

Signcryption Scheme with Forward Secrecy Based on Hyper Elliptic Curve Cryptography



Nizamuddin

484/FBAS/MSCS/F08

Supervisor

Qaisar Javaid

Assistant Professor

Co- supervisor

Shehzad Ashraf Chaudhry

Lecturer

Department of Computer Science

Faculty of Basic & Applied Sciences

International Islamic University, Islamabad

2012



7H-8828
Accession No. _____

MSC
004
NIS

1. Computer literacy
2. Computer system

DATA ENTERED

B. 04/26/13

Department of Computer Science,
International Islamic University Islamabad

Date: 16/02/2012

Approval Certificate

It is certified that we have read the thesis titled "Signcryption Scheme with Forward Secrecy Based on Hyper Elliptic Curve Cryptography" submitted by Nizamuddin Reg. No. 484-FBAS/MSCS/F08. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the degree of MS in Computer Science.

1. External Examiner

Dr. Abdus Sattar

Former D.G

Pakistan Computer Bureau,
Islamabad Pakistan

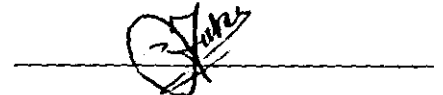


2. Internal Examiner

Dr. Muhammad Zubair

Assistant Professor DCS

International Islamic University,
Islamabad

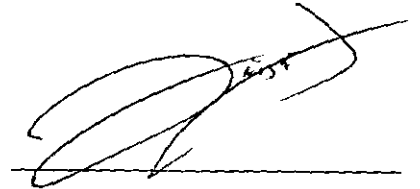


3. Supervisor

Mr. Qaisar Javaid

Assistant Professor DCS

International Islamic University,
Islamabad

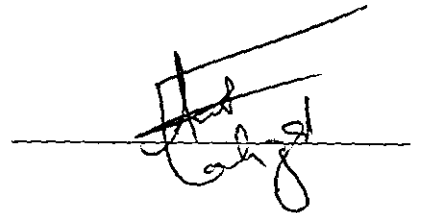


4. Co. Supervisor

Mr. Shehzad Ashraf Chaudhry

Lecturer DCS

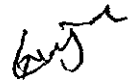
International Islamic University,
Islamabad



This research work is submitted to the
Department of Computer Science
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
As a partial fulfillment of the requirement for the award of the Degree
of MS in Computer Science

Declaration

I hereby declare and affirm that this thesis neither as whole nor as a part thereof has been copied out from any source. It is further declared that I have completed this thesis on the basis of my personal efforts, made under the sincere guidance of my supervisors. If any part of thesis report is proven to be copied out or found to be reproduction of some other I shall stand by the consequences. No portion of the work presented in this report has been submitted in support of an application for other degree or qualification of this or any other university.



Nizamuddin

484-FBAS/MSCS/F08

Dedicated to
My Beloved Parents

Acknowledgement

All Praise and Glory be to Almighty Allah (Subhanahu WA Ta'ala) Who gave me the courage and patience to carry out this work.

Peace and Blessings of Allah be upon His last Prophet Muhammad (peace be upon him), who said: "Allah makes the way to Janna' easy for him who treads the path in search of knowledge."

I would like to thank my supervisor Mr. Qaisar Javaid and Co-supervisor Mr. Shehzad Ashraf Chaudhry for their acceptance, support and taking interest in my research work.

I am thankful to Dr Muhammad Sher and all faculty members of the Department of Computer Science for their valuable guidance and knowledge.

I would like to thank my Family for all their love, understanding and prayers. Their prayers and encouragement always help me to take the right steps in life.

On a personal note I thank my father for all their love, understanding, prayers and everything. Baba one day I must do something special for you.

I am also thankful to my sister Bibi Je for the endless love and memorable help she always gave me.

Special thanks to my sincere friend Noorul Amin for his motivation, social and moral support during my studies.

Regards to all my colleagues and friends; thanking Azhar Resham, Zahid Mahmood Chaudry, Abdelmutilib Ibrahim, Eng Hanifullah, Jahangir Khan, Musa khan and Muhammad Sadiq Khan, for exchanging ideas, motivation, social and moral support.

Last but not least, I thank my sincere friend and wife for her unconditional love and patience during the very first year of our marriage.

To all of you thank you very much!

Nizamuddin

Abstract

Signcryption is an emerging cryptographic technique provides the functionality of digital signature and encryption with significant less cost. Hyperelliptic curve cryptography is on its way from pure academic interest to industrial applications due to its efficiency and high security per bit. In this thesis we present four signcryption schemes based on hyperelliptic curve cryptography for confidential and authenticated message delivery. The proposed schemes fulfill all the security parameters of signcryption and equivalent in function to signature-Then-encryption technique with less computation cost and communication overhead. The proposed work is divided in three sections; in section one, proposed scheme has fulfill the security parameters of signcryption, in section two proposed scheme has additional feature of forward secrecy and in section three proposed scheme has properties of forward secrecy and direct public verifiability.

Proposed schemes have less computation cost, communication overhead and are suitable for restricted computation devices like mobile devices, smart card based applications and many more.

