- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

C. How digital signature works:

A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation.

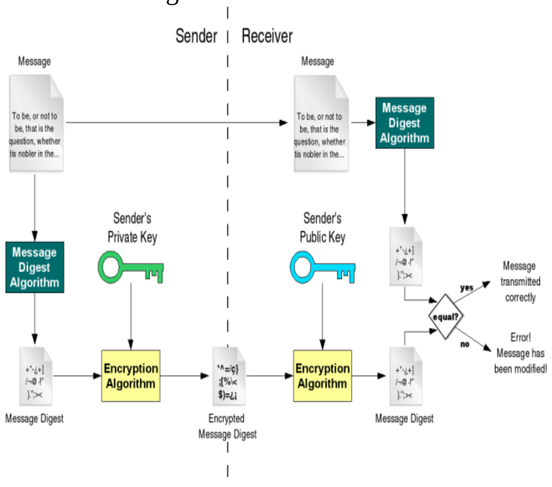

Fig 1: Digital Signatures [28]

The digital signature for a message is generated in two steps:

1. A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: (a) it is always smaller than the message itself and (b) Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.

2. The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*.

The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:

1. Using the sender's public key decrypts the digital signature to obtain the message digest generated by the sender.
2. Uses the same message digest algorithm used by the sender to generate a message digest of the received message.
3. Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver). If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

D. Techniques based on digital signature:

There are various techniques which are based on digital signature and use their concept for communication:

- **Group Signature:** The concept of group signatures allows a group member to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature's originator can be revealed by a designated entity.
- **Ring Signature:** A similar system that excludes the requirement of a group manager and provides true anonymity for signers.
- **Threshold Signature:** A threshold signature involves a fixed-size quorum (threshold) of signers. Each signer must be a genuine group member with a share of a group secret signing key. A (t,n) threshold signature scheme supports n potential signers, any t of which can on behalf of the group. Threshold signatures reveal nothing about the t signers; no one can trace the identity of the signers (not even a trusted center who have set up the system).
- **Multisignature:** A multisignature represents a certain number of signers signing a given message. Number of signers is not fixed and signers' identities are evident from a given multi-signature. A multisignature is much shorter (sometimes constant) than the simple collection of individual signatures.
- **Proxy Signature:** A proxy signature allows a delegator to give partial signing rights to other parties called proxy signers. Proxy signatures do not offer Anonymity.
- **Blind Signature:** A signer can sign messages for users. The signer does not know the message he is signing. The signer should not be able to recognize the message nor the signature he has produced. The user is anonymous w.r.t all other users. Blind Signature implemented based on Schnorr Signature. It is lot faster than group signature.

E. Algorithms based on digital signature:

- **RSA** is an algorithm for public-key cryptography that is based on the presumed difficulty based on the presumed difficulty of factoring large integer, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.
- **The Digital Signature Algorithm** (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186, adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1. The standard was expanded further in 2000 as FIPS 186-2 and again in 2009 as FIPS 186-3.
- **The ElGamal signature scheme** is a digital signature scheme which is based on the difficulty of computing discrete logarithms. It was described by Taher ElGamal in 1984.
- In cryptography the **Rabin Signature Scheme** is a method of Digital signature originally proposed by Michael O. Rabin in 1979. The Rabin Signature Scheme

was one of the first digital signature schemes proposed, and it was the first to relate the hardness of forgery directly to the problem of integer factorization.

- In cryptography, the **Boneh-Lynn-Shacham signature scheme** allows a user to verify that signer is authentic. The scheme uses a pairing function for verification and signatures are group elements in some elliptic curve.

III. GROUP SIGNATURE TECHNOLOGY

Group signature schemes are an important building block for many security applications. In contrast to ordinary signature schemes where there is only one signer, group signature schemes allow any member of a group of signers to sign documents on behalf of the group. In general, a *group manager* controls the group membership and issues *group signing keys* to group members. The group signing keys allow a group member to sign documents on behalf of the group. In particular, a group signature scheme provides anonymity and unlinkability to the signer, i.e. everybody can verify that the signature is valid on behalf of a group, but nobody except for the group manager can identify the signing member. Furthermore it is computationally hard for anybody but the group manager to decide whether two different valid signatures were generated by the same group member. These attractive security properties make group signature schemes appealing to applications such as electronic voting, electronic auctions and many applications where it is desirable to hide organizational structure. Group signature schemes are also used in electronic cash systems to conceal the cash-issuing banks' identities and identity escrow systems

A. Concept of group signature:

There are three participants in this scheme which are as follows:

- **Group Manager:** The manager of group for managing the memberships and generating the membership keys of group members (Signers). Group Manager enabling signers to sign on behalf of the group, and revealing the identity of the signature's originator when dispute.
- **Group Member:** The group member, he/she have his/her membership key, and he/she can using the membership key to sign message on behalf of the group.
- **Verifier:** Receiver of group signature or anyone can check the validity of the group signature by the public key of group.

