Efficient Identity Based Signcryption Scheme and Solution of Key-Escrow Problem

Vikas Kumar

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

June 2014

Efficient Identity Based Signcryption Scheme and Solution of Key-Escrow Problem

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Vikas Kumar

(Roll No.- 211CS2363)

under the supervision of

Prof. R. K. Mohapatra

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

June 2014

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

Certificate

This is to certify that the work in the thesis entitled ***Efficient Identity Based Signcryption Scheme and Solution of Key-Escrow Problem*** by ***Vikas Kumar*** is a record of 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 with the specialization of Information Security in the department of Computer Science and Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT Rourkela
Date: June 2, 2014

Ramesh Kumar Mohapatra
Asst. Professor, CSE Department

Declaration

I, Vikas Kumar (Roll No. 212CS2363) understand that plagiarism is defined as any one or the combination of the following

1. Uncredited verbatim copying of individual sentences, paragraphs or illustrations (such as graphs, diagrams, etc.) from any source, published or unpublished, including the internet.

2. Uncredited improper paraphrasing of pages or paragraphs (changing a few words or phrases, or rearranging the original sentence order).

3. Credited verbatim copying of a major portion of a paper (or thesis chapter) without clear delineation of who did or wrote what.

I Have made sure that all the ideas, expressions, graphs, diagrams, etc., that are not a result of my work, are properly credited. Long phrases or sentences that had to be used verbatim from published literature have been clearly identified using quotation marks.

I affirm that no portion of my work can be considered as plagiarism and I take full responsibility if such a complaint occurs. I understand fully well that the guide of the thesis may not be in a position to check for the possibility of such incidences of plagiarism in this body of work.

Date: June 2014

Vikas Kumar

M.Tech in Computer Sc. and Engg.

NIT Rourkela

Acknowledgment

First of all, I would like to express my deep respect and gratitude towards my supervisor Prof. Ramesh Kumar Mohapatra, who has been appreciated me behind the work. He convincingly conveyed spirit of adventure in regard to advanced cryptography and give me the opportunity to work under him in the field of security. Without his invaluable advices it would not have been possible for me to complete this project work. I am greatly thankful to him for his expert, sincere and valuable guidance and encouragement.

Secondly, I wish to express my sincere thanks to Prof. S. K. Jena, Prof. A. K. Turuk, Prof. B.D. Sahoo, Prof. D.P. Mohapatra, Prof. S. K. Rath, Prof. S. Chinara and all computer science departments for their valuable guidance, suggestions and encouragements during my research work. I would like to thank to administrative and technical staff of NIT Rourkela for providing equipment and software related to thesis.

I would like to express my deep love for my friends.

Finally I would like to express my deep respect and love for my family who is backbone for me. Especially my mom-dad who has been supported me very well in all situations and at last I thank god for giving me nice family and friends.

Vikas kumar

Roll-212cs2363

Abstract

In cryptography for sending any information from sender to receiver, we have to ensure about the three types of security policies i.e. integrity, confidentiality and authentication. For confidentiality purpose, encryption-decryption technique is used and for authentication purpose digital signature is used, so to ensure this three properties, first sender encrypt the message and then sign the message. Same process done at the receiver end that means first message is decrypted then verified, so it's two step process that increases the communication as well as computation cost. But in many real life applications where more speed and less cost is required like e-commerce applications, we can't use signature then encryption technique, so signcryption is the cryptographic primitives that provides signature as well as encryption at the same time on a single step. First signcryption scheme is proposed by Yullian Zheng in 1997, Since then many signcryption scheme is proposed based on elliptic discrete logarithm problem (ECDLP) , Bilinear pairing, Identity Based and certificate less environment. Many of the Signcryption scheme used Random Oracle Model for their security proofs and few are based on standard model.

In this thesis we have surveyed the existing identity based signcryption scheme and compare their security properties and efficiency. Along with this we have proposed two schemes of which 1st one is an signcryption scheme based on identity and the 2nd one signcryption scheme with certificateless environment. We start with some formal definition of signcryption primitives and complete the thesis with comparision with other models.

Keywords: Signcryption, Unsigncryption, PKG (Private Key Generator), Hash function, bilinear pairing, public key cryptography.

Contents

List of Figures

List of Tables

Acronyms

Acronyms	Description
AES	Advanced Encryption Standard
DES	Data Encryption Standard
CA	Certification Authority
BDHP	Bilinear Diffi-Hellman Problem
DLP	Discrete Logarithm Problem
BPGSC	Bilinear Pairing based Generalized Signcryption
CDHP	Computational Diffie-Hellman Problem
CLGSC	Certificateless Generalized Signcryption
CRHF	Collision Resistance Hash Function
DSA	Digital Signature Standard
ECC	Elliptic Curve Cryptosystem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECGSC	Elliptic Curve based Generalized Signcryption
GF	Galois Field
GSC	Generalized Signcryption
HMAC	Hashed Message Authentication Code
IBGSC	Identity based Generalized Signcryption
IDGSC	ID based Generalized Signcryption
KGC	Key Generation Center
MAC	Message Authentication Code
MD	Message Digest
OWF	One-Way Function
PKG	Private key Generator
PKI	Public-Key Infrastructure
RSA	Rivest, Shamir, Adelman
SHA	Secure Hash Algorithm

Symbols and Notations

Notations	**Description**
$\mid$	Divides
$\parallel$	Concatenation
$=$	Equality
$\equiv$	Congruence
$\approx$	Approximately
$\forall$	For all
$\geq$	Greater than equal to
$\leq$	Less than equal to
$\neq$	Not equal to
$\oplus$	XOR operation
$\perp$	False
$\top$	True
$\times$	Multiplication
hash()	One way hash function
$\lvert p \rvert$	Number of bits in p
G	Group
E	Elliptic curve
mod	modulo operator
GF(p)	The finite field of order p
Z_p	set of non-negative integers less than p
$D_k()$	Symmetric key decryption
$E_k()$	Symmetric key encryption

Chapter 1

Introduction

In this era information is treated as a asset which has a value like other assets. The assets have to be secured from attacks and threats. To keep secure, information must be follow different properties like integrity, confidentiality and availability. Integrity means information can't be changed by others. Confidentiality means only authorized people can read the information and availability means information must be available when it is needed.

Now a days in computer, internet is just a part of daily routine. The world is just like virtual network where people can communicate through internet, that means information is distributed so confidentiality plays a very crucial role in distributed environment when message is transmitted from one computer to another.

The most important function of cryptography is integrity and confidentiality. Confidentiality can be achieved by encryption and integrity can be preserved by digital signature. Encryption technique is divided into two categories: Private Key Encryption technique and Public Key Encryption technique [1]. In private key encryption there is a same secret key between sender and receiver but in public key encryption [2] technique there are two keys (public and private key) between sender and receiver where public key is known by all the people and private key is secret. Private Key encryption is fast as compared to public key encryption. Public key encryption technique is best suited in authentication and digital signature. In public key cryptography any message that is encrypted by public key can be decrypted by matching private key. Similarly any message that is signed by private key can only be verified by matching public key. For achieving confidentiality first

message is encrypted by receiver's public key and decrypted by receiver's private key. Similarly for achieving integrity message is signed by sender's private key and verified by sender's public key. In public key cryptography [3] for ensuring integrity, confidentiality and authentication first message is signed then encrypted and send to the receiver side. In receiver side first message is decrypted then it is verified. It's the two step process called *Signature-Then-Encryption* [3, 4] technique. In this application cost is more and efficiency is less and in real time application where quick response is required signature then encryption can not be used. To eliminate it, Yullian Zheng [4] in 1997 proposed the new cryptography primitives called **signcryption** where signature followed by encryption can be performed on single step that increase the efficiency and reduce the cost. It has not be used in some application where only one functionality like encryption or authentication is required but after some time generalized signcryption [5] scheme is used to eliminate it. In other words without any computation it provides confidentiality and integrity both as well as separately.