Table of Contents

Chapter 1.....	1
1. 1 Introduction.....	2
1.2 Cryptography.....	2
1.2.1 Encryption.....	3
1.2.2 Symmetric Encryption.....	3
1.2.3 Asymmetric Encryption.....	3
1.3 Digital Signature.....	4
1.3.1 Direct Approach.....	4
1.3.2 Arbitrated Approach.....	4
1.3.3 Digital Signature Standard.....	5
1.4 Signature and Encryption.....	5
1.4.1 Signature-Then-Encryption.....	5
1.4.2 Encryption-Then-Signature.....	5
1.5 Shortcoming of Signature and Encryption.....	5
1.6 Signcryption.....	6
1.6.1 Notation Guide.....	6
1.6.2 Key Generation.....	6
1.6.3 Signcryption.....	7
1.6.4 Unsigncryption.....	7
1.7 Signcryption Vs Signature& Encryption Cost Comparison.....	7
1.8 Signcryption Applications.....	8
1.8.1 MANET and Sensor Networks.....	8
1.8.2 Satellite Communication.....	8
1.8.3 Electronic and Mobile Commerce.....	8
1.9 Motivation.....	8
1.10 Thesis in Brief.....	9
Chapter 2.....	10
2 .1 Literature Review.....	11
2.2 Schemes Based on Discrete Logarithm Problem.....	11
2.3.1. Parameters Setup.....	11
2.2.1. Y. Zheng [1] Signcryption Scheme.....	11
2.2.2. F. Bao and H. Deng [34] Signcryption Scheme.....	12

2.2.3. C. Gamage, J. Leiwo, and Y. Zheng [35] Signcryption Scheme	12
2.3. Schemes Based on Elliptic Curve Discrete Logarithm Problem	12
2.3.1. Parameters Setup	12
2.3.2. Y. Zheng and H. Imai [36] Signcryption Scheme	13
2.3.3. R. J. Hwang, C. H. Lai and F. F. Su [37] Signcryption Scheme	14
2.3.4. M. Toorani and A.A. Beheshti Shirazi [38] Signcryption Scheme	15
2.3.5. R. K. Mohapatra and B. Majhi [39] Signcryption Scheme	16
2.4. Schemes Based on Hyperelliptic Curve Discrete Logarithm Problem	17
2.4.1. Parameters Setup	17
2.5 Observation	19
2.6 Problem Statement	20
2.7 Contribution	20
Chapter 3	22
3.1 Mathematical Background	22
3.2 Abstract Algebra	22
3.2.1 Algebraic properties	22
3.2.2 Algebraic Structures	23
3.3 Hard Problems and Public Key Cryptosystems	23
3.3.1 Integer Factorization Problem	23
3.3.2 Discrete Logarithmic Problem	24
3.3.3 Elliptic Curve Discrete Logarithm Problem	24
3.3.4 Hyper Elliptic Curve Discrete Logarithm Problem	24
3.4 Hyper Elliptic Curve	24
3.4.1 Points on Hyper Elliptic Curve	25
3.4.2 Divisors	25
3.4.3 Representations of Divisors	26
3.4.5 Addition of Divisors	26
3.5 Hyper Elliptic Curve Cryptosystem	28
Chapter 4	30
4.1 Proposed Signcryption Schemes	30
4.2 Signcryption Scheme	30
4.2.1 Signcryption	30
4.2.2 Unsigncryption	31

4.2.3 Correctness Proofs of the Proposed Scheme.....	31
4.2.4 Security Analysis of Proposed Scheme	31
4.3 Signcryption Scheme with Forward Secrecy	32
4.3.1 Signcryption	33
4.3.2 Unsigncryption	33
4.3.3 Correctness Proofs of the Proposed Scheme.....	34
4.3.4 Security Analysis of Proposed Scheme.....	34
4.4 Signcryption Schemes with Forward Secrecy and Public Verifiability	34
4.4.1 Signcryption	34
4.4.2 Unsigncryption	35
4.4.3 Proofs of the Proposed Scheme.....	35
4.4.4 Security Analysis of Proposed Scheme	36
4.5 Cost analysis of Proposed Schemes and Results	36
Chapter 5.....	41
5.1 Conclusion	41
5.2 Limitations of the Proposed Work.....	41
5.3 Future Direction.....	41
References.....	43

List of Figures

Figure 1.1 Symmetric key encryption.

Figure 1.2 Asymmetric cryptosystem.

Figure 3.1 Algebraic structure.

Figure 3.2 Hyperelliptic curve.

Figure 3.3 Elliptic curve point addition.

Figure 3.4 Hyperelliptic curve divisor addition.

Figure 4.1 Comparative computation cost of sign-then-encryption Vs Signcryption.

Figure 4.2 Comparative computation cost of decryption-then-verification Vs Unsigncryption.

Figure 4.2 Communications overhead analysis.