A group signature scheme consists of the following four procedures:

- **Setup:** a probabilistic interactive protocol between a designated group manager and the members of the group. Its result consists of the group's public key Y, the individual secret keys x of the group members, and a secret administration key for the group manager.
- **Sign:** a probabilistic algorithm which, on input a message m and a group member's secret key x, returns a signature s on m.
- **Verify:** an algorithm which, on input a message m, a signature s, and the group's public key Y, returns whether the signature is correct.
- **Open:** on input a signature s and the group manager's secret administration key this algorithm returns the identity of the group member who issued the signature s together with a proof of this fact.

It is assumed that all communications between the group members and the group manager are secure.

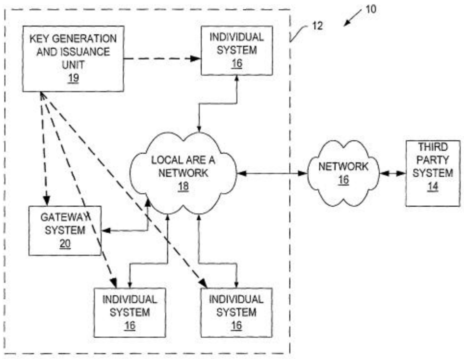

Fig 2: Group Signatures [27]

B. Properties and Keys used in group signature:

A group signature scheme must satisfy the following properties:

- Only group members are able to correctly sign messages **(unforgeability)**.
- It is neither possible to find out which group member signed a message **(anonymity)** nor to decide whether two signatures have been issued by the same group member **(unlinkability)**.
- Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so **(security against framing attacks)**.

A consequence of the last property is that the group manager must not know the secret keys of the group members.

There are three types of key are used in this scheme as:

- **Master Public Key:** anyone who knows this key can verify that some group member has signed the message..
- **Master Secret Key:** given to all group members for signing of messages.
- **Administrative Key:** only known to manager to identify that which group member has signed the message.