1.1 Message Encryption

It's the process where message (plain text) is converted into unintelligent format (cipher text) so that nobody can understand it. It's important so that unauthorized people can't see the original message. In cryptography there are many message encryption techniques like DES (data encryption standard) and AES (Advanced Encryption standard) [6]. Encryption algorithms are classified into two forms: public key encryption where public key of receiver is used for encryption and private key encryption where secret key between sender and receiver is used for encryption.

1.2 Message Decryption

It's the process where unintelligent format of message is converted into readable format. Decryption is of two types: public key decryption where receiver decrypts the message with his own private key and private key decryption where shared

secret key between sender and receiver is used for decryption. The process of encryption and decryption is shown in the figure 1.1.

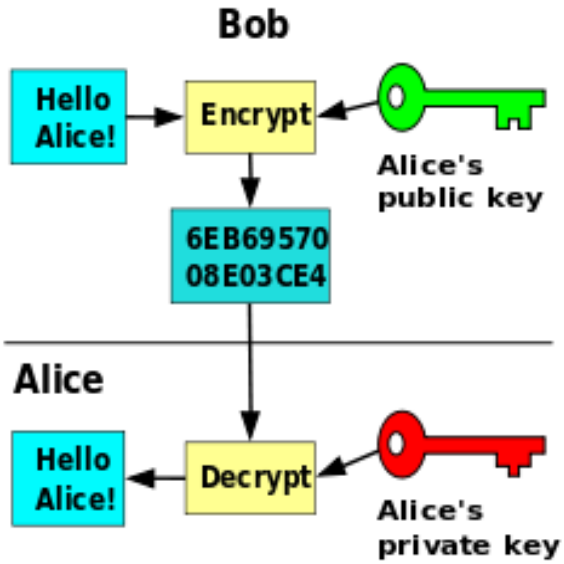

Figure 1.1: Public Key Encryption-Decryption Process

1.3 Message Authentication

It's used to protect the integrity of message where one party sends the message to another party in such a way if the message is modified in route then receiver can easily detect the message. Message authentication is divided into two categories [7]: private key authentication (MAC) and public key digital signature (DSS, ECDSA).

1.4 Digital Signature

Here one party checks the authenticity of another party to check whether he is getting the message from genuine user or not. To authenticate the message digital signature technique is used where message is signed by the private key of sender and verified by the public key of sender at receiver end. Here sender can not deny that he has never sent the message. The process is shown in figure 1.2

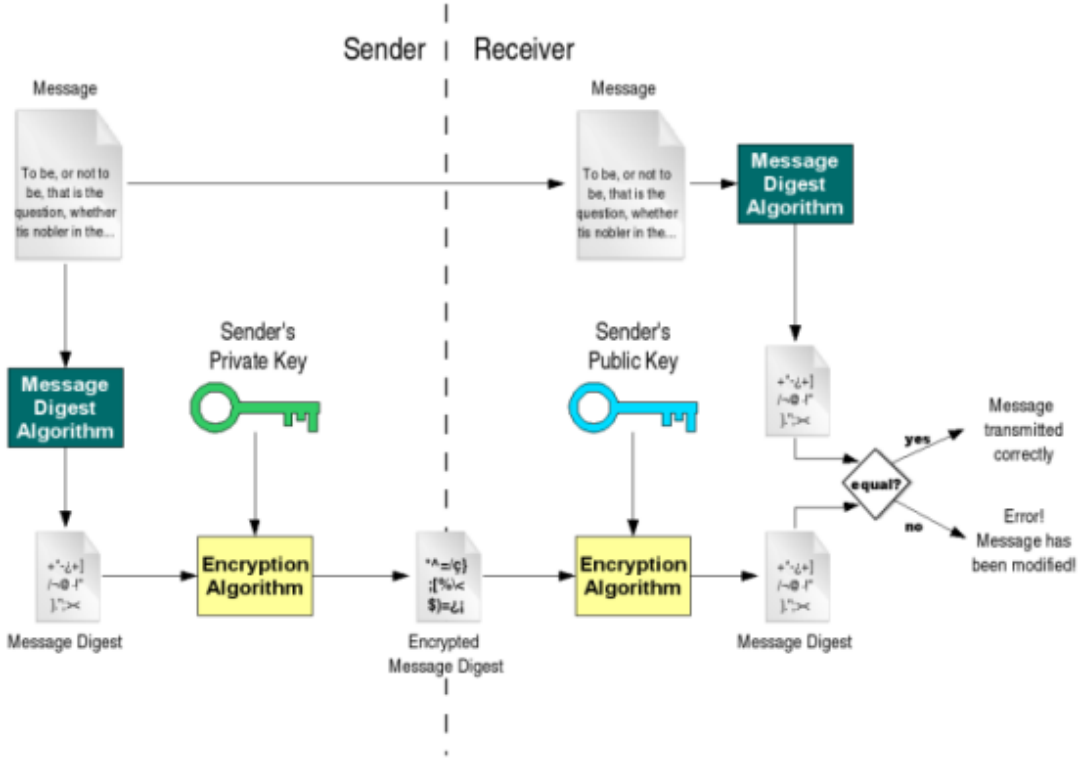

Figure 1.2: Digital Signature Process

1.5 Signature Then Encryption

It is the traditional method to achieve both the confidentiality and authenticity [3]. Here first Message is encrypted then it is signed at sender side, now the Message and signature pair is sent to the receiver side where first Message is decrypted then verified by receiver. It is two step process so it takes lot of machine cycle, that increase its computation as well as communication overheads so in many application that requires fast response, *Signature then Encryption* is not suitable. so in next paragraph we are going to discuss the new primitive called *Signcryption*. The process is shown in figure 1.3

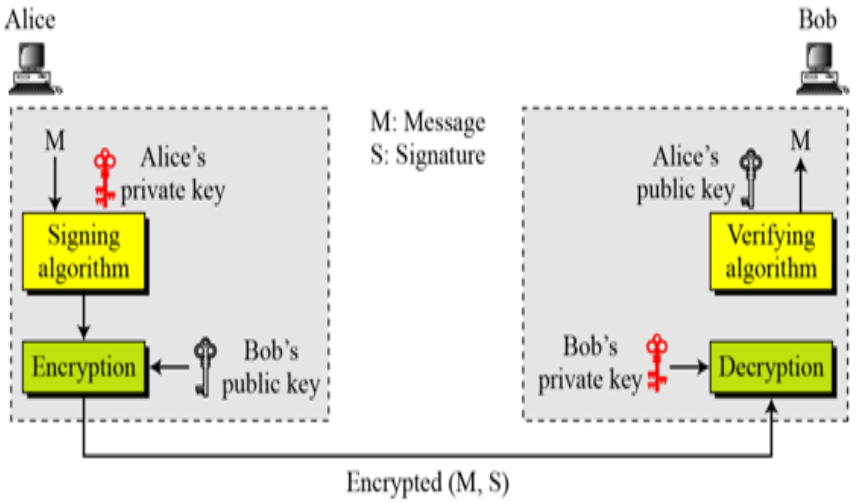

Figure 1.3: Signature then Encryption Technique

1.6 Signcryption

Signcryption is a cryptographic primitive proposed by Yullian Zheng in 1997 [4], which achieves integrity and confidentiality in a single logical step. Signature then encryption requires two steps but by signcryption only one step is sufficient for achieving confidentiality and integrity so signcryption reduces the communication as well as computation cost and increase the efficiency [8]. In many application like mobile agent protocol, Key management and routing protocol and electronic transaction protocol signcryption are using.