List of Tables

Table 2.1 Shorthand digital signature.....17
Table 3.1 NIST recommended key size26
Table 3.2 Environment settings.....38

List of Abbreviations

AES	Advance Encryption Standard
CA	Certificate Authority
DES	Data Encryption Standard
IFP	Integer Factorization Problem
DLP	Discrete Logarithmic Problem
ECC	Elliptic Curve Cryptosystem
ECDLP	Elliptic Curve Discrete Logarithmic Problem
ECPA	Elliptic Curve Point Addition
HECC	Hyperelliptic Curve Cryptosystem
HECPM	Hyperelliptic Curve Point Multiplication
HECDLP	Hyperelliptic Curve Discrete Logarithmic Problem
HECDA	Hyperelliptic Curve Divisor Addition
HECDM	Hyperelliptic Curve Divisor Multiplication
DSS	Digital Signature Standard
SDSS	Shortened Digital Signature Scheme
SECDSS	Shortened Elliptic Curve Digital Signature Scheme
SHECDSS	Shortened Hyperelliptic Curve Digital Signature Scheme
KH	Keyed Hash Function
MAC	Message Authentication Code
MD	Message Digest
MIPS	Million of Instructions per Second
SHA	Secure Hash Algorithm

Chapter 1
Introduction

1.1 Introduction

Networks make dispersion of information rapidly fast. Most important factor associated with fast dispersion of information is its security, especially in wireless networks. Initially security is provided through private key encryption [1]. Introduction of public key or asymmetric encryption provided a new way to security and led towards authentication. In early day's confidentiality and authentication treated separately, however, if provided simultaneously total cost will be the sum of encryption and digital signature.

A new paradigm, signcryption provided both confidentiality and authentication simultaneously at less cost than combined cost of encryption and digital signature.

With the introduction of asymmetric cryptographic techniques it has become possible to achieve authenticity of the message; sender uses any one of the digital signature schemes depending upon the level of security. A decade before, message encryption and digital signature were viewed as important but distinct building blocks, a two step approach as "Signature-Then-Encryption". This approach has main drawback of high processing and communication cost. It has become possible to combine both the operations logically in a single step. This process is called Signcryption [1, 2], which simultaneously fulfills the security attributes of an encryption as well as digital signature. Various Signcryption schemes have been proposed based on ElGamal, RSA and Elliptic Curve Cryptography. There are still efforts required to develop such schemes based on hyper elliptic curve cryptography.

1.2 Cryptography

The term Cryptography have long history and derived from two Greek words *kryptós* and *gráphein*[3], *kryptós* means hidden or secrete and *gráphein* means to write. Cryptography is a practice of writing the messages in secret forms which are not understandable to unintended entities.

The need of Cryptography has felt when human being came out of caves; Egyptian first used cryptography in 1900 BC. In Greece civilization (486 BC) the known cryptographic technique was to write on a tape wrap a around a stick. In Roman Civilization the Caesar cipher (60 –50 BC) was the known cryptographic method. In modern age this field has extensive development and cryptographic technique has been standardized.

Cryptography broadly consists of two processes encryption and decryption. In encryption process we encode the information in such a way the unauthorized user must not read, while in decryption process we retrieve the original information from the coded one.

1.2.1 Encryption

Encryption is the process through which we conceal messages (plaintext) with the help of algorithms and keys such that unintended user cannot understand the message, Figure 1.1 shows the process. Encryption techniques are broadly classified into Symmetric and Asymmetric [3].

1.2.2 Symmetric Encryption

Symmetric Encryption is also called shared key Encryption. These Encryption techniques are based on substitution, transposition, mathematical functions or combination of these [4].

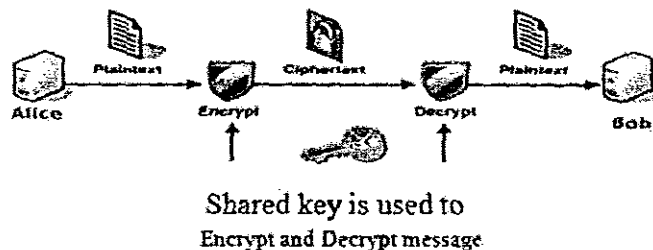


Figure 1.1 Symmetric key encryption

Symmetric encryption has low computational and communication cost as compared to asymmetric encryption [5]. The major shortcoming of this technique is key distribution. If we have n numbers of users to communicate with each other we need $n(n - 1)/2$ keys which are very expensive to distribute.

1.2.3 Asymmetric Encryption

Asymmetric Encryption use two keys public and private and are based on the hardness of some mathematical problem over a group structure [6]. The two popular problems are integer factorization problem and discrete logarithmic problem. Asymmetric Encryption techniques are costly in term of computation but have less problems of key distribution.

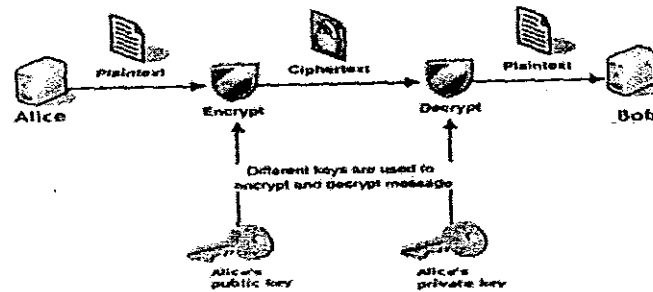


Figure 1.2 Asymmetric cryptosystem

The main group structures proposed for asymmetric encryption are:

1. The group of integers $Z(7, 8)$
2. The Abelian group of points on EC defined over finite Field F_q [9]
3. The group of Divisor of the Jacobian of HEC over finite field F_q [10]
4. The group of Divisor of the Jacobian of SEC over finite field F_q [11]
5. Two cyclic groups $(G, +)$ and (G, \cdot) of prime order [12]

1.3 Digital Signature

Digital signature is an authentication technique which uses private key of the creator and appends code bits to the original message which must verify the source and content of the message and verified by a third party in case of dispute. Digital signature technique can be broadly categorized as Direct approach and Arbitrated approach.

