

# Group Signature Scheme Resistant against Colluding Attack

Vinay Iyer



Department of Computer Science and Engineering  
National Institute of Technology Rourkela  
Rourkela-769 008, Odisha, India

# Group Signature Scheme Resistant against Colluding Attack

*In partial fulfillment of the requirements*

*for the degree of*

***Master of Technology***

*by*

***Vinay Iyer***

*(Roll 211CS2277)*

*under the supervision of*

***Prof. Sujata Mohanty***



Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India



Computer Science and Engineering  
**National Institute of Technology Rourkela**  
Rourkela-769 008, India. [www.nitrkl.ac.in](http://www.nitrkl.ac.in)

June 1, 2013

## Certificate

This is to certify that the work in the thesis entitled *Group Signature Scheme Resistant against Colluding Attack* by *Vinay Iyer*, bearing roll number 211CS2277, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology in Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

*Prof. Sujata Mohanty*

# Acknowledgment

Apart from the efforts of me, the success of any project depends largely on the encouragement and guidelines of many others. I offer my enduring gratitude to the faculty, my fellow students, who have inspired me to continue my work in this field.

My first and sincere appreciation goes to Prof. Sujata Mohanty, my supervisor for all I have learned and the continuous help and support in all stages of this thesis. I would also like to thank for being an open person to ideas and for encouraging and helping me to shape my interest and ideas.

I would like to express my deep gratitude and respect to Prof. Bansidhar Majhi and Prof. Sanjay Kumar Jena whose advices and insight was invaluable to me. For all I learned from them, and for providing the vision for the success of project. Their attitude to research inspired me to continue to the master's work and made me a proud member of the academic family of research.

I would like to thank my family, relatives and friends, especially my mother and father for always believing in me, for their continuous love and their supports in my decisions and my elder brother vivek raman who has always being an inspiring role for me in life and without whom I could not have made it here.

In the end, I would like to extend my thanks to our Head of Department, Prof. Ashok Kumar Turuk for valuable advice and encouragement with providing me the resources that I used for this research. The guidance and support received from all the members who contributed and who are contributing to this project, was vital for the success of the project. I am grateful for their constant support and help.

*Vinay Iyer*

# 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. Group signature can have wide application to corporate world, banks, and e-commerce applications.

In this thesis, we designed a group signature protocol 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. Full traceability feature is confirmed in the proposed scheme. The scheme can have wide applications in real life scenarios such as e-banking, e-voting, and e-commerce applications.

**Keywords:** anonymity; colluding attack; discrete logarithm; group signature; unforgeability

# Contents

<b>Certificate</b>	<b>i</b>
<b>Acknowledgment</b>	<b>ii</b>
<b>Abstract</b>	<b>iii</b>
<b>List of Figures</b>	<b>vii</b>
<b>List of Tables</b>	<b>viii</b>
<b>1 Introduction</b>	<b>2</b>
1.1 Basic Concepts and Requirement Of Group Signature . . . . .	3
1.2 Colluding Attack in Group Signature . . . . .	5
1.2.1 Defining Collusion . . . . .	5
1.2.2 Roles under The Colluding Attack . . . . .	6
1.2.3 Consequences of Colluding Attack . . . . .	7
1.3 Application of Group Signature . . . . .	7
1.3.1 Voting System . . . . .	7
1.3.2 Sales and Bidding System . . . . .	7
1.3.3 Corporate Organisation . . . . .	8
1.4 Motivation and Objective . . . . .	8
1.5 Problem Statement . . . . .	8
1.6 Organization of Thesis . . . . .	9
<b>2 Literature Survey</b>	<b>11</b>
2.1 Cryptography Concepts and Signature Requirements . . . . .	11

2.1.1	Discrete Logarithm Problem (DLP)	12
2.1.2	Cryptographic Hash Function	12
2.1.3	Random Number Generator	13
2.1.4	Prime Numbers and Primality Test	13
2.2	Classification of group signature schemes	14
2.2.1	Static Group Signature	14
2.2.2	Dynamic Group Signature	15
2.2.3	Group Signature with Verifiable Opening	15
2.2.4	Group Signature with Distributed Roles	16
2.3	Literature review of Group signature schemes	16
2.3.1	Group Signature based on DLP	16
2.3.2	Group Signature with anonymity and separability	17
2.3.3	Group Signature based on Threshold Scheme	18
2.3.4	Short Group Signature	19
2.4	Chapter Summary	19
<b>3</b>	<b>Group signature scheme resistant against colluding attack</b>	<b>22</b>
3.1	Proposed Scheme	22
3.1.1	Setup phase	22
3.1.2	Join phase	23
3.1.3	Signature generation phase	24
3.1.4	Verification phase	24
3.1.5	Open phase	25
3.2	Chapter Summary	25
<b>4</b>	<b>Security Analysis of Proposed Scheme</b>	<b>27</b>
4.1	Security analysis of the proposed scheme	27
4.2	Performance analysis of the proposed scheme	31
4.3	Chapter Summary	32
<b>5</b>	<b>Implementation and Results</b>	<b>34</b>
5.1	Implementation	34