1.7 Identity Based Signcryption

In public key cryptography if we have multiple sender and receiver then we have n number of public-private key pairs [9]. To manage it we require PKI (public key infrastructure) but it increases the cost and reduce the efficiency so Shamir proposed the new scheme in 1984 [10, 11], i.e., identity based scheme where any user's public id like email address, MAC address is used as a public key that reduces the key management issue. Here to assure that the public key belongs to individual user, certificate is provided to user, again it increases the cost so

to minimize it trusted third party is used to see the communication, called PKG (private key generator) [12, 13].

1.8 Security Parameters

• ***Confidentiality:*** It means only the genuine user can access the message, unauthorized member should not access the message [3]. Message can be read by the receiver whom sender wants to transmit.

• ***Integrity:*** Integrity means message can not be changed by unauthorized party in the channel, for checking integrity of message, hash function is used. First message is converted into digest [3] then receiver calculate the digest and match calculated digest with original digest. If it matches then message is not changed.

• ***Unforgability:*** It means the inability of any entity to produce a valid message-signature pair except the designated signer [3].

• ***Public Verifiability:*** It means any third party can easily verify that the signcrypted text is valid or not, without any requirement for the secret key of the sender or the recipient.

• ***Non-Repudiation:*** Non Repudiation means sender can not deny of sending the message. Means the receiver can prove that message comes from sender side [3].

• ***Authentication:*** It involves confirming the identity of a system user. Authentication often involves verifying the validity of any form of identification. It means, the receiver of the message should be convinced about the senders legitimacy [3].

• ***Forward Secrecy:*** It defines the message should not expose its information even when some private parameters (secret key) is revealed.

1.9 Thesis Organization

The thesis is organized as follows:

Chapter-2: We will discuss various survey work related to thesis. The survey is classified into 4 parts: Signcryption scheme based on elliptic curve [14], Signcryption scheme based on bilinear pairing [15,16], Identity based scheme and certificate

less scheme.

Chapter-3: Here we will discuss various mathematical preliminaries that are required for implementation of the proposed scheme. Here we will discuss about hash function and properties of elliptic curves.

Chapter-4: Here we have proposed a new ***Modified improved identity based Signcryption Scheme*** and compared their complexities and efficiency with existing schemes.

Chapter-5: Here we have proposed the second new ***Modified improved certificateless Signcryption scheme*** and compared their complexities and efficiency with existing schemes.

Chapter-6: Here we will discuss the remarks and future scope of work.

Chapter 2

Litrature Review

2.1 Related Work

Confidentiality and integrity are the two important parameters that must be satisfied for secure communication [3]. These two parameters are achieved by encryption and signature. These two things can be performed with different ways: Signature then encryption, encryption then signature, signature and encryption etc. In many real time application privacy and authenticity simultaneously can be achieved by some protocol like SSL (Secure Socket Layer), IPSec (Internet Protocol Security), and PGP (Pretty Good Privacy) but this method is not good because of some reason, like it has low efficiency, and cost is sum of encryption and authentication. So to enhance the security in 1997 Zheng [4] proposed the new primitive called signcryption where authentication and encryption can be done on single step. Compared with available scheme it has low communication cost, less computation overheads and higher efficiency. In many application like electronic transaction protocol, mobile agent protocol and key management protocol signcryption is used. In 2002, Baek et al. [9] first describe the fully practical efficient signcryption scheme then after many signcryption scheme is developed based on RSA problem, Diffie-Hellman problem [17], bilinear based [18] etc. the different variation of signcryption is Also designed like parallel signcryption [19], hybrid signcryption [20], identity based signcryption [21], multi receiver signcryption [22], group signcryption [23] and so on.

2.2 Identity Based Cryptosystem

Identity based cryptosystem was introduced by Shamir in 1984 [11]. The main idea is to use any public string as a public key. The string may be any phone number, email address, MAC address, social security number or any publically available parameter. Here Private Key can be derived by trusted party called PKG (Private Key generator). PKG have their master public and master private key that helps to generate the private key of any user that reduces the key management problem. The main problem of identity based cryptography is **key escrow problem** [10,15]. Here PKG gives private key to all users that mean PKG can sign crypt as well as design crypt any message and PKG can forge any user. Here at security point of view no third party can do all these things, So to solve it we have proposed the new scheme based on certificateless cryptography [24, 25].

2.3 Certificateless Cryptography

Certificateless cryptography first proposed by Al- Riyami and Paterson [25] that avoids drawbacks of Identity based cryptography. It inherits from identity based technique, trusted party present here that generate the private key for all user but every user again generate their own private key, i.e., partial private key so the private key will be the combination of two private keys, i.e., partial private key and private key given by PKG, that reduces the Key Escrow issue.

2.4 Framework of Identity based Signcryption scheme

The algorithm consists of four steps which are:

Setup (1^k): Its randomized algorithm run by **PKG**. given a security parameter k, the algorithm generates the system parameters *params* and master secret key **Msk** [26] and master public key **Mpk**.

Key Generation (Mpk, Msk, ID): PKG takes user ID as input and generate corresponding public private key pair Q_u/S_u [18].

Signcryption (Mpk, Q_r, S_s): To send the message from sender S to receiver R, this algorithm takes input (S_s, ID_r, m) and output signcrypted text $\sigma = SIGNCRYPT(S_s, ID_r, m)$

Unsigncryption (Q_s, S_r): Receiver takes (ID_s, S_r, σ) as input and output m if σ is a valid signcryption done by sender S to receiver R, otherwise output false ($\perp$) if it is not valid [27].

2.5 Framework for Certificateless Signcryption Scheme

It consists of six different algorithms [24, 25, 28]. The steps are:

Setup (1^k): An algorithm is run by PKG to generate their own Master Private key and public parameter. Given a security parameter **k** the algorithm generate the secret key **Msk**, public key **Mpk** and public parameters *params*.

Extract-Partial-Private-Key (ID_u, Msk, *params*): A randomized algorithm that takes **Msk**, *params* and users identity as a input and gives their partial secret key D_u. The algorithm is run by PKG after verifying users identity.

Generate-User-Keys (ID_u, *params*): An algorithm run by user that takes user id and *params* as input and gives secret value **x** and public key **PK**. User generates their own private key that will be useful for creating full private key.

Set-Private-Key (D_u, x, *params*): An algorithm that takes partial secret key D_u and secret key generated by user i.e. **x** as an input and generate the full private key S_u for particular user U. this algorithm is executed by user to generate their full private key.

Signcryption (ID_r, m, S_s): To send the message from sender S to receiver R, this algorithm takes input (S_s, ID_r, m) and output signcrypted text $\sigma = SIGNCRYPT(S_s, ID_r, m)$.