C. Previous work done and analysis in group signature:

Group signature can be used to conceal organizational structures. For example, an employee of a company can use group signature to sign document on behalf of the company. In this situation, it is sufficient for a verifier to know that some behalf of the company has signed. Verifier does not need to check whether the employee is allowed to sign document on behalf of the company. Chaum and Heyst proposed four schemes. There are only one scheme corresponding the anonymity of information theoretic and others just achieving the anonymity of computational. Some of their schemes do not allow a group manager to add group member after the initial setup. These schemes are non-flexible and not corresponding the actual requirement. And, some of their schemes need the group manager to contact each member in order to open a signature when dispute. The schemes are not have efficiency and not corresponding the actual necessary [8]. A member of improvements and enhancements followed the initial work. In 1994, Chen and Pedersen proposed two new schemes. These schemes allow the addition of new member after the initial setup of the system and the distribution of the function of the functionality of the group manager. However, one of their schemes is corresponding the anonymity of information theoretic and the other just achieving the anonymity of computational. Furthermore, their schemes have the drawback that the group manager can falsely accuse a group member of having signed a message. In summary, the group manager can forge a signature [9]. Besides, there is some new group signature schemes were to be proposed, continually. In 1997, Camenish proposed a efficient group signature scheme. This scheme allows the addition of new members after the initial setup and also achieves the anonymity of the computational. Furthermore, the function of the group manager can be split for several people to achieve load balance. But, this scheme has an important flaw where the size of the group's public key and the length of signatures have increasing with the adding of the group members. Hence, if the member of group is increasing, then the capital and computation also increased. This problem is improved by Camenisch and Stadler in 1997. Their scheme is an efficient group signature scheme and the size of group's public key and the length of signatures, as well as the computational effort for signing and verifying, is independent of the number of group members. Moreover, the public key maintains unchanged if new members are added to the group. But their scheme also has a flaw; it cannot avoid the Coalescent quasi attacks. Some of valid group members can cooperate to generate a group signature and make the group manager cannot to find the identity of the signer [4] [6]. This flaw was proposed by Ateniese and Tsudik in 1999. But this attack only appears in some special cases. In accordance with the flaw, Camenisch proposed an improved scheme in 2000. This scheme make the size of group's public key and length of signatures are independent of the number of group members. This scheme also corresponds the requirements and security of necessary [13] [2]. In general, the scheme proposed by Camenisch is more efficient and secure than previous scheme. But it does not have the deletion function when group member must leave the group. In fact, this problem also has many people to strive, including the Kim and Bresson. Kim added the deletion function in Camenisch and Michel's scheme [25]. On the other hand, Killan and Petrank also indicate the concept of separability. That is, if the group manager is split into a membership manager and a revocation manager, the revocation manager and the membership manager work in concert to open the identity of the signer. But they did not propose any group signature scheme to achieve this function. In 2002, Xia and You proposed a group signature scheme with strong separability. That is, the revocation manager can work without the involvement of the membership manager. But in 2003, Wang point out that Xia and You's scheme does not satisfy unlinkability and unforgeability [12] [19]. Besides, Park proposed an ID based group signature scheme which is based on Ohta and Okamoto's scheme and Schoenmarker's method. However, their scheme has some flaws. It is all of previous group signature signed by other members will be invalid if the group is changed, and the length of a group signature is dependent upon the number of group members. In 1999, Tseng and Jan tried to solve the problem. Hence, they proposed a novel ID based group signature scheme. Unfortunately, their scheme has been proved to be universally forgeable in 1999. That is, everyone is able to produce a valid group signature on an arbitrary message, which cannot be traced by the group manager [14] [15]. In 1998, Lee and Chang proposed an efficient group signature scheme based on discrete logarithm problem. However, some scholars pointed out their scheme is insecure. Then, Tsang and Jan proposed two improvement group signature schemes in 1999, respectively. But, their scheme also does not satisfy unlinkability and unforgeability. In 2002, Shi also improved Lee and Chang's scheme. Unfortunately, Zhang pointed out that Shi's scheme is still insecure [16] [17]. The development of group signature scheme is starting with added the necessary properties. When Camenisch and Stadler proposed a group signature scheme to solve the problem that the size of the group's public key and the length of signature are development of the number of group members. Then, the research of group signature was getting into a new state. Recently, group signature scheme focus on adding new processes such as revocation procedure.

D. Requirements of group signature:

Many schemes have been proposed, however all should follow these basic requirements:

- **Unforgeability:** Only group members can issue valid signatures on behalf of the entire group; i.e. only group members can issue signatures that are verifiable by the group public key.
- **Conditional Signer Anonymity:** Anyone can easily check that a message /signature pair was signed by some group member, but only the group manager can determine which member issued the signature. There is also a slightly different model which one might want to consider in which the signer's anonymity is always retained, even with respect to the group manager, but this is not the model we consider in this thesis.
- **Undeniable Signer Identity:** The group manager can always determine the identity of the group member who issued a valid signature. Moreover, he can also prove to some other entity (such as a judge) which member signed a given document without compromising that particular group member's anonymity in previous or future messages he may sign.
- **Unlinkability:** Determining if two different signatures were computed by the same group member is

computationally infeasible for everyone but the group manager.

- **Security against Framing Attacks:** No subset of group members (perhaps including the group manager) can sign a message on behalf of another group member. That is, if the Open procedure is invoked on the message, it should not specify the name of another group member not belonging to the original subset.
- **Coalition Resistance:** No subset of group members (perhaps including the group manager) should be able to collude and generate valid group signatures that are untraceable. In particular, we want to prevent attacks in which a coalition of group members get together, pool their information, and generate signatures which are approved by the Verify procedure, but for which the Open procedure fails to reveal any group member.
- **Exculpability:** Neither a coalition of group members nor the group manager can generate signatures that will be opened by the OPEN procedure as generated from another group member. This means a group member cannot be blamed to have generated a signature that he actually did not generate.
- **Traceability:** A trusted entity can always open a valid signature using the OPEN procedure and identify the actual signer. This trusted entity can either be the group manager or some other entity, usually called the revocation manager. For simplicity we assume this trusted entity is the group manager in this case. If a separate entity is desired, the scheme can be easily adapted to support a separate revocation manager.
- **Soundness and Completeness:** Valid signatures by group members always verify correctly, and invalid signatures always fail verification.
- **Revocability:** The group manager can revoke a group member so that this group member cannot produce a valid group signature any more after being revoked.
- **Unforgeable tracing verification:** The revocation manager cannot falsely accuse a signer of creating a signature he did not create.
- **Distinguishable:** Due to different member group signature keys are different and each group private key is unique, so we can distinguish group members according to their corresponding private keys.
- **Non-repudiation:** Once a member makes his signature, the synthesis mapping *T* will contain his private key. Each group private key is unique and only the members have their own private keys. Therefore, no one can deny the signature once he made the signature.