6 Conclusion and Future Work	39
Bibliography	40
Dissemination of Work	43



# List of Figures

1.1	Layout of standard group signature system . . . . .	4
1.2	Scenario of collusion attack . . . . .	6
3.1	Layout of the proposed scheme . . . . .	23
3.2	Join phase of the proposed scheme . . . . .	24
5.1	Setup phase of the proposed scheme . . . . .	35
5.2	Join phase of the proposed scheme . . . . .	36
5.3	Signature generation and verification phase of the proposed scheme	37

# List of Tables

4.1 Performance comparison . . . . .	31
--------------------------------------	----

# **Chapter 1**

**Introduction**

# Chapter 1

## 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 [11]. 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.

Following the first schemes 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 sig-

nature 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 [4]. Later, Kim et al. extended their scheme to support efficient member revocation. 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 [13].

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, [7,25] 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.

## 1.1 Basic Concepts and Requirement Of Group Signature

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 Figure 1.1. 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. The concept of group signature was first proposed by Chaum and Heyst that allows any member of a group to sign message on behalf of a group. According to the Chaum and Heyst, 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.

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 have following five phases[18]:

- 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.

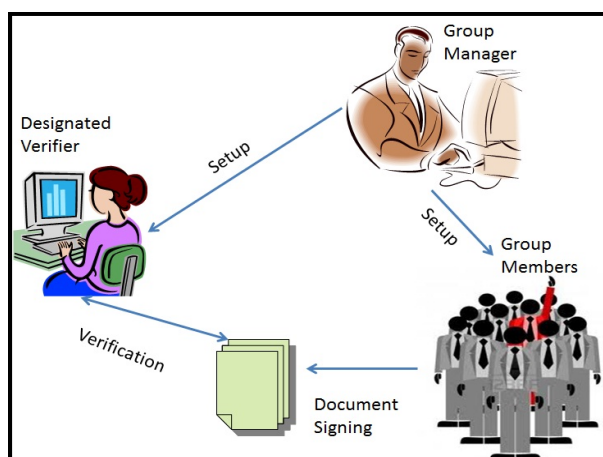


Figure 1.1: Layout of standard group signature system

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.
- Unforgeability: 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.

## 1.2 Colluding Attack in Group Signature

### 1.2.1 Defining Collusion

Collusion as the name suggest is a 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 observed in figure below. 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 colluders, according to the type of content and the kind of adopted protection system.

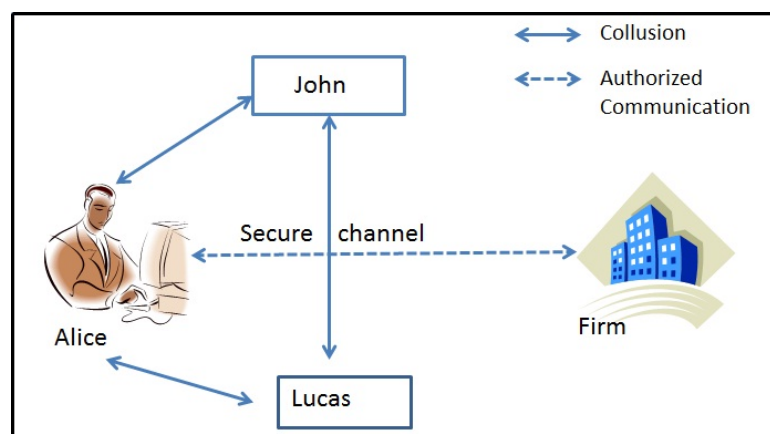


Figure 1.2: Scenario of collusion attack

### 1.2.2 Roles under The Colluding Attack

The Colluding attack has another flavor with small variation ie stated as coalition. The coalition can be thought of subpart of collusion where a set of member collide to achieve the respective objective. Coalition is another security threat basically discussed with respect to the group. so if we consider the security part for collusion, then coalition can be avoided. In general, the group signature involves the group manager who is responsible in distributing many security parameter between members, which is a very critical role where collusion is possible, secondly the group member who are responsible in signing the documents can also collude which makes the member very critical issue and finally the verifier who is responsible for verifying the signature in the document can also collude which can create a threat to the integrity of the document. Above all discussed roles were involved in the system, but a non group member or a set of non group members can also collude with the group member which can be huge threat to the real time system. So to avoid or to resist the colluding attack one must consider all possible roles



in the system, but one can avoid this attack up to a certain limit because of the unpredictable nature of different roles in system of secure communication.