Unsigncryption (Q_s, S_r): Receiver takes (ID_s, S_r, σ) as input and output m if σ is a valid signcryption done by sender S to receiver R, otherwise output false ($\perp$) if it is not valid.

2.6 Comparison of existing Signcryption Schemes

The related works on signcryption is classified into four categories:

1. Signcryption Scheme without Bilinear Pairing

• IDSH: An Efficient Identity-Based Signcryption Scheme without Bilinear Pairings by hassan. [29]

2. Bilinear Pairing Based Schemes

• IDSSBL: Efficient and provable secure Identity Based signature and signcryption from bilinear map by barreto and libert [18].

• IDG: Analysis and Improvement of Identity-Based Designated Verifier Signature Scheme by guozhi chen.

• IDLQ: A new identity based Signcryption scheme from pairings By Benoit Libert,and Jean- Jacques Quisquater [27].

• IDSS: Cryptanalysis of Two Identity Based Signcryption Schemes by Qi Xia and Chunxiang Xu [30].

3. Certificateless Environment

• ICST: Certificateless Proxy Identity-Based Signcryption Scheme QI Yanfeng, and TANG Chunming [28].

• ICSM: Certificateless Signcryption by M. Barbosa and P. Farshim [24].

4. Signcryption Scheme for Multi Receiver

• IMS: An Efficient Identity-Based Signcryption Scheme for Multiple Receivers by S. Sharmila Deva Selvi [21].

• IML: Cryptanalysis of two identity-based Signcryption schemes and an identity-based multi-signcryption scheme by Liang Hu, Wei Yuan, Fan-er Meng [30].

• MIDSCYK: An Efficient Provably Secure Multi Recipient Identity-Based Signcryption Scheme [31]

The table 2.1 shows the comparision of different schemes.

SCHEMES	KG	S	U
IDSH	4M	4M	5M
IDLQ	2M	2M+2P+2E	3P(+1)+2E
ICST	4M	3M	9M
ICSM	5M	4M+1P+1E	2P(+2)+1M
MIDSCYK	2M	(3+n)M+2P+1E	4P+1E

Table 2.1: Comparison of Computation Cost of Signcryption Scheme including Key Generation

M: Point multiplication P: No of Pairing operation; E: Exponentiation

(+): No of pre computed terms; S: Signcryption; D: Designcryption

KG: Key generation; n: number of receiver.

2.7 Observation

Here different pairing based signcryption scheme and certificateless based signcryption is compared. Table 2.2 gives the observation of different schemes.

Scheme	Signcryption			Unsigncryption		
	M	E	P	M	E	P
IDSH	4	0	0	5	0	0
IDLQ	2	2	2	0	2	3 (+1)
ICST	3	0	0	9	0	0
ICSM	4	1	1	1	0	2 (+2)
MIDSCYK	3+n	1	2	0	1	4

Table 2.2: Comparison of Computation Cost of Signcryption Scheme including Key Generation

M: point multiplication; E: Exponentiation; P: Pairing; (+) Precomputed operation; n: number of receiver

2.8 Motivation

In public key cryptography for providing confidentiality and integrity encryption and signature process is used but it is a sequential process that means first message is encrypted then signed at sender side likewise message is decrypted then verified at receiver side. So it consumes a lot of machine cycle and enhances the

complexity of system but in many applications like e-commerce where we need more speed and efficiency, signature then encryption technique can not be used. So to achieve confidentiality and integrity simultaneously on a single step, signcryption is used. The main aim of this paper is to design the efficient signcryption scheme that reduces the cost and increases the efficiency and to remove the Key Escrow Problem.

2.9 Objective of Research

1. To design an efficient identity based Signcryption scheme that have less overheads.
2. To design an efficient certificateless Signcryption Scheme to avoid key escrow problem.

Chapter 3

Mathematical Background

3.1 Mathematics of Cryptography

In this chapter we will be going to discuss various mathematical properties of cryptography that is useful to understand the mathematics description of this paper. Some important function like group, ring, bilinear map, field, elliptic curve will be discussed here.

3.1.1 Modular Arithmetic

Set of Residues: Z_n Here Z is the set of integer. Modulo operations result always gives non-negative integer [3]. Suppose k is the modulo operation then value of k is between 0 to k-1, suppose **a mod k** is any modulo operation where 'a' is any integer then result varies between 0 to k-1.

Example: Z_k= $\{0, 1, 2....(k-1)\}$

Z_4= $\{0, 1, 2, 3\}$

Z_1= $\{0\}$

Z_9=$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

Additive Inverse : Suppose m and n are two number in Z_k then it is called additive inverse of one another if m + n = 0 (mod k)

Example: in Z_{10} 10-4 = 6 is additive inverse of 4, so in generalized way for Z_k, n = k - m

Multiplicative Inverse : Two number a and b are multiplicative inverse of each other if, m $\times$ n $\equiv$ 1 (mod k) for example in Z_{10} the multiplicative inverse of 3 is 7 because 3*7 $\equiv$ 1 (mod 10). The integer m in Z_k has a multiplicative inverse exist only if gcd (k, m) = 1. For example, 8 have no multiplicative inverse in Z_{10} because gcd (10,8) $\neq$ 1

Some new sets :

1. Z_k^*: it is the subset of Z_k and contains only those integers for which multiplicative inverse exist. In Z_k each member contains additive inverse but only few member contains multiplicative inverse. Example:

Z_6 =$\{0, 1, 2, 3, 4, 5\}$ Z_6^*= $\{1, 5\}$

Z_7= $\{0, 1, 2, 3, 4, 5, 6\}$ Z_7^*= $\{1, 2, 3, 4, 5, 6\}$

Z_{10}= $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ Z_{10}^*= $\{1, 3, 7, 9\}$

2. Z_p: its same as Z_k but k is replaced with prime no p. Z_p includes all integers between 0 to p-1. Each member that belongs to Z_p has a additive inverse and all members have multiplicative inverse excluding 0.

3. Z_p^*: its same as Z_n^* but here p is prime number. In Z_p only some member have multiplicative inverse but in Z_p^* all member have multiplicative inverse excluding 0. Z_p^* contain all integer from 1 to p-1. Example:

Z_{11}^*= $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

3.1.2 Mathematics of Symmetric Key Cryptography

Algebraic Structures : Cryptography requires different sets of integer and different operation performed on that integer. Algebraic structure is the combination of integers and operations. There are many algebraic structures like groups, rings, fields.

Groups : A group [32] is the set of element that contains operation of binary "$\bullet$" And satisfy four operations. Commutative group is a group that satisfies five operations including commutativity, also called abelian group. The properties are as follows:

1. Closure : If i and j is the element of G then k = i • j is Also the element of G that means if we apply any operation on any element of group G then result will Also belongs to group G.
2. Associativity : If i, j, l are the element of group G, then (i • j) • l = i • (j • l) in other words order doesn't matter for applying group operation.
3. Commutativity : If p, q belongs to group G, then p • q = q • p
4. Existence of identity element : for all i in group G there exist an identity element 'ie' such that ie • i = i • ie = i.
5. Existence of inverse : for each i in group G there exist an element i' such that i • i' = i' • i = ie

Finite Group : A group is called finite if it contains number of elements that is finite otherwise its called infinite group.

Order of Group : It is the number of unique element present in group. If number of element is finite then its called order is finite otherwise order is infinite.