IV. APPLICATIONS OF GROUP SIGNATURE

There are various possible applications of group signature in which the concept of group signature scheme helps out which are as follows:

- A company has several computers, each connected to the local network. Each department of that company has its own printer (also connected to the network) and only persons of that department are allowed to use their department's printer. Before printing, therefore, the printer must be convinced that the user is working in that department. At the same time, the company wants privacy: the user's name may not be revealed. If, however, someone discovers at the end of the day that a printer has been used too often, the director must be able to discover who misused that printer, to send him a bill.
- They can be used in invitations to submit tenders. All companies submitting a tender form a group and each company signs its tender anonymously using the group signature. Once the preferred tender is selected, the winner can be traced while the other bidders remain anonymous.
- A further application of a group signature scheme is electronic cash. In this case, several banks issue coins, but it is impossible for shops to find out which bank issued a coin that is obtained from a customer. The central bank plays the role of the group manager and all other banks issuing coins are group members.
- An English auction is another application of group signature which allows one seller to offer an item for sale. Many potential buyers then submit bids for the item attempting to outbid each other. The winner is the bidder with the highest bid after a given time-out period where no bid higher than the current highest bid has been made. The winner must pay the seller an amount equal to the winning bid.
- Another application is the Trusted Computing effort, where a computing device is required to authenticate as proper (i.e., secure) device, i.e., that it has obtained attestation by some third party. To protect privacy of the device’s user, this authentication should not allow identification of the device. In fact, the protocol standardized by the Trusted Computing Group to achieve this uses the Ateniese et al. group signature scheme but without its anonymity revocation feature.
- Vehicle Safety Communications (VSC) system is another application. The system embeds short-range transmitters in cars; these transmit status information to other cars in close proximity. For example, if a car executes an emergency brake, all cars in its vicinity are alerted. To prevent message spoofing, all messages in the system are signed by a tamper-resistant chip in each car. (MACs were ruled out for this many-to-many broadcast environment.) Since VSC messages reveal the speed and location of the car, there is a strong desire to provide user privacy so that the full identity of the car sending each message is kept private. Using group signatures, where the group is the set of all cars, we can maintain privacy while still being able to revoke a signing key in case the tamper resistant chip in a car is compromised. Due to the number of cars transmitting concurrently there is a hard requirement that the length of each signature be under 250 bytes.
- Another application is as follows: Company A buys product from company B, but he does not know whether price is reasonable or not. Thus, ask company B to give them a menu. And then, personnel in company B send a

new menu and produce a group signature for it on behalf of company B to sell the products to company A by the price on the menu. After company A receives the menu and the group signature, it can verify whether they are matched and valid message sent by company B. if verification is passed, company A will believe the menu that is indeed quoted a selling price by company B. But company A does not know the identity of signer from beginning to end. Assume after company A reads the menu, he thinks the price is cheap and then orders product from company B. When the company A pays the money to company B, company A discovers the bill is higher than the menu price. Thereupon, company A takes the menu and group signature to prove that he is right. And after company B makes sure, he discovers that his own personnel makes mistake. And then, the group manager of company B exposes the identity of signer and asks them to deal with it.

- Another application is for keycard access to restricted areas where it is inappropriate to track individual employee's movements, but necessary to secure areas to only employees in the group.
- Biometric-based authentication schemes are also an application which works on group signature scheme and has four components: Human user H, who uses his biometric data to authenticate himself to a service provider. Sensor client S, which extracts human user's biometric trait using some biometric sensor and communicates with the service provider. Service provider P, who deals with human user's authentication request, granting access or not. Card Issuer I, who holds two master secrets,: U which is needed to derive keys in the scheme and V which is the private key only used in case of legal warrant, with W the corresponding public key.
- Electronic toll pricing system is another application of group signature. Electronic Toll Pricing (ETP) systems, by collecting tolls electronically, aim to eliminate delays due to queuing on toll roads and thus to increase the throughput of transportation networks. Since Norway built the first working ETP system in 1986, ETP systems have been implemented worldwide. Nowadays, by exploiting the availability of free Global Navigation Satellite Systems (GNSS), traditional ETP systems are evolving into more sophisticated location-based vehicular services. They can offer smart pricing, e.g., by charging less who drive on uncongested roads or during off-peak hours.