### **1.2.3 Consequences of Colluding Attack**

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. The whole strength of secure system lies in the trust and security parameters used in the system, So considering the consequences of colluding attack, if collusion is possible then the signature can be easily forged crashing whole system of signing the document thus a threat to the security of digital information or message.

## **1.3 Application of Group Signature**

### **1.3.1 Voting System**

E-voting also known as electronic voting collectively means to cast vote and count the votes electronically. E-voting is physically supervised by representatives of governmental or independent electoral authorities where group signature would be beneficial. Voting is also performed within the voter's sole influence, and is not physically supervised by representatives of governmental authorities where the authorization plays a vital role as trusted party is needed to govern the voting scheme, in such case group signature can be best applicable.

### **1.3.2 Sales and Bidding System**

Electronic commerce, commonly known as e-commerce, is a type of industry where buying and selling of product or service is conducted over electronic systems such as the Internet and other computer networks. It consists of the exchange of data to facilitate the financing and payment aspects of business transactions. Group signature is effective and efficient way of providing security in communicating within an organization.

### 1.3.3 Corporate Organisation

Any organisation well developed consist of many roles working for the particular objective to be achieved which comprises of vital information to be shared between them, thus group signature proves to be efficient way to authorise the information among everyone and saving the valuable time with a reliable approach.

## 1.4 Motivation and Objective

We are very much aware of digital signature and its benefits regarding the security of information, so extending the idea of digital signature into group where multiple documents or information can be authorised in parallel and time saving system. The group signature was introduced in early 90's but 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 work is motivated from the previous scheme developed where collusion resistant was not a centralised idea of securing the information or documents, thus a safe and secure group signature scheme where all the condition can be efficiently satisfied and providing better security, performance compared to other group signature schemes.

## 1.5 Problem Statement

The Objective of thesis is to design a group signature scheme based on following assumptions:

1. Group signature scheme based upon hard computational assumptions, such as, discrete logarithm problem (DLP) and computational Diffie Hellmann (CDH) problem.
2. Group signature scheme must be unaffected by joining or leaving of any member.

3. Group signature scheme must be resistant against colluding attack, which enhances unforgery against compromised group of members.
4. Group signature scheme must satisfy security features such as anonymity, traceability, and unlinkability.

## **1.6 Organization of Thesis**

This thesis is organized as follows, Chapter 2 gives a brief introduction of preliminary of thesis. The proposed scheme is described in Chapter 3. Security analysis and performance evaluation of proposed scheme is done in Chapter 4. Discussion about implementation and result is depicted in Chapter 5. Finally we conclude with future work in Chapter 6.

# **Chapter 2**

## Literature Survey

# Chapter 2

## Literature Survey

In this section, we reviewed the literature related to various group signature schemes and their security features. First, we give a brief overview of cryptography concepts then preliminaries related to discrete logarithms, hash functions, random number generations, and prime number with primality test. Later, we reviewed some popular group signature schemes based on security features.

### 2.1 Cryptography Concepts and Signature Requirements

Cryptography can be defined as protecting information by transforming into an unreadable format, called cipher text. Only those who possess a secret key can decipher the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses, but in case of the signature needs a public key system where the signer signs with private key and the verifier verifies with the signer's public key.

### 2.1.1 Discrete Logarithm Problem (DLP)

Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups[30]. 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

$$\log_b(a) = n, \text{ if and only if } a = b^n \quad (2.1)$$

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  $n$ .

### 2.1.2 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[31]. 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.

### 2.1.3 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[32]. 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.

### 2.1.4 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[35]. 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 absolute certainty 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 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.

## 2.2 Classification of group signature schemes

The classification of group signature protocol can be described in four types ,firstly Static Group signature, secondly dynamic group signature with revocation, thirdly group signature scheme with verifiable opening with the consideration of PKI explicitly and finally group signature scheme where group manager can be distributed among different role. The basic functionality of this classification follows the standard group signature scheme as generation of secret and public keys, generating the group key, signature generation from group, designated verification and opening of group signature.

### 2.2.1 Static Group Signature

Static group signatures consist of four polynomial time algorithm[27] 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.



### 2.2.2 Dynamic Group Signature

Dynamic group signature [22] as the name suggests the randomness and non-deterministic nature of scheme. 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 signature, 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.

### 2.2.3 Group Signature with Verifiable Opening

The distinguished property of signature is to preserve signers 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 algorithm as the dynamic group signature but the difference here comes in the open procedure, where the algorithm is divided into two procedure 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 outputs the identity if accused with proof. In judgement procedure, algorithm takes the proof and signature and reveals the validity of managers signature proving to

be verifiably open procedure.

### 2.2.4 Group Signature with Distributed Roles

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 membership 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 verifiably 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.

## 2.3 Literature review of Group signature schemes

### 2.3.1 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 [6]. 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 the group member changes, 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[18]. 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-Chang scheme[8]. In the same year, Sun showed in that the Tseng-Jan scheme is still not unlinkable. After that, Tseng-Jan [9] proposed to improve their scheme.