Subgroup: A subset SG is called the subset of group G if SG itself is a group with respect to the operation on G, in other words if G =$\langle r, \bullet \rangle$ is a group and SG = $\langle t, \bullet \rangle$ is a group under the same operation and t is non empty subset of r, then SG is called subgroup of G. the above definition gives:
1. If i and j the member of both group then k = i • j is Also the member of both group.
2. Same identity element exists for both.
3. If i belong to both groups then inverse of i also belongs to both groups.
4. The group made of identity element of G, SG = $\langle \{ie\}, \bullet \rangle$, is a subgroup of G.
5. Each group is itself a subgroup.

Cyclic Subgroup : If any subgroup of a particular group can be produced by the power of a component, subgroup is known as cyclic. Here power indicates,

group operation is performed repeatedly.
i^k $\rightarrow$ i • i • i....•i (k times)

Cyclic Group : It is the group that includes its self Cyclic Subgroup. The Component that can generate cyclic sub group can Also produce the whole group itself, that component is called **generator** of the group. If gr is a generator then, the elements in finite cyclic group can be written as $\{ie, gr_1, gr_2, ..., gr_{k-1}\}$, where gr_k = ie. a cyclic group can have many generators.
Example: The group Ge = $\langle Z_6, +\rangle$ is a cyclic group with two generator, ge = 1 and ge = 5 The group Ge =$\langle Z_{10}, *\rangle$ is a cyclic group with two generators, ge=3 and ge=7.

Order of an element : order of i ord(i) is the smallest integer k such that i^k=ie, the order of an element is the order of the cyclic group that it generates.

Ring: A ring [33] Ri is a type of algebraic structure that have two operation. First one satisfies the all five operation of abelian group and 2nd operation satisfy only the first two, means closure and associativity. It is denoted by Ri = $\langle\{...\}, *, \square\rangle$. 2nd operation is distributed over 1st operation. Distributive means for all i, j and k element of Ri, we have i □ (j • k) = (i □ j)•(i □ k) and (i • j) □ k = (i □ k) • (j □ k).
The ring that satisfies commutative property is called commutative ring.

Field : Field [33] is one type of commutative ring in which 2nd operation satisfies all five properties that defined for the 1st operation excluding the identity of the 1st operation (Zero element) has no inverse.

Finite Fields : A finite field is the field with finite number of element. Galois demonstrated that a field to have finite, number of component must be t^k, where t is prime number and k is positive integer. Finite field is Also called **Galois**

fields and described as GF(t^k).

3.2 Elliptic-Curve Cryptosystem

Elliptic-curve system in cryptography is suggested in 1985 [34] by victor miller and Neal Koblitz . Elliptic-curve cryptosystem uses elliptic curve scheme.

Definition of elliptic-curve : An Elliptic-curve [34] over a field which is finite, is non-singular cubic curve that have 2 variables, where f(P, Q) = 0 . The field P is usually taken to be the complex numbers, real number, rational number, algebraic expressions of rationale numbers or a finite field. By, non-singular means all 3 roots of EC must be distinct.

General form of elliptic-curve (EC) : Any elliptic curve can be defined by following equation. $A^2 = B^3$+ aB + b, here B is not a continuous point, chosen from particular field GF (P) or GF (2^k). The figure 3.1 shows the elliptic curve of equation $Y^2 = x^3$ - x + 1.

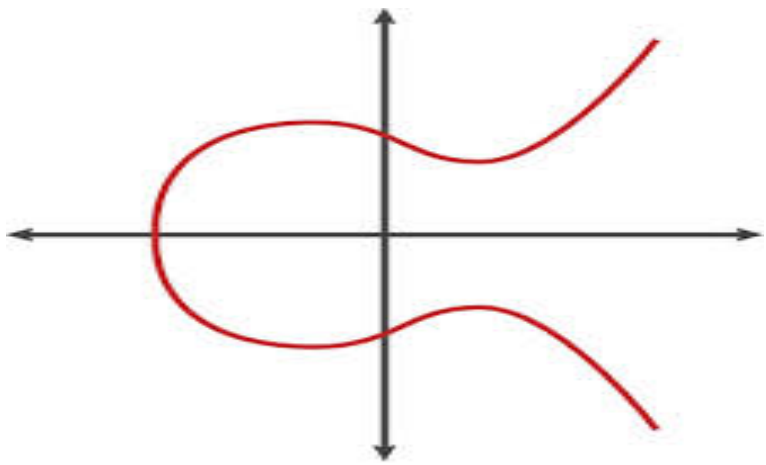

Figure 3.1: graphical representation of elliptic curve $Y^2 = x^3$ - x + 1

Properties:

1. Symmetric over x-axis.

2. Cubic curve in the variable x.

Why ECC?

Elliptic curve cryptography is public key encryption technique based on EC theory that is mainly used to make smaller, faster, and efficient keys of cryptography. Elliptic-Curve-Cryptosystem generates key with the help of EC equation but not of key generation with traditional method like product of very large prime number. it gives security level with a 164-bit key but other systems (like RSA) requires a 1,024-bit key to achieve it. Here ECC helps to make equivalent security with less computation power and battery resource usage. It is becoming most popular for mobile applications. In every 10 years key size becomes double so traditional methods can't be used due to large bit key. Table 3.1 shows some currently used RSA key length by some organization. If key size increase then definitely it increases the security but it causes serious problem. If we double the RSA key length then decryption will be 8 times slower. Table 3.1 gives the RSA key length of some organization and table 3.2 gives the security level of ECC and RSA.

Organization	RSA Key length
ICICI bank	2048
Google	1024
Facebook	1024
Amazon	2048
eBay	2048
Online SBI	2048
Canara Bank	2048

Table 3.1: RSA Key length of some organization

Cipher text size also becomes large. Speed of encryption also infected with large key length, which is slower by factor of 4. Table 3.2 gives the security level of ECC and RSA scheme.

From table it is clear that ECC takes less key length so as compared to RSA it is more efficient.

Security Level	80	112	120	128	256
ECC	160	185	237	256	512
RSA	1024	2048	2560	3072	15360

Table 3.2: RSA and ECC key Sizes

Application of ECC : ECC takes low power and low key length, so any application that takes less power and more security, ECC is used. In many areas it is using like

1. Wireless communication devices
2. Online transactions
3. Mobile devices
4. Smart cards
5. Web servers

3.3 Cryptographic Hash Function

Cryptographic hash function [35] is a function that takes variable length string as a input and gives Fixed length string i.e. **message digest**.

h_a:$\{0,1\}^* \rightarrow \{0,1\}^k$ where k is length of MD means message digest. Let's take a function f(I) = J that maps I to the image J. I is called preimage of J. The output is called hash value or message digest. Here we use J=h_a(I) that denotes, applying hash function into variable length message I and that gives fixed length digest J. hash function should follow some characteristics:

1. x should be variable length and y is fixed length.
2. For given I its easy to compute J but vice versa should be very tough that means hash function should be one way function.
3. Two messages doesnt have same message digest.
4. Hash function must be easy to compute.

Suppose I and J is message then h_a(I)=h_a(J) is infeasible. Today Hash function is used in various cryptographic techniques like message authentication code (MAC), digital signature, random sequence generator used in key agreements, authentication protocol etc. Hash function need to satisfy the 3 main properties:

1. Preimage Resistance : Given a digest J=h_a(I), its computationally infeasible to compute I. That is, computational cost of getting the input I must be $\geq 2^k$, where h(I) = J and $|J|$ = k.
Hash function for which preimage cant be solved efficiently is called preimage resistance.
2. 2nd *preimage resistance:* Given message I its computationally infeasible to compute different message I' that have same message digest. i.e. h_a(I)=$h_a(I')$ is infeasible to compute thats called second preimage resistance.
3. Collision resistance : It is impossible to find two messages with same message digest. That means if I and I' two different message then h_a(I)=$h_a(I')$ is impossible. This property is known as collision resistance.