1.3.1 Direct Approach

Direct approach only involves sender and receiver, usually the sender encrypt the entire message or hash value of the message with his private key. Confidentiality is provided through encryption with public key.

The main drawback is the validity of the scheme is that it just depends on the sender private key, so the sender can claim that the key was stolen by someone and forged the signature.

1.3.2 Arbitrated Approach

In arbitrated approach [13] there is an arbitrator between sender and receiver, the sender sends a signed message to an arbitrator who verifies the origin and the content of the message and sends to receiver with an indication of verification.

1.3.3 Digital Signature Standard

NIST [14] published the Digital Signature Standard in FIPS 186 in 1991 and revised in 1993. DSS used digital signature algorithm based on the technique proposed by ElGamal [7]. Later on ECDSA [15] was proposed by Vanstone and HECDSA is a natural generalization of ECDSA.

1.4 Signature and Encryption

To maintain the confidentiality authenticity and integrity of the message at the same time, two approaches are used sign and encrypt or encrypt and sign, both method have their own merits and demerits.

1.4.1 Signature-Then-Encryption

The mostly used approach is *sign and encrypt*. In this approach for maintaining the confidentiality authenticity and integrity of the message, sender first digitally signs the message or its hash, then message and signature both are encrypted with receiver public key as in public key cryptosystem or shared symmetric key as in PGP. Receiver will first decrypt the message with his own private key or shared symmetric key and then verify using sender public key. The approach is similar to signing a letter and enclosed in envelope. The technique has drawbacks as loss of confidentiality in public verifiability, encryption is performed either the data is original or altered and lack of authentication in firewall application.

1.4.2 Encryption-Then-Signature

This is an alternative approach to *signature-then-encryption*, for maintaining the confidentiality authenticity and integrity of the message. The sender first encrypts the message and then digitally signs the cipher text or its hash value. Receiver will first verify the cipher text using sender public key and then decrypt the message with his own private key. The technique has drawbacks as the signature is easier to forge as to attack.

1.5 Shortcoming of Signature and Encryption

In any cryptosystem computation and communication cost matter and the main issue, either signature-then-encryption or encryption-then-signature the cost equals; the cost of signing and encryption, which consume more machine cycle and add redundant bits. Popular cryptosystem ElGamal is not suitable for encryption as it lead to expansion of cipher text, ECC and HECC leads to expansion as well as probabilistic

encryption, RSA also lead to expansion of message for small amount of data. Moreover the computation cost of public key cryptosystem is also high.

Is it possible to send a message of arbitrary length with cost less than that required by signature-then-encryption?

1.6 Signcryption

Y. Zheng [1] was the earliest who coined the word signcryption. He developed signcryption scheme based on ElGamal cryptosystem.

The motivation was to solve the challenge: "Whether it is possible to transport / store messages of varying length in a secure and authenticated way with an expense less than that required by Signature-Then-Encryption". Signcryption scheme have three phases keys generation, signcryption and Unsigncryption [1].

1.6.1 Notation Guide

The following notations are used to describe the system.

p : a large prime number (public to all)	y_b : Bob public key
q : a large prime factor of $p-1$ (public to all)	H : a one way hash function
g : a random integer $g \in [1,2, \dots p - 1]$	KH : Keyed hash function
x_a : Alice private key	m : Message
y_a : Alice public key	c : Cipher text
x_b : Bob private key	E_k/D_k : Symmetric Encryption/Decryption

1.6.2 Key Generation

For secure communication Alice and Bob will generate private and public keys.

Alice keys:

Alice selects " x_a " as private key randomly from $[1,2, \dots p - 1]$ and will calculate " y_a " as public key $y_a = g^{x_a} \text{ mod } p$

Bob keys:

Bob selects " x_b " as private key randomly from $[1,2, \dots p - 1]$ and will calculate " y_b " as public key $y_b = g^{x_b} \text{ mod } p$

1.6.3 Signcryption

The signcryption technique is used to generate signcrypted text, the detail is as under:

Signcryption $(m, p, q, g, x_a, y_a, y_b, hash, KH)$

1. Chose a random number $x \in [1, 2, \dots, q - 1]$
2. Calculate $k = y_b^x \text{ mod } p$
3. Split k into k_1 and k_2
4. Compute $r = KH_{k_2}(m)$
5. Compute s
 $s = x / (r + x_a) \text{ mod } q$ if SDSS₁ is used, or

$s = x / (1 + x_a \cdot r) \text{ mod } q$ if SDSS₂ is used

6. Symmetric encryption $c = E_{k_1}(m)$
7. Send Signcrypted text (c, r, s) to Bob

1.6.4 Unsigncryption

Bob receive signcrypted text, to obtain plain text and verify the text, the following