In 2000, Li et al.[2] demonstrated that two schemes of the Tseng-Sun's paper, which are called TJ1 and TJ2 in Li et al's paper, 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.

### **2.3.2 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 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 conflict of authenticated content[26].In 2009, a new improved group signature was introduced by Cheng Lee et al. where the problem of unlinkability and unforgeability was enhanced based on the discrete logarithm.

### 2.3.3 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 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, 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 realise a real group signature, which is based on pivot threshold scheme[7].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.

### 2.3.4 Short Group Signature

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 Dan Boneh 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).

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, Shi and Zang, including both dynamic groups, concurrent join and proposed extremely dynamic short signature scheme with strong security under random oracle assumption[23]. 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 [(Jung Yeon Hwang, Chung, Cho, & Nyang, 2011 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. 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.

## 2.4 Chapter Summary

The review of group signature gives us the idea of enhancement of signature scheme with various security features to be applicable in real time application, but due to the complexities and active attacks analyzed, has failed the scheme to be fully applicable. The most unpredictable attack is the colluding attack where the sig-

nature schemes proposed, considers only the features that are predictable. Thus reviewing the schemes proposed till now, we propose a new scheme that is centrally based on avoiding the colluding attack.

# **Chapter 3**

**Group Signature Scheme**

**Resistant against Colluding Attack**

# Chapter 3

## Group signature scheme resistant against colluding attack

We propose a novel group signature scheme which provides full anonymity of signer, full traceability of the signature, resistant to colluding attack and forgery attack. A trusted third party (TTP) is an entity involved in the proposed scheme who manages all critical communications among the group members and group manager.

### 3.1 Proposed Scheme

The proposed group signature scheme consists of four participants namely, group manager, group members, designated verifier, and trusted third party. The scheme consisting of following five phases. The system model of proposed scheme is shown in Figure 3.1.

#### 3.1.1 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  $(q - 1) = 0 \text{ mod } p$  and also chooses a random private key  $Y$ . Manager also computes group key as  $g_k = (y-1)^\delta$ , where the  $\delta$  is a randomly chosen parameter.



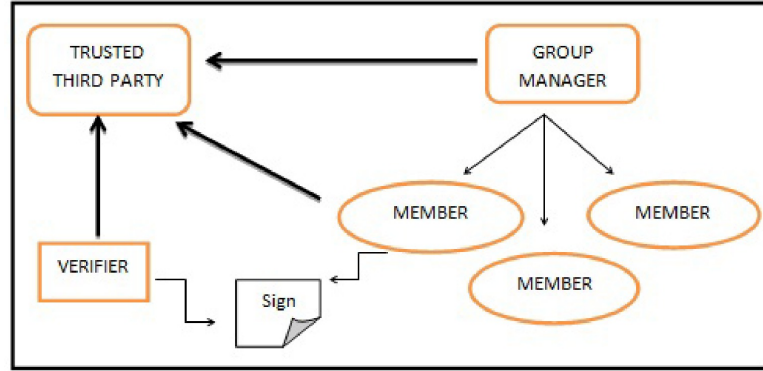


Figure 3.1: Layout of the proposed scheme

### 3.1.2 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  $d = y^\alpha \text{ mod } p$  where  $\alpha$  is randomly chosen by the group manager. Then the manager splits the secret key  $d$  into two parts as  $d_1$  and  $d_2$ . The key division can be done through any method which is appropriate to the manager. Here the manager has a flexibility to decide the splitting method but one important concern regarding the splitting is that the division should be lossless. The secret keys  $d$  and  $d_1$  are sent to each member in encrypted form using the member's public key. The key  $d_2$  is sent to the trusted third party (TTP) which manages keys of each member. Each member chooses a primitive element  $e_0$  in  $\mathbb{Z}_p$ , and computes  $e_1 = e_0^{\frac{p-1}{q}} \text{ mod } p$ . The Member chooses a secret key  $x$  and computes  $e_2 = e_1^{xd} \text{ mod } p$ .

Members are organized according to a structure as shown in Figure 3.2. 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.