Message Detection Code (MDC): MDC is the message digest that can prove the integrity of message that means message has not been changed. If sender wants to send message and be sure that the message is not changed during transmission then sender can create a message digest and send both the message and message digest towards receiver. Receiver can create the new message digest and compared it with old one. If message digest is same then message is not altered and it is accepted.

Message Authentication Code (MAC) : MDC only ensure about integrity of message but MAC can ensure integrity as well as data origin authentication. To achieve it MDC is converted into MAC. The difference between MDC and MAC is that in MAC a secret key (Private Key) is used between parties.
Sender uses hash function to create MAC from the concatenation of key and the message, h_a(K | M) then sends the message and MAC over insecure channel. Receiver separates the message from the MAC then he makes the new MAC from the concatenation of the message and secret key. Receiver then compares the newly created MAC with the one received. If the two MACs match, the message is au-

thentic and has not been modified by imposter.

Random oracle model : Random oracle model was introduced in 1993 by bellare and rogaway [36]. It is an ideal mathematical model for hash function. The behaviour of this model is given as:
1. When any new message comes then oracle create the fixed size of digest for that message and save the message and digest in oracle record.
2. When any message is exist and digest exists for that message then oracle simply puts the message digest in their record.
3. The digest for any new information is independently chosen from previous digest.

Pigeonhole principle : Random oracle model can be understood by the pigeonhole principle. It states that if we have n pigeonholes and n+1 pigeons then 2 pigeon is occupied in at least one pigeonhole. In generalized way, if m pigeonholes are occupied by tm+1 pigeons, then at least one pigeonhole is occupied by t+1 pigeons. Because the main idea of hashing dictates that the digest should be shorter than the message, according to principle there can be collision. In other words there must be some digest that corresponds to more than one message so the relationship between messages and possible digests is many to one.

3.4 Pairing Based Cryptography

The main idea of pairing based cryptography [37] is mapping between two important groups which allow a new scheme that is based upon the reduction of one problem to another that means reduction of problem which is hard from one group to problem which is easier as compared to first one in another group.

Bilinear Maps:
Bilinear Map allows mapping between different groups. let G_1 is cyclic additive group with generator p_r. Bilinear map is Also called pairing because it allows pair

of element from Gr_1 and Gr_2 to another group Gr_t.

Suppose Gr_1, Gr_2, Gr_t are cyclic groups with large prime order q_r. Generally Gr_1, Gr_2 are additive group and Gr_t are multiplicative group. A bilinear pairing is described as e_r: $Gr_1 \times Gr_2 \rightarrow Gr_t$ that satisfy the bilinear property:

e_r(iP, jQ) $= e_r(P, Q)^{ij}$ for all P $\in Gr_1$, Q $\in Gr_2$ and all i, j $\in$ Z.

It means if p_r is generator of Gr_1 and Q_r is generator of Gr_2 then $e_r(p_r,Q_r)$ is generator of Gr_t. The mapping is called computable if there exist some algorithm that can efficiently compute $e_r(P_r,Q_r)$ for $P_r,Q_r \in Gr_1$. if $Gr_1 = Gr_2$ then paring is called symmetric otherwise pairing is known as asymmetric. if $Gr_1 = Gr_2 = Gr_t$ then pairing is called self bilinear map Gr $\times$ Gr $\rightarrow$ Gr.

Bilinear pairing :

if Gr_1 is cyclic additive group and Gr_2 is cyclic multiplicative group of the same order q_r, suppose P_r is generator of Z_q^*. a bilinear pairing is a map $e_r : Gr_1 \times Gr_2 \rightarrow Gr_t$ that satisfies the following properties:

1. Bilinearity: for every P_r,Q_r,$R_r \in Gr_1$, $e_r(P_r, Q_r+R_r) = e_r(P_r,Q_r)e_r(P_r,R_r)$ or $e_r(P_r+Q_r,R_r) = e_r(P_r,R_r)e_r(Q_r,R_r)$

for any i,j $\in Z_q^*$

$e_r(\mathrm{i}P_r,\mathrm{j}Q_r) = e_r(P_r, Q_r)^{ij} = e_r(\mathrm{ij}P_r,Q_r) = e_r(P_r,\mathrm{ij}Q_r) = e_r(iP_r, Q_r)^j = e_r(P_r, iQ_r)^j$

$= e_r(jP_r, Q_r)^i = e_r(P_r, jQ_r)^i$

$e_r(k_rP_r,Q_r) = e_r(P_r, Q_r)^{k_r} = e_r(P_r,k_rQ_r) = e_r(P_r, Q_r)^{k_r}$

2. Non-Degeneracy : If everything maps to identity then it is undesirable, if P_r is generator of Gr_1 then $e_r(P_r,P_r)$ is generator of Gr_2 that means if there exist $P_r \in Gr_1$ such that $e_r(P_r,P_r) \neq 1$ where 1 is identity element of Gr_2.

3. Computability : There must be exist an algorithm that can efficiently compute $e_r(P_r,Q_r)$ for every P_r,$Q_r \in Gr_1$.

Chapter 4

Modified Identity Based Signcryption Scheme (MIBS)

In this chapter we have proposed efficient identity based Signcryption scheme with bilinear pairing and compare their efficiency with existing schemes.

4.1 Frame Work of the MIBS Scheme

The algorithm for MIBS consists of 4 steps: MIBS (SETUP, KEY-GENERATION, MIS, and MIU. the description is as follows:

• **SETUP(1^k) :** The randomized algorithm run by PKG (trusted party) to generate the public and private key of **PKG** (private key generator) where security parameter k is given. The algorithm will generate the system parameter *params*. Suppose PKG chooses **Msk** as a secret key and **Mpk** as public key.

• **KEY-GENERATION (*Mpk*, *Msk*, ID):** Given identity ID of user PKG will generate their public (Q_{id}) and private key (S_{id}).

• **MIS (S_s, ID_r, m):** For sending the message from sender S to receiver R this algorithm takes (S_s, ID_r, m) as a input and gives Signcypted text σ = MIS(S_s, ID_r, m) as output.

• **MIU (ID_s, S_r):** This algorithm takes (ID_s, S_r, σ) as input and gives out-

put m when σ is valid otherwise gives invalid message ($\perp$).

4.2 Description of the MIBS Scheme

SETUP : Given the security parameter 1^k, trusted party generates two groups Gr_1 and Gr_2 of prime order p. P is the generator of Gr_1 and e: $Gr_1 \times Gr_1 \rightarrow Gr_2$. three hash function are used here which is as follows:

- $H_0 : \{0,1\}^* \rightarrow Z_q^*$

- $H_1 : G_2 \rightarrow Z_q^*$

- $H_2 : \{0,1\}^* \rightarrow Z_q^*$

here n denotes the number of bits to represent message. trusted party generate $Msk \in Z_q^*$ as the secret key and calculate public key $Mpk = Msk \times$ P.

$params : \langle Gr_1, Gr_2, P, Mpk, H_0, H_1, H_2, e \rangle$

KEY-GENERATION : Suppose user ID is U_{id}, here trusted party generate the private key for user U.