Unsigncryption technique:

Unsigncryption $(c, r, s, p, q, g, x_b, y_a, y_b, hash, KH)$

1. Compute $k = (y_a \cdot g^r)^{s \cdot x_b} \text{ mod } p$ if SDSS₁ is used, or
2. Compute $k = (g \cdot y_a^r)^{s \cdot x_b} \text{ mod } p$ if SDSS₂ is used
3. Split k into k_1 and k_2
4. Symmetric Decryption $m = D_{k_1}(c)$
5. Compute $KH_{k_2}(m)$
6. Message is valid if $KH_{k_2}(m) = r$

1.7 Signcryption Vs Signature & Encryption Cost Comparison

Computation cost and communication overhead are two basic parameters to measure the efficiency of any cryptographic technique. Signcryption technique has 50% less computation cost and 76.8% to 96.0% less communication overhead compare to signature-Then-Encryption technique using DSS and ElGamal encryption.

1.8 Signcryption Applications

As resource utilization is critical issue in future communication system due to its cost effectiveness; signcryption have application in information, Internet and network security. Here we present applications in some of the specific fields.

1.8.1 MANET and Sensor Networks

Mobile ad hock networks are gaining significant application in future communication. MANET has issue of energy and secure communication. Signcryption has less computation and communication cost and can handle these problems.

Signcryption minimize infrastructure support, key distribution and overcome computation and communication cost [16, 17, 18, 19, 20, 21, 22, 23].

Sensor networks are infrastructure less consist of nodes having limited energy, bandwidth. Signcryption provides cost effective security, save energy and bandwidth due to less computation and communication cost [24, 25, 26, 27].

1.8.2 Satellite Communication

Satellite communication has global application in science, entertainment, information sharing and military task. Secure satellite system is the need of the current age, due to cost effectiveness signcryption is the best choice for satellite to provide secure satellite communication [28, 29].

1.8.3 Electronic and Mobile Commerce

Conventional commerce is shifting to electronic where buying and selling are one click away from consumers such as Amazon and eBay. Mobile phones provide facility of internet access, as a result m-commerce gaining popularity. E&M commerce need strong security mechanism with low cost, where signcryption can provide secure and cost effective transaction [30, 31, 32].

1.9 Motivation

Asymmetric cryptosystems based on mathematical hard problem bring a revolution in the world of cryptography. Since 1976 till now different cryptosystems have been developed, all of them have their own advantages and limitations. The key size recommended beyond 2010 for cryptosystems on hard problem integer factorization such as El-Gamal, RSA cryptosystems is 2048 bits. Elliptic curve cryptosystem

reduce the key length significantly recommended key size beyond 2010 is 256 bits. The cryptosystem which provide highest security per bit is hyper elliptic curve cryptosystem [33], on its way from pure academic interest to industrial applications, out forming ECC in computation and communication cost, so this is attractive to use HECC for signcryption having significant application in this world of computing.

1.10 Thesis in Brief

The thesis consists of five chapters. First chapter is an introduction containing a brief historical background of encryption, digital signature, signature then encryption and Signcryption. Chapter two discusses various literature surveyed related to the work. Various Signcryption scheme based on elliptic curve and hyper elliptic curve cryptography are discussed .Chapter three consist of mathematical background. Chapter four contain proposed Signcryption schemes based on HECC. The security features along with the computation and communication cost are analyzed. Finally, Chapter five discusses the concluding remarks with the scope of further research direction.

Chapter 2

Literature Review

2.1 Literature Review

Literature review makes research more credible by providing information about the work already done in the specified area. In this thesis the literature review portion is divided in three portions for ease of understanding. Review schemes are categorized on the basis of DLP, ECDLP and HECDLP.

2.2 Schemes Based on Discrete Logarithm Problem

In this section we present review of those signcryption schemes which are based on DLP which state that: $x, y \in Z_p$ such that $y \neq 0$ and x is the generator of Z_p , finding a unique integer k , $0 \leq k \leq p - 1$ such that $y = x^k \text{ mod } p$, integer k is called discrete logarithm of y to the base x .

2.3.1. Parameters Setup

1. p : a large prime number ($p \geq 2^{1024}$)
2. q : a large prime factor of $p-1$ ($q \geq 2^{1024}$)
3. g : a random integer $g \in [1, 2, \dots, p - 1]$
4. x_a : Alice private key
5. y_a : Alice public key
6. x_b : Bob private key
7. y_b : Bob public key
8. h : a one way hash function
9. kh : Keyed hash function
10. m : Message
11. c : Cipher text
12. E_k/D_k : Symmetric Encryption / Decryption

2.2.1. Y. Zheng [1] Signcryption Scheme

Y. Zheng [1] was the earliest who coined the word signcryption. He developed signcryption scheme based on ElGamal cryptosystem. The motivation was to solve the challenge "Whether it is possible to transport / store messages of varying length in a secure and authenticated way with an expense less than that required by Signature – Then-Encryption". The proposed scheme logically combined the functionality of digital signature and encryption and reduced computation cost up to 50% and communication cost up to 85% compared to Signature-Then- Encryption technique. He was unable to develop such schemes based on popular public key cryptosystem

such as RSA and ECC, for which he put an open challenge for researcher. More over his scheme not provide feature like public verifiability and forward secrecy.