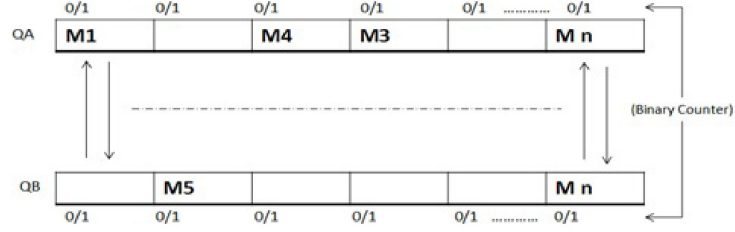


Figure 3.2: Join phase of the proposed scheme

### 3.1.3 Signature generation phase

In this phase, a member  $X_i$  chooses a random number  $\beta$  from 1 to  $q$  and computes the signature as:

$$s_1 = h(M|e_1^\beta \text{ mod } P) \quad (3.1)$$

$$s_2 = \beta + x \times (id + d_2) \times s_1 \text{ mod } q \quad (3.2)$$

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  $e_1, e_2$  are encrypted using verifiers public key and finally the message, signature with hash  $M, s_1, s_2$  along with the hash of key  $h(d_2)$  encrypted via manager's public key are finally encrypted using group key and send to the verifier. The value of  $\beta$  will vary with respect to each message.

### 3.1.4 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.

$$s' = h(M|e_1^{s_2} \times e_2^{-s_1} \text{ mod } p) \quad (3.3)$$

If the value of  $S'$  satisfies the following,  $s_1 = S' \bmod p$ , then signature is accepted otherwise rejected.

### 3.1.5 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.

## 3.2 Chapter Summary

The above work shows the working principle of our proposed scheme. Since the scheme should be efficient against active attacks, so we analyze the security and performance of our scheme with respect to the standard group signature scheme and proving that the proposed scheme is safe and secure against many active attacks.

# **Chapter 4**

## **Security Analysis of the Proposed Scheme**

# Chapter 4

## Security Analysis of Proposed Scheme

### 4.1 Security analysis of the proposed scheme

In this section, we analyze the security feature of the proposed scheme including computational efficiency. Then we prove that the proposed scheme is resistant against the colluding attack. Also, we proved that the proposed scheme satisfies the unforgeability, anonymity, verifiability, and exculpability. Then we compared the proposed scheme with some popular group signature schemes and found that our scheme has less computation overhead. Also we proved that group signature is independent of number of members in a group.

*Correctness: The group signature  $s_1, s_2$  for a message  $M$  is indeed a valid signature.*

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

$$S' = h(M|e_1^{s_2}.e_2^{-s_1} \text{ mod } p) \quad (4.1)$$

$$S' = h(M|e_1^{\beta+x(id+d_2)s_1 \text{ mod } q}.e_2^{-s_1} \text{ mod } p) \quad (4.2)$$

$$S' = h(M|e_1^{\beta+x(id+d_2)s_1 \text{ mod } q}.e_2^{-x.d.s_1 \text{ mod } q} \text{ mod } p) \quad (4.3)$$

$$S' = h(M|e^\beta \text{ mod } p) \quad (4.4)$$

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

In the following, we postulate some theorems regarding the basic security requirements:

**Theorem 1:** *It is impossible to determine the signer from two given signatures.*

**Proof:** We have two signer's signature with different message as M and N respectively. The signature produced are based on discrete logarithm problem where we have:

$$\begin{aligned} & \{M, s_1, s_2, [Mg_{pu(h(d_a))}]\}_{vkey} \\ & \{N, f_1, f_2, [Ng_{pu(h(d_b))}]\}_{vkey} \end{aligned}$$

The above scheme surely follows unlinkability as the two signatures are encrypted with verifier's key and hash or message digest is further encrypted with manager's key if the encryption is compromised, then only signature can be viewed with the digest encrypted with manager's key which will also be needed to link, thus complexity of scheme involved would reveal nothing about the signer.

**Theorem 2:** *It is impossible for any non group member to forge a valid signature  $s_1, s_2$  produced by the proposed scheme.*

**Proof:** To forge a signature of message M, the adversary must know the secret of group member to sign the message, which is surely secure with respect to the DLP assumption. Another secret is the group key which is known to group members and the verifier which makes it more secure to be forged. If forger intercepts a message M and its two signature  $s_1, s_2$ , he can find another message  $M'$ , with the same pair of signature  $M'$ , but this would not benefit the forger much as the scheme is in better position because

$$s_1 = h(M|e_1^\beta \text{ mod } p)$$

which means that the hash function is applied to the combination of message and parameter which is secret and varying. The above forging is only possible if the signature are obtained but these are already encrypted and the secret is known to member only so it is difficult to forge and it also requires computing the discrete logarithm, which is very difficult.

**Theorem 3:** *No one other than the group manager can link a signature to a group member to sign it.*

**Proof:** The key is provided by the manager which is one way hashed with the signature encrypted by the manager's key  $[Mg_{pu(h(d_a))}]$  which allows only manager to know the identity and even if the encryption is compromised, revealing the digest would not affect as the data is hashed which difficult for any adversary to know the signer's identity. The value obtained would be irrelevant for the non-group member thus providing anonymous group signature.