V. GROUP SIGNATURE ATTACKS

There are various attacks imposed on different group signature schemes which will be described here as follows:

- **Meet-in-the-middle attack:** This type of attack can be used for forging signatures on mixed-type digital signatures schemes, and takes less time than an exhaustive attack. This has been analyzed that an optimal strategy for forgers to apply this attack, pointing out that an intermediate value of 64 bit length is not secure for any mixed-type digital signatures scheme.
- **Forgery attack:** Shi's group signature scheme is not secure; Fangguo Zhang and Kwangjo Kim propose a universal forgery attack of this group signature scheme against the known-message attack [18].
- **Unforgeability attack:** This is another attack which should be possible on group signature scheme. It has been proved that the scheme is universally unforgeable; namely, anyone can forge a valid group signature on another message by a valid signature. Unforgeability is the basic property of group signature. This property is a primitive condition of group signature which be used in electronic commerce.
- **Unlinkability attack:** Unlinkability is an important property of group signature which is distinguished from other signature types. Unlinkability means that, given two group signatures, it is hard to distinguish whether the two group signatures were produced by the same signer. It has been proved that Zhang et.al's signature does not satisfy unlinkability [20].
- **Conspiracy attack:** Conspiracy attack against group signature, put forward by Taiwan scholar Li C.M, means that malicious members can recover the secret polynomials to obtain group private key under their conspiring in order to impersonate others signature irresponsibility. Many scholars have done a lot of works to resist conspiracy attack, but the conspiracy attack has always been difficult to solve in group signature system.
- **Coalition Quasi-Attack against CS97:** A coalition attack happens when some collection of group members (possibly including the group manager) collude and combine their secret membership keys in such a manner that they can generate a valid, yet untraceable group signature for a particular message. These signatures are untraceable in the sense that the Open procedure will fail to identify a particular group member when given this message and signature pair as input. A potentially more dangerous attack is one where some coalition can get together and fraudulently generate a signature that appears to be from some other member of the group [21].

VI. CHALLENGES AND EFFICIENCY OF GROUP SIGNATURE

A. Challenges of group signature:

There are lots of challenges in group signature which we will try to cover under this category as follows:

- Exposure of secret keys for non-cryptographic” reasons, such as a compromise of the underlying storage system or human errors, are one of the greatest threats to many cryptographic protocols in practice. In group signature schemes, if a group member's group signing key is exposed to an attacker, the attacker can then sign any documents on behalf of the group. And the danger of the exposure of signing keys escalates as the group size increases.
- Any practical group signature scheme must support dynamic group membership. In practice, group members

may join, leave, or be excluded from the group during at any time. Previous group signature schemes can support group member joins efficiently, but not group member exclusion events.

- In Delay-Tolerant Networks (DTNs), security and efficiency are paramount concerns for data transmission. To enhance efficiency, message ferries were introduced to DTN, which commonly builds up a new class of DTN, i.e., the Ferry-based DTN (FDTN). However, although several message ferry-based approaches were proposed to improve the message efficiency, none of them was able to handle the severe security challenges caused by Ferries.
- Any proposed scheme that based on group signature must satisfy all of their requirements like anonymity, unlinkability, unforgeability, traceability, revocability etc. This is the major challenge in this respect as every scheme has some flaws as they do not meet the requirements.

B. Efficiency of group signature:

The following parameters are of interest when evaluating the efficiency of a particular group signature scheme:

1. The size (number of bits) of the group public key Y.
2. The size (number of bits) of an actual group signature on a message.
3. The efficiency of the Setup, Sign, Verify, and Open protocols.

VII. CONCLUSION

In this paper, we have presented various aspects of group signature like overview, properties, keys, applications, and challenges. Apart from it, a brief and comparative analysis of group signature techniques is presented with their advantages and disadvantages which can help the new researchers in related areas. We also tried to present various types of attacks on group signature and requirements for this technique. In this paper we tried to give the complete information about the group signature which will help the new researchers to get the maximum knowledge in this domain.

REFERENCES

[1] D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In V. Atluri, B. Pfitz-mann, and P. D. McDaniel, editors, ACM Conference on Computer and Communications Security, ACM, 2004.

[2] G.Ateniese, J.Camenisch, M.Joye, and G.Tsudik, "A Practical and provably secure coalition-resistant group signature", in Advances in Cryptology 2000.