2.2.2. F. Bao and H. Deng [34] Signcryption Scheme

Zheng's signcryption scheme needs engagement in zero knowledge interactive protocol for verification of message by third party. F. Bao and H. Deng [34] design direct verifiable signcryption scheme. The proposed scheme computation cost is more than Zheng scheme, which overall reduced computation cost up to 16% and communication cost up to 85% compared to Signature-Then- Encryption technique. The scheme provides public verification of plaintext, which is a threat to confidentiality, moreover the computation cost significantly large compared to Zheng.

2.2.3. C. Gamage, J. Leiwo, and Y. Zheng [35] Signcryption Scheme

Traditional signcryption schemes allow message verification after decryption. Is it possible to check the authenticity of message at firewall without decryption? C. Gamage, J. Leiwo, and Y. Zheng [35] scheme is a modified form of F. Bao and H. Deng [2] signcryption and provides solution to the problem of authentication of secure message by firewall without disclosing message confidentiality, reduce computation cost up to 40% compared to traditional approach and communication cost is equivalent to Y, Zheng. Their scheme only verifies the cipher text to protect confidentiality of message in firewall application and don't provide feature like forward secrecy.

2.3. Schemes Based on Elliptic Curve Discrete Logarithm Problem

In this section we present review of those signcryption schemes which are based on ECDLP states that: P and Q are points on E such that order of P is n , find an integer k , $0 \leq k \leq n - 1$ such that $P = kQ$.

2.3.1. Parameters Setup

1. q : A large prime number ($q \geq 2^{160}$)
2. C : an Elliptic Curve over prime field F_q of order q
3. G : point of order ($n \geq 2^{160}$) chosen from points on C
4. d_a : Alice private key $d_a \in \{0, 1, 2, \dots, q - 1\}$
5. P_a : Alice public key $P_a = d_a G$
6. d_b : Bob private key $d_b \in \{0, 1, 2, \dots, q - 1\}$

7. P_b : Bob public key $P_b = d_b G$
8. h : a one way hash function
9. kh : Keyed hash function
10. m : Message
11. c : Cipher text
12. E_k/D_k : Symmetric Encryption / Decryption

2.3.2. Y. Zheng and H. Imai [36] Signcryption Scheme

Y. Zheng and H Imai [36] Proposed first signcryption scheme based on ECC. Compare to ElGamal and RSA Elliptic curve cryptosystem used small key size to provide equivalent security and attractive for resource constrained environment.

Proposed scheme

Alice needs to send a message m to Bob in an authenticated and confidential way:

Alice:

Signcryption $(m, n, q, d_a, P_a, P_b, H, KH, E_k)$

1. Select an integer $k \in \{1, 2, 3, \dots, n-1\}$ randomly
2. Compute kP_b
3. Compute $(K_1, K_2) = H(kP_b)$
4. $c = E_{K_1}(m)$
5. Compute $r = KH_{K_2}(m, bind_{info})$
6. $s = \left(\frac{k}{(r+d_a)}\right) \bmod n$ If ECDS₁ is used

$$s = \left(\frac{k}{(1+r.d_a)}\right) \bmod n \text{ If ECDS}_2 \text{ is used}$$

7. Signcrypted text for message m is (c, r, s)

Bob:

Unsignryption($c, r, s, n, q, d_b, P_a, P_b, H, KH, D_k$)

1. Compute $u = sd_b \text{ mod } n$
2. Compute $(K_1, K_2) = H(uP_a + urG)$ If ECDSS₁ is used
 Compute $(K_1, K_2) = H(urP_a + uG)$ If ECDSS₂ is used
3. Compute $m = D_{K_1}(c)$
4. Check $KH_{K_2}(m || \text{bind_info}) = r$, if satisfied accept the message, otherwise reject

The proposed scheme reduces the computation cost 58% and communication cost 40% when compared Signature-Then-Encryption based on ECC. The scheme has no facility like public verification and forward secrecy.

2.3.3. R. J. Hwang, C. H. Lai and F. F. Su [37] Signcryption Scheme

The previous schemes based on ECC lack direct public verifiability and forward secrecy. The motivation to R. J. Hwang, C. H. Lai and F. F. Su [37] Proposed scheme was public verifiable and forward secure signcryption scheme based on ECC.

Alice:

Signcryption ($m, n, q, d_a, P_a, P_b, H, KH, E_k$)

1. Verify Bob public key P_b using his certificate
2. Select an integer $k \in \{1, 2, 3, \dots, n-1\}$ randomly
3. Compute $(r_1, r_2) = R = kG$
4. Compute $(k_1, l) = K = kP_b$
5. Generate cipher text $c = E_{K_1}(m)$
6. Compute $h = H(m || r_1)$
7. $s = d_a - h.r \text{ mod } n$
8. Signcrypted text for message m is (c, r, s)

Bob:

Signcryption $(c, n, q, d_b, P_a, P_b, H, D_k)$

1. Verify Alice public key P_a using his certificate
2. Compute $(k_1, l) = d_b R$
3. Generate plain text $m = D_{K_1}(c)$
4. Compute $(r_1, r_2) = R$
5. Compute $h = H(m || r_1)$
6. Check $s * G + h * R = P_a$
7. if satisfied m is correct otherwise corrupted

Proposed scheme provide forward secrecy, however, the confidentiality of information sustain even if the sender private key disclosed. Trusted third party can verify the plaintext using (m, r, s) . The scheme has less computational cost at sender for sender side so more suitable for mobile devices.