**Theorem 4:** *The group signature remains unaffected even if the group member leaves or joins the group.*

**Proof:** The above scheme is surely unaffected if member leaves or joins the group, as the manager provides the secret key which is independent of number of member in a group and the group key computed is based on discrete logarithm assumption which is independent of number of group member,  $g_k = (y - 1)^\delta$  so if a member leaves manger has to simply remove the key from list and ensure the same to trusted third party(TTP) and similarly if a new member joins, then secret is generated and TTP is ensured about the joining of the member in the group.

**Theorem 5:** *No one other than the designated verifier can verify the signature.*

**Proof:** The signature generated by the members are verified by the designated verifier as the verifier is registered from the certificate authority where the verifier is the only member to check the integrity of the signature as the signature parameter are encrypted via verifier's key which can be known by the verifier only.

**Theorem 6:** *No set of group member can forge a valid signature.*

**Proof:** Since the signature procedure for members are done in particular structure defined where members are organized with respect to the slot-id and each member

is assigned a binary counter, managed by trusted third party only. The security of scheme can be well understood in the cases that are discussed below. The management of member signing the document can be considered under following cases:

**CASE 1:** *Initially all the member are arranged in a structure QA or QB depending on the choice of the trusted third party.*

Here the member will be arranged into slots where each slot consist of slot id provided by the trusted third party. Now if any member is signing the document, then counter assigned to the slot are changed from 0 to 1 until signing of document is completed and the member is send to the other structure with the initial values reassigned to avoid collusion.

**CASE 2:** *If the member try to sign a document using other member's key.*

In this case if a member signs a document using other member's key, which will not be practically possible as the trusted third party has the database maintained for each member where the member key is not enough to, sign the document as trusted third party's key is also required which resist the collusion.

**CASE 3:** *The members are changed after regular interval according to the trusted third party (TTP).*

The TTP varies the member slot with respect to the slot id after regular interval providing randomness in the procedure of signing the document.

**CASE 4:** *Even the group manager or verifier is not aware of the trusted third party management.*

Here the manager's job is completed after assigning the key to the trusted third party and after there is no interaction and similarly the verifier is only concerned with verifying the document, providing transparency in the whole system of signing the document. Thus structure management is done by the trusted third party.



Now if the member colludes then they can produce a valid signature but in this case since they follow an organized structure which makes it impossible for the manager or the members to produce a valid signature i.e., if the member knows a secret of other member he cannot produce the signature as the structure provides a secret that is mapped at the time of signature, so makes it impossible for member to collude. Even the non-group member who knows the secret cannot forge the signature as each member is mapped with the slots provided that are mapped by trusted third party thus avoiding the coalition in the signature generation.

## 4.2 Performance analysis of the proposed scheme

The complexity of any signature scheme mostly depends on four operations, namely, exponentiation, multiplication, inverse operation and hash functions. So we compare well-known group signature schemes. The result of the comparison is shown in Table. In this evaluation, the time for performing modular addition and subtraction operations are ignored.

The following notations are used to analyze the performance of the schemes.

$T_E$  is the computation time requirement for modular exponentiation.

$T_M$  is the computation time requirement for modular multiplication.

$T_I$  is the computation time requirement for modular inverse operation.

$T_H$  is the computation time requirement for performing hash functions.

Table 4.1: Performance comparison

Phases	Kim's Scheme[6]	Lee and Chang's Scheme[18]	J. Zhang's Scheme[4]	Proposed Scheme
Signature generation	$3T_E + 4T_M + T_H$	$6T_E + 5T_M$	$4T_E + 5T_M + T_H$	$2T_E + T_M + T_H$
Signature verification	$3T_E + 3T_M + T_H$	$5T_E + 4T_M$	$4T_E + 2T_M + 2T_H$	$2T_E + T_M + T_I + T_H$

It is observed from table that, the computational cost of above the group signature generation and verification phase of the proposed scheme is considerably lower than the existing schemes. In the signature generation phase of the proposed scheme, one inverse operation is used. The proposed scheme is secure and. So, if security is the utmost priority, then the proposed scheme will be more advantageous.

### **4.3 Chapter Summary**

The proposed group signature scheme has being analyzed with respect security requirement which shows the correctness of the proposed scheme and the performance analysis shows that the scheme is efficient and effective with respect to the security of message integrity. Our proposed scheme has being implemented under certain assumption with various phases described above of the group signature which is shown in next chapter.