[3] Q.L.Xu. A Modified Threshold RSA Digital Signature Scheme. Chinese Journal of Computer, 2000.

[4] J. Camenisch, "Efficient and generalized group signatures", in Advances in Cryptology, Euro Crypto 1997.

[5] Sun Huihui, Chen Shaozhen. An Efficient Forward Secure Group Signature Scheme with Revocation. JOURNAL OF ELECTRONICS, 2008.

[6] J. Camenisch and M.Stadler, "Efficient group signature scheme for large groups", in Advances in Cryptology, Crypto 1997.

[7] J. Camenisch and M. Michels, "Separability and efficiency for generic group signature schemes". In M. Wiener, editor, Advances in Cryptology, CRYPTO 1999.

[8] D. Chaum and E. Heyst, "Group Signatures", in Advances in Cryptology, Euro crypt, 1991.

[9] L. Chen and T.P. Pedersen, "New Group Signatures", in Advances in Cryptology, Euro crypt 1994.

[10] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of rsa functions. In Advances in Cryptology, 1996.

[11] Y. Wang, J. Zhang and X. Chen, "Security analysis of the improved group signature", Information Theory Workshop 2003.

[12] M.K. Franklin and M.K. Reiter, "The design and implementation of a secure auction service", IEEE Transactions on Software Engineering, 1996.

[13] G. Tsudik, G. Ateniese, "Some open issues and new directions in group signatures", in Advances in Cryptology Crypto 1999.

[14] G. Tsudik and G. Ateniese, "Quasi-efficient revocation of group signatures", in To Appear in Financial Cryptography, 2002.

[15] M. Harkavy, H. Kikuch and J.D. Tygar, "Electronic auction with private commerce", in Proceedings of the 3rd USENLX Workshop on Electronic Commerce, August 1998.

[16] L. Harn and Y.Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm", Electronics Letters, 1994.

[17] W.H. He, "Digital signature scheme based on factoring and discrete logarithms", Electronics Letters, 2001.

[18] Fangguo Zhang and Kwangjo Kim, "Security of A New Group Signature Scheme", IEEE TENCON'02

[19] E. Petrank J. Kilian, "Identity Escrow", in Advances in Cryptology Crypto 1998.

[20] Jianhong Zhang and Jiancheng Zou, "On the Security of a Constant-Size Group Signature Scheme" in Advances in Cryptology 1998.

[21] Zulfikar Amin Ramzan, "Group Blind Digital Signatures: Theory and Applications" in Advances in Cryptology 1999.

[22] C. Popescu, "Group signature schemes based on the difficulty of computation of approximate e-th roots", Proceedings of Protocols for Multimedia Systems, 2000.

[23] Trevathan, J., Ghodosi, H. and Read, W. "Design Issues for Electronic Auctions", in 2nd International Conference on E-Business and Telecommunication Networks, 2005.

[24] Ming-Te Chen, Chun-I Fan, Wen-Shenq Juang and Yi-Chun Yeh, "AN EFFICIENT ELECTRONIC CASH SCHEME WITH MULTIPLE BANKS USING GROUP SIGNATURE", International Journal of Innovative Computing, Information and Control, July 2012

[25] H.J. Kim, J.I. Lim and D.H. Lee, "Efficient and secure member deletion in group signature schemes", Proceeding of the Third

International Conference on Information Security and Cryptology 2001.

[26] N. Asokan, P. A. Janson, M. Steiner and M. Waidner, The state of the art in electronic payment systems, IEEE Computer, 1997.

[27] http://www.freepatentsonline.com/7093133.html (Last used on 9/4/2013)

[28] http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html "Chapter 9. Fundamental Security Concepts", (Last used on 9/4/2013).

AUTHOR'S PROFILE

Mr. Aayush Agarwal received his B.Tech in IT from G.B.T.U Lucknow, Uttar Pradesh, India in 2010.Currently, he is doing M.Tech in IT from C-DAC Noida(Affiliated to G.G.S.I.P.U New Delhi), India. He is working on the project **"Group Signature Scheme for Online Bidding".** His interest areas are Cryptography and Network Security, Operating Systems, and DBMS.

Ms Rekha Saraswat is a Sr. Lecturer in CDAC, Noida (Affiliated to G.G.S.I.P.U New Delhi), India. She has 10 years of expertise in the field of teaching. Her area of interests are Computer networks, Object oriented software engineering and Operating system.