In verification process the confidentiality of message not maintained. The computational cost is 40% more than [36].

2.3.4. M. Toorani and A.A. Beheshti Shirazi [38] Signcryption Scheme

Besides other flaws the computation and communication cost of previous signcryption schemes with public verifiability and forward secrecy are high. M. Toorani, A.A. Beheshti Shirazi [38] proposed scheme which decreases the computation and communication cost.

Proposed scheme

Alice:

Signcryption $(m, n, q, d_a, P_a, P_b, H, HMAC, E_k, ID_b, ID_A)$

1. Select an integer $k \in \{1, 2, 3, \dots, n-1\}$ randomly
2. Compute $(x_R, y_R) = R = kG$
3. Compute $(x_k, y_k) = K = (k + x_R d_a)P_b$
4. Compute $k_1 = H(x_k || ID_A || y_k || ID_b ||)$
5. Generate cipher text $c = E_{k_1}(m)$
6. Compute $t = HMAC_{k_1}(m || x_R || y_R || ID_b || ID_A)$

7. Compute $s = td_a - k \text{ mod } n$
8. Signcrypted text for message m is (c, R, s)

Bob:

Unsignryption $(c, R, s, n, q, d_b, P_a, P_b, H, HMAC, E_{k_1}, ID_b, ID_A)$

1. Validate public key P_a of Alice
2. Compute $(x_R, y_R) = R$
3. Compute $(x_k, y_k) = K = d_b(R + x_R P_a)$
4. Compute $k_1 = H(x_k || ID_A || y_k || ID_b ||)$
5. Generate cipher text $m = D_{k_1}(c)$
6. Compute $t = HMAC_{k_1}(m || x_R || y_R || ID_b || ID_A)$
7. Check $sG + R = tp_a$
8. if satisfied m is correct otherwise corrupted

The proposed scheme provides public verifiability and forward secrecy, suitable for store/forward applications and resource-constrained devices.

In the verification phase the session key is provided to the judge which becomes a serious threat to confidentiality.

2.3.5. R. K. Mohapatra and B. Majhi [39] Signcrypton Scheme

As resources are critical to utilize and such signcrypton schemes are needed having less computation and communication cost. R. K. Mohapatra and B. Majhi scheme [39] fulfill these needs.

Proposed scheme

Alice:

Signcrypton $(m, n, q, d_a, P_a, P_b, H, KH, E_k)$

1. Select an integer $k \in \{1, 2, 3, \dots, n-1\}$ randomly
2. Compute kP_b
3. Compute $k_1 = H(kG)$
4. Compute $(K_2, K_3) = H(kP_b)$
5. $c = E_{K_1}(m)$
6. Compute $r = KH_{K_3}(c || k_1 || ID_A || ID_b ||)$

7. $s = \left(\frac{k}{(r+d_a)} \right) \text{mod } n$
8. Compute $T = rG$
9. Signcrypted text for message m is (c, T, s)

Bob:

Unsignryption($c, r, s, n, q, d_b, P_a, P_b, H, KH, D_k$)

1. Compute $K_1 = H(sT + sP_a)$
2. Compute $(K_2, K_3) = H(d_b sT + d_b sP_a)$
3. Compute $r = KH_{K_3}(c || k_1 || ID_A || ID_b ||)$
4. Compute $m = D_{K_2}(c)$
8. Check $rG = T$, if satisfied accept the message, otherwise reject

Proposed signcryption schemes fulfill all the basic requirement of signcryption, directly public verifiable and provide forward secrecy. The scheme reduces communication overhead up to 42% compared to Signature-Then-Encryption.

2.4. Schemes Based on Hyperelliptic Curve Discrete Logarithm Problem

In this section we present review of those signature and encryption schemes which are based on HECDLP state that: D_1 and D_2 are divisor in the Jacobian J such that order of D_1 is n , find an integer k , $0 \leq k \leq n - 1$ such that $D_2 = kD_1$.

2.4.1. Parameters Setup

1. q : A large prime number ($q \geq 2^{80}$)
2. C : A Hyperelliptic Curve over prime field F_q
3. D : A divisor of large prime order n in $J_c(F_q)$, $n \geq 2^{80}$
4. d_a : Sender Alice private key $d_a \in \{0, 1, 2, \dots, p-1\}$
5. P_a : Sender Alice public key $P_a = d_a D$
6. d_b : Receiver Bob private key $d_b \in \{0, 1, 2, \dots, p-1\}$
7. P_b : Receiver Bob public key $P_b = d_b D$
8. φ : A function which map a divisor to integer value
9. h : a one way hash function
10. kh : Keyed hash function

11. m : Message
12. c : Cipher text
13. E_k/D_k : Symmetric Encryption / Decryption

In [60-62] proposed architectures for secure banking and e-commerce communication based on Hyperelliptic curve using HEC-ElGamal technique encryption [61] defined as follows