$Q_u = H_0(ID_u)$

$S_u = MskQ_u$

MIS(Q_r, S_s,*Mpk*): If sender S with identity ID_s wants to send a message to receiver R with identity ID_r then the different steps followed by him is:

- Select x Uniformly from Z_q^*
- U $\leftarrow$ xP
- Y $\leftarrow e(Q_r, Mpk)^x$
- B $\leftarrow H_1$(Y)
- C $\leftarrow$ B $\oplus$ M
- T $\leftarrow H_2$(Y, U, M, Q_s, Q_r, ID_s, ID_r)
- V $\leftarrow$ UT + S_s

- $\sigma \leftarrow$ (C, U, V)

MIU: After receiving σ receiver does the following steps:

- Y $\leftarrow$ e(S_r, U)
- B $\leftarrow H_1$(Y)
- M $\leftarrow$ B $\oplus$ C
- T $\leftarrow H_2$(Y, U, M, Q_s, Q_r, ID_s, ID_r)

Message Verification :

If e(V, P) $\leftarrow$ e$(U, P)^T$. e(Q_s, Mpk)

Correctness :

- Y $\leftarrow$ e(S_r, U)
- Y $\leftarrow$ e($MskQ_r$,xP)
- Y $\leftarrow e(Q_r, MskP)^x$
- Y $\leftarrow e(Q_r, Mpk)^x$

So Y $\leftarrow e(Q_r, Mpk)^x \leftarrow$ e(S_r, U)

Mathematical Proof of verification :

- e(V, P) $\leftarrow$ e(UT + S_s, P)
  $\leftarrow$ e(UT, P)e(S_s, P)
  $\leftarrow$ e$(U, P)^T$ e($MskQ_s$, P)
  $\leftarrow e(U, P)^T$ e(Q_s, MskP)
- e(V, P) $\leftarrow e(U, P)^T$ e(Q_s, Mpk) (***Verified***)

4.3 Efficiency analysis

The main purpose of our scheme is to reduce the complexity and enhance the efficiency. There are two types of cost first Computation that includes the various mathematical operations like multiplication, division, pairing, exponentiation and communication cost that includes transmission complexity. The scheme simply

remove the complexity of various existing scheme like [16, 38]. In table 4.1 we have compared the computation complexity of our scheme with existing one. Our scheme gives better performance as compared to [16,38] so its the improved version of identity based Signcryption scheme. Table 4.1 shows the efficiency comparision of our proposed scheme with existing schemes.

Scheme	**Signcryption**			**Unsigncryption**		
	M	E	P	M	E	P
Libert Quisquater	2	2	0 (+2)	0	2	3 (+2)
X Boyens	3	1	0 (+1)	2	0	3 (+1)
Chow et al. s	2	0	0 (+2)	1	0	4
Li Fa-Gen Et Al.S	3	1	1 (+1)	0	2	2 (+2)
Proposed scheme	2	1	0 (+1)	0	1	3 (+1)

Table 4.1: Efficiency Comparison with other Signcryption schemes

M: Number of point multiplication in group G_1; E: Number of exponentiation in G_2 ; P: Number of pairing Computation; (+): Precomputation of pairing

Chapter 5

Certificateless Signcryption Scheme (CIBS)

In this chapter we have proposed efficient certificateless Signcryption scheme with bilinear pairing and compare their efficiency with existing schemes.

5.1 Frame Work of improved CIBS scheme

The algorithm for CIBS consists of 6 steps: CIBS(SETUP, EXTRACT-PARTIAL-PRIVATE-KEY, GENERATE-USER-KEY, SET-PRIVATE-KEY CIS, CIU. the description is as follows:

• **SETUP**(1^k) **:** The randomized algorithm run by PKG (trusted party) to generate the public and private key of **PKG** (private key generator) where security parameter k is given. The algorithm will generate the system parameter *params* . Suppose PKG chooses **Msk** as a secret key and **Mpk** as public key.

• **EXTRACT-PARTIAL-PRIVATE-KEY (*params*, *Msk*, ID):** Given identity ID of user PKG will generate their public key (Q_{id}) and partial private key (D_{id}).

• **GENERATE-USER-KEY**(ID_u, ***params***)**:** Here user run an algorithm that takes user id as input and generate the secret key x and public key PK of user.

• **SET-PRIVATE-KEY(D_u, x, *params*):** An algorithm that takes partial private key (D_u) and secret key (x) as input and return the full private key S_u.

• **CIS (S_s, ID_r, m):** For sending the message from sender S to receiver R this algorithm takes (S_s, ID_r, m) as a input and gives Signcypted text σ = CIS(S_s, ID_r, m) as output.

• **CIU (ID_s, S_r):** This algorithm takes (ID_s, S_r, σ) as input and gives output m when σ is valid otherwise gives invalid message ($\perp$).

5.2 Description of the improved CIBS Scheme

SETUP : Given the security parameter 1^k, trusted party generates two groups Gr_1 and Gr_2 of prime order p. P is the generator of Gr_1 and e: $Gr_1 \times Gr_1 \rightarrow Gr_2$. Three hash functions are used here which is as follows:

- $H_0 : \{0,1\}^* \rightarrow Z_q^*$
- $H_1 : Gr_2 \rightarrow Z_q^*$
- $H_2 : \{0,1\}^* \rightarrow Z_q^*$

Here n denotes the number of bits to represent message. trusted party generate $Msk \in Z_q^*$ as the secret key and calculate public key $Mpk = Msk \times$ P.

$params : \langle Gr_1, Gr_2, P, Mpk, H_0, H_1, H_2, e \rangle$

EXTRACT-PARTIAL-PRIVATE-KEY: Suppose user ID is U_{id}, here trusted party generate the private key for user U.

$Q_u = H_0(ID_u)$

$D_u = Msk.Q_u$

GENERATE-USER-KEY(ID): An algorithm is used by user that takes input as identity and public parameter and output the secret value x and public key PK.

PK_u = x.P

SET-PRIVATE-KEY(D_u,x,*Params*): An algorithm that takes input as partial secret D_u and secret value x and return the full private key S_u.

CIS (S_s, *Mpk*, Q_r): This algorithm takes S_s, *Mpk*, Q_r as a input and gives σ as output.

- Pick random r $\in Z_q^*$
- U $\leftarrow$ rP
- Y $\leftarrow$ e(Q_r, *Mpk*)^r
- B $\leftarrow$ H_2(Y)
- C $\leftarrow$ B $\bigoplus$ M
- T $\leftarrow$ H_1(U, M, Y, Q_s, Q_r, ID_s,ID_r)
- V $\leftarrow$ D_s + xT +rT
- σ $\leftarrow$ (C, U, V)

CIU (S_b, Q_s, *Mpk*): Algorithm that takes σ as an input and gives m as output and check whether it is genuine or not.