# **Chapter 5**

## **Implementation and Results**

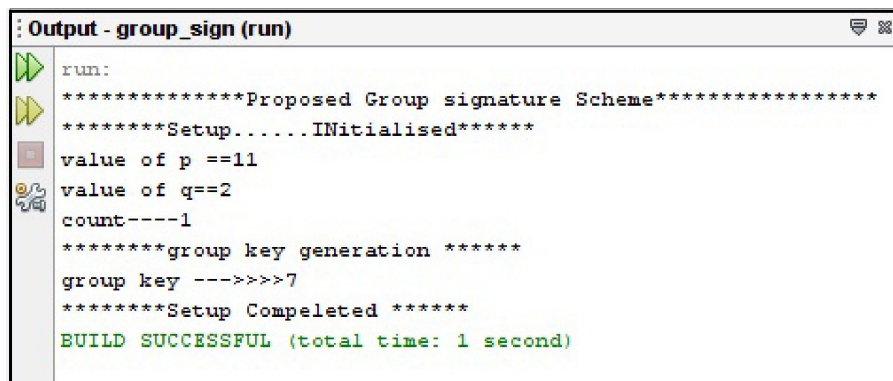
# Chapter 5

## Implementation and Results

### 5.1 Implementation

The implementation of proposed scheme is done using Java platform and Mysql as database for storing the key parameters. The proposed scheme implemented in Java Big integer values, where the Crypto and Security package are used for generating the secret key parameters for members and the hash function algorithm for signature generation phase. The random prime number generation is done using the Util package of Java. Here we have ten members in a group and the key parameter of size 512 bits and is supported by standard hardware configuration with 100 GB of hard disk and Ram size of 2 GB in windows platform system. The implementation consists of following steps in proposed scheme:

- Setup phase
- Join phase
- Signature generation phase
- Verify phase



```
Output - group_sign (run)
run:
*****Proposed Group signature Scheme*****
*****Setup.....Initialised*****
value of p ==11
value of q==2
count----1
*****group key generation *****
group key --->>>7
*****Setup Completed *****
BUILD SUCCESSFUL (total time: 1 second)
```

Figure 5.1: Setup phase of the proposed scheme

Proposed Group signature Scheme:

Setup Phase: (Computation done using Big Integer values)

Manager selects the prime number  $p = 11$

Another parameter computed  $q = 2$

Manager selects a random secret and computes the Group key  $gk = 7$

```

Output - group_sign (run)
run:
*****Proposed Group signature Scheme*****
*****Join phase initiated*****Random key of member----15722562090536181149
Secret key of member----8
*****Splitting the key*****
key of Member are----8 half key 3
key of Member for Trusted third party---- 11
*****Member parameter Computing*****
parameters of member for e1 --- 14270951998287218291
parameters of member for e2 --- 1
***** Join phase FINISHED *****

```

Figure 5.2: Join phase of the proposed scheme

Join phase:

Key generation of member[i]:

Key of member[i] —————15722562090536181149

Secret key of member —————8

Manager divides the key:

d————8

d2————3

d1————11

The key d and d2 send to member and d1 send to the trusted third party.

Member[i] parameter computation:

Member[i] calculates e1————14270951998287218291

Member[i] calculates e2————17567

```

Output - group_sign (run)
run:
*****Proposed Group signature Scheme*****
*****signature phase Initiated*****
****Enter the message****
hello this is confidential
-----Initial phase of signing
*****The signature parameters*****
The Signature S1 given as83bd9b367e6a39d9dc34e5dea47f7ad306151de9
*****The signature S2***** 1
The Second signature given as value--> 15
*****verification initiated*****
verification initiated..... 1
*****verification finished*****  hello this is confidential83bd9b367e6a39d9dc34e5dea47f7ad306151de9
BUILD SUCCESSFUL (total time: 33 seconds)

```

Figure 5.3: Signature generation and verification phase of the proposed scheme

Signature generation and verification:

Member[i] generates the signature on message:

Message-- >hello this is confidential

Signature parameters computed:

S1 signature computed----- > as83bd9b367e6a39d9dc345des47t7ad306342151de9

S2 signature computed- - - - - - - > 1523

Signature sent to the verifier with (message, S1, S2)

Verification Initiated-- >member[i] (message S1, S2)

Output of verifier

hello this is confidential

as83bd9b367e6a39d9dc345des47t7ad306342151de9 (verified)

Verification Finished.

# Chapter 6

Conclusion and Future Work



# Chapter 6

## Conclusion and Future Work

The proposed group signature scheme is secure scheme based on discrete logarithm problem assumption. The proposed scheme is proved to be resistant against colluding attack such that neither the group manager nor any set of group member can produce a valid signature of a message on behalf of a group member.

The proposed scheme satisfies standard security features like anonymity, unforgeability, and unlinkability. 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.