- Y $\leftarrow$ e(D_r, U)
- B $\leftarrow$ H_2(Y)
- M $\leftarrow$ B $\bigoplus$ C
- T $\leftarrow$ $H_1(U, M, Y, Q_s, Q_r, ID_s, ID_r)$

Verification :

If e(V,P) = e(Q_s, *Mpk*).$e(T, PK_s)$.e(T,U)

Correctness :

- Y $\leftarrow$ e(D_r, U)
- Y $\leftarrow$e($Msk.Q_r$,U)
- Y $\leftarrow$e($Msk.Q_r$,rP)
- Y $\leftarrow$e(Q_r,Msk.rP)
- Y $\leftarrow$e(Q_r,Msk.Pr)
- Y $\leftarrow$e(Q_r,Mpk.r)
- Y $\leftarrow$ e(D_r,U) $\leftarrow$ e(Q_r, Mpk)^r

Mathematical proof of verification

e(V, P) $\leftarrow$ e(D_s + xT +rT, P)

$\leftarrow$ e(D_s,P)e(xT,P)e(rT, P)

$\leftarrow$ e($Msk.Q_s$, P) e(T, xP) e(T,rP)

e(V, P) $\leftarrow$ e(Q_s, Mpk) e(T,PK_s) e(T,U) (***Verified***)

5.3 Efficiency Analysis

Computation cost is the parameter that defines any algorithms efficiency. Here in table 5.1 we have compared our proposed algorithm with existing one [24], and proved that our scheme is more efficient than existing one. Table 5.1 shows the efficiency analysis of our scheme with existing one.

Scheme	Signcryption			Unsigncryption		
	M	E	P	M	E	P
Barbosa et al.	4	1	0 (+1)	1	0	4 (+1)
Proposed Scheme	3	1	0 (+1)	0	0	4 (+1)

Table 5.1: Efficiency Comparison with Certificateless Signcryption Scheme

M: number of point multiplications in G1; E: number of exponentiation in G2; P: number of pairing computations; (+): Pre-computation of pairing

Chapter 6

Conclusion and Future Work

Identity based Signcryption is a approach that reduces the communication as well as computation cost and increase the efficiency of the system, here we have proposed the new improved identity based scheme that is more efficient as compared to some existing scheme. We have compared the complexity of our proposed scheme with existing work and proved that our scheme is efficient. Later we proposed the new certificateless signcryption scheme to avoid the key escrow problem that comes in identity based cryptosystem and compared their efficiency with existing scheme and proved that our certificateless scheme is the improved version. In many application where less time is required Identity based signcryption is the great solution like AD-hoc network, mobile computing and embedded system.

Bibliography

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology-Eurocrypt 2004*, pp. 506–522, Springer, 2004.

[2] P.-K. Encryption, "Public key encryption," *Virtual Private Network (VPM)*.

[3] B. A. Forouzan, *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[4] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Advances in Cryptology-CRYPTO'97*, pp. 165–179, Springer, 1997.

[5] G. Yu, X. Ma, Y. Shen, and W. Han, "Provable secure identity based generalized signcryption scheme," *Theoretical Computer Science*, vol. 411, no. 40, pp. 3614–3624, 2010.

[6] M.-L. Akkar and C. Giraud, "An implementation of des and aes, secure against some attacks," in *Cryptographic Hardware and Embedded Systems-CHES 2001*, pp. 309–318, Springer, 2001.

[7] G. Tsudik, "Message authentication with one-way anh functions," *ACM SIGCOMM Computer Communication Review*, vol. 22, no. 5, pp. 29–38, 1992.

[8] D. Nalla and K. C. Reddy, "Signcryption scheme for identity-based cryptosystems.," *IACR Cryptology ePrint Archive*, vol. 2003, p. 44, 2003.

[9] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Public Key Cryptography-PKC 2005*, pp. 380–397, Springer, 2005.

[10] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in CryptologyCRYPTO 2001*, pp. 213–229, Springer, 2001.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*, pp. 47–53, Springer, 1985.

[12] J. Malone-Lee, "Identity-based signcryption.," *IACR Cryptology ePrint Archive*, vol. 2002, p. 98, 2002.

[13] J. K. Rout, *An Improved Certificateless Generalized Signcryption Scheme.* PhD thesis, 2013.

[14] A. Enge, "Bilinear pairings on elliptic curves," *arXiv preprint arXiv:1301.5520*, 2013.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[16] B. Libert and J.-J. Quisquater, "New identity based signcryption schemes from pairings.," *IACR Cryptology ePrint Archive*, vol. 2003, p. 23, 2003.

[17] D. Boneh, "The decision diffie-hellman problem," in *Algorithmic number theory*, pp. 48–63, Springer, 1998.

[18] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology-ASIACRYPT 2005*, pp. 515–532, Springer, 2005.

[19] Y. Dodis, M. J. Freedman, and S. Walfish, "Parallel signcryption with oaep, pss-r, and other feistel paddings.," *IACR Cryptology ePrint Archive*, vol. 2003, p. 43, 2003.

[20] A. W. Dent, "Hybrid signcryption schemes with outsider security," in *Information Security*, pp. 203–217, Springer, 2005.

[21] S. Selvi, S. S. Vivek, J. Shriram, and C. P. Rangan, "Identity based partial aggregate signature scheme without pairing," in *Sarnoff Symposium (SARNOFF), 2012 35th IEEE*, pp. 1–6, IEEE, 2012.

[22] X. Boyen, "Multipurpose identity-based signcryption," in *Advances in Cryptology-CRYPTO 2003*, pp. 383–399, Springer, 2003.

[23] D. Kwak, S. Moon, G. Wang, and R. H. Deng, "A secure extension of the kwak–moon group signcryption scheme," *computers & security*, vol. 25, no. 6, pp. 435–444, 2006.

[24] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pp. 369–372, ACM, 2008.

[25] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT 2003*, pp. 452–473, Springer, 2003.

[26] P. S. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Advances in cryptologyCRYPTO 2002*, pp. 354–369, Springer, 2002.

[27] G. Chen and S. Wan, "Analysis and improvement of identity-based designated verifier signature scheme," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, pp. 2388–2391, IEEE, 2012.

[28] Q. Yanfeng, T. Chunming, L. Yu, X. Maozhi, and G. Baoan, "Certificateless proxy identity-based signcryption scheme without bilinear pairings," *Communications, China*, vol. 10, no. 11, pp. 37–41, 2013.

[29] Hassan, "An efficient identity based signcryption scheme without bilinear pairing,"

[30] Q. Xia and C. Xu, "Cryptanalysis of two identity based signcryption schemes," in *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*, pp. 292–294, IEEE, 2009.

[31] H. Elkamchouchi and Y. Abouelseoud, "Midscyk: An efficient provably secure multi-recipient identity-based signcryption scheme," in *Networking and Media Convergence, 2009. ICNM 2009. International Conference on*, pp. 70–75, IEEE, 2009.

[32] S. R. Blackburn, C. Cid, and C. Mullan, "Group theory and cryptography," *This page intentionally left blank*, p. 133, 2010.

[33] N. Koblitz, *A course in number theory and cryptography*, vol. 114. Springer, 1994.

[34] V. Miller, "Short programs for functions on curves," *Unpublished manuscript*, vol. 97, pp. 101–102, 1986.

[35] B. Preneel, "Cryptographic hash functions," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 431–448, 1994.

[36] X.-Y. Jia, B. Li, and Y.-M. Liu, "Random oracle model," *Ruanjian Xuebao/Journal of Software*, vol. 23, no. 1, pp. 140–151, 2012.

[37] M. Maas, *Pairing-based cryptography.* PhD thesis, Masters thesis, Technische Universiteit Eindhoven, januari 2004. BIBLIOGRAFIE BIBLIOGRAFIE, 2004.

[38] S. S. Chow, "Removing escrow from identity-based encryption," in *Public Key Cryptography–PKC 2009*, pp. 256–276, Springer, 2009.