# Bibliography

- [1] J. Y. Hwang, S. Lee, B. . Chung, H. S. Cho, and D. Nyang. Group signatures with controllable linkability for dynamic membership. *Information Sciences*, 222:761–778, 2013.
- [2] N. . Lee, T. Hwang, and C. . Li.  $(t, n)$  threshold untraceable signatures. *Journal of Information Science and Engineering*, 16(6):835–846, 2000.
- [3] J. J. . Chen and Y. Liu. A traceable group signature scheme. *Mathematical and Computer Modelling*, 31(2-3):147–160, 2000.
- [4] J. Zhang, J. Zou, and Y. Wang. An improved group signature scheme. In *Lecture Notes in Computer Science*, volume 3592, pages 185–194, 2005.
- [5] T. Isshiki, K. Mori, K. Sako, I. Teranishi, and S. Yonezawa. Using group signatures for identity management and its implementation. In *Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-located with the 13th ACM Conference on Computer and Communications Security, CCS'06*, pages 73–78, 2006.
- [6] Y. He. New dynamic group signature scheme. *Wuhan University Journal of Natural Sciences*, 11(6):1693–1696, 2006.
- [7] L. Fengyin, Y. Jiguo, and J. Hongwei. A new threshold group signature scheme based on discrete logarithm problem. In *Proceedings - SNPD 2007: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, volume 3, pages 1176–1181, 2007.
- [8] Y. Geng, G. Shao, M. Zheng, and G. Cui. An improved efficient group signature scheme for large groups. *HuazhongKejiDaxueXuebao (ZiranKexue Ban)/Journal of Huazhong University of Science and Technology (Natural Science Edition)*, 37(7):66–69, 2009.
- [9] H. Park, S. Lim, I. Yie, K. Kim, and J. Song. Strong unforgeability in group signature schemes. *Computer Standards and Interfaces*, 31(4):856–862, 2009.
- [10] H. . Liu, W. . Xie, J. . Yu, and P. Zhang. Efficiency identity-based threshold group signature scheme. *TongxinXuebao/Journal on Communications*, 30(5):122–127, 2009.
- [11] D. Chaum and E. van Heyst. Group signatures. *Lecture Notes On Computer Science*, 547(8):257–265, 1991.

- 
- [12] 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.
- [13] Giuseppe Ateniese and Gene Tsudik. Some open issues and new directions in group signatures. pages 196–211. Springer-Verlag, 1999.
- [14] 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.
- [15] Mihir Bellare and Sara K. Miner. A forward-secure digital signature scheme. pages 431–448. Springer-Verlag, 1999.
- [16] 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.
- [17] Li-Hua Li, Chi-Yu Liu, and Min-Shiang Hwang. Cryptanalysis of an efficient secure group signature scheme. *SIGOPS Oper. Syst. Rev.*, 38(4):66–69, October 2004.
- [18] W.B. Lee and C.C. Chang. Efficient group signature scheme based on the discrete logarithm. volume 145, pages 15–18. IEE, 1998.
- [19] S.J. Park S.J. Kim and D.H Won. Convertible group signatures. volume 1163, pages 311–321. Springer-Verlag, 1996.
- [20] J. Camenisch. Efficient and generalized group signatures. volume 1233, pages 465–479. Springer-Verlag, 1997.
- [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] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA*, pages 136–153, 2005.
- [23] Cécile Delerablée and David Pointcheval. Dynamic fully anonymous short group signatures. In *VIETCRYPT*, pages 193–210, 2006.
- [24] 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.
- [25] Yuan-Lung Yu and Tzer-Shyong Chen. An efficient threshold group signature scheme. *Applied Mathematics and Computation*, 167(1):362–371, 2005.

- [26] Fucai Zhou, Jun Zhang, and Jian Xu. Research on anonymous signatures and group signatures. *Comput. Commun.*, 31(17):4199–4205, November 2008.
- [27] 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. Springer-Verlag, 2003.
- [28] Jan Camenisch and Jens Groth. Group signatures: better efficiency and new theoretical aspects. In *Proceedings of the 4th international conference on Security in Communication Networks*, SCN'04, pages 120–133. Springer-Verlag, 2005.
- [29] R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué. A group signature scheme based on the integer factorization and the subgroup discrete logarithm problems. In *Proceedings of the 4th international conference on Computational intelligence in security for information systems*, CISIS'11, pages 143–150. Springer-Verlag, 2011.
- [30] 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.
- [31] P. Rogaway and T. Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance, 2004.
- [32] 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 SAC'98*, volume 1556 of *LNCS*, pages 72–80, Kingston, Ontario, Canada, 1998. Springer.
- [33] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, 1 edition, 2008.
- [34] Behrouz A. Forouzan. *Cryptography & Network Security*. McGraw-Hill, Inc., 1 edition, 2008.
- [35] Henk C. A. van Tilborg and Sushil Jajodia, editors. *Encyclopedia of Cryptography and Security, 2nd Ed.* Springer, 2011.

# Dissemination of Work

## **Journal**

1. Sujata Mohanty, Bansidhar Majhi, Vinay Iyer, "A novel DL based group signature scheme resistant against colluding attack", Journal of cryptography and communication, Springer (Communicated on March 2013).

## **Conference**

1. Vinay Iyer, Sujata Mohanty and Bansidhar Majhi, "A Novel Group Signature Scheme Resistant against Colluding Attack", International Conference on Advances in Computer Electronics and Electrical Engineering CEEE13. (Paper Accepted).