Encryption

1. Calculate $Q = kD$ and $Q = (u(x), v(x))$
2. Calculate $P_k = kP_b$ and $P_k = (u(x), v(x))$
3. Encode message to divisor: $m \xrightarrow{\text{divisors encoding}} P_m$
4. Calculate $C_m = (Q, P_m + P_k)$ or
 $C_m = ((u(x), v(x)), (u(x), v(x)))$

Decryption

Extract from $C_m = (Q, P_m + P_k)$

1. Calculate $\eta_b Q$
2. Extract $P_m + P_k$ from C_m
3. Calculate $P_m = P_m + P_k - \eta_b Q$
4. Extract message from divisor: $P_m \rightarrow m$

The architecture do not use standard digital signature to provide authenticity of information.

In [47] author proposed generalized equations for hyperelliptic curve digital signature algorithms (HECDSA) and shorthand digital signature which is defined in Table 1

Table 2.1: shorthand digital signature [47]

HECDSA *	Signing (r, s)	Verification
HECDSS ₁	$r = \text{hash}(\varphi(kD), m)$ $s = \left(\frac{k}{(r+d_a)} \right) \text{mod } n$	$R = s (P_a + rD)$ $r' = \varphi(R) \text{mod } n$ <p>Check $\text{hash}(r', m) = r$</p>
HECDSS ₂	$r = \text{hash}(\varphi(kD), m)$ $s = \left(\frac{k}{(1 + r \cdot d_a)} \right) \text{mod } n$	$R = s (rP_a + D)$ $r' = \varphi(R) \text{mod } n$ <p>Check $\text{hash}(r', m) = r$</p>

HECDSA and HEC-ElGamal are used to provide authenticity and confidentiality in hyperelliptic curve cryptosystem. These cryptosystems still having high computation cost and communication overhead are not suitable for resource constrained environments like wireless networks, satellite communication etc.

Due to its high reliability and efficiency and shorter parameters Hyperelliptic curve cryptosystem moving from academic interest to industrial application and provide the functionality of both encryption and digital signature.

2.5 Observation

On the basis of literature review it has been observed that till now different schemes have been proposed based on RSA, El-Gamal and ECC, among them Y. Zheng and H. Imai Signcryption scheme have less computation and communication cost but lack of forward secrecy and R. K. Mohapatra schemes have feature of forward secrecy and public variability with considerable less computation cost communication cost and both the schemes are based on ECC: Hyperelliptic curve cryptosystem use shorter parameters, low cost and high security per bit and more attractive for future cryptographic age. To replace HECC traditional approach signature and encryption by signcryption approach are not focused till now.

2.6 Problem Statement

Currently, there are different Signcryption techniques based on ElGamal, RSA and Elliptic Curve cryptography. Hyper elliptic curve cryptosystem provide high security per bit, use short parameters and high efficiency. To provide confidentiality and authenticity HECC use signature and encryption technique having following limitations.

1. High Cost, as cost of public key encryption is high compared to private key encryption plus cost of signature.
2. In encryption phase the plaintext is mapped to divisor (an element of Jacobian group)

$$m \xrightarrow{\text{divisors encoding}} P_m$$
 In some cases may not possible, due to which encryption become impractical.
3. Communication cost become at least double of plain text, as $P_m = ((u(x), v(x)))$ and $C_m = (((u(x), v(x)), (u(x), v(x))))$.
4. If private key of sender compromised the system becomes insecure.

2.7 Contribution

To overcome the limitations enlisted in problem statement portion we proposed three Signcryption schemes based on hyper elliptic curve cryptosystem. Proposed scheme one addresses problem one, proposed scheme two addresses all of the above mentioned problems while scheme three has additional property of direct public verifiability.

Chapter 3
Mathematical Background

3.1 Mathematical Background

In contrast to symmetric cryptosystem, asymmetric cryptosystem are purely mathematical based. The understanding of abstract algebra and theory of number are essential for understanding any asymmetric cryptosystem. Giving detail back ground in abstract algebra, theory of number and hyperelliptic curve cannot be covered in one chapter and at least one book needs be studied in each subject. In this chapter abstract level information is provided for detail good references for the study of abstract algebra are [40, 41] for number theory are [42] and for hyperelliptic curve [43, 44].

3.2 Abstract Algebra

The name algebra derived from the book title “الكتاب المختصر في حساب الجبر والمقابلة” written by Abu Ja'far Muhammad ibn Musa Al-Khwarizmi (780-850) one of the famous scholars in the “house of wisdom” in Baghdad. Abstract algebra is the study algebraic structure, which consist of set and operations on set e.g. Groups, Ring, field, vector spaces etc.

3.2.1 Algebraic properties

Let G be set, $+$ (addition) and $*$ (multiplication) be two binary operators

- I. Closed under addition: For all $a, b \in G$, $a + b \in G$
- II. Associative under addition: For all $a, b, c \in G$, $a + (b + c) = (a + b) + c$
- III. Additive Identity element: There is exist an element identity $e, g \in G$ such that $g + e = e + g = g$
- IV. Additive Inverse element: For all $a \in G$, there is an element $a^{-1} \in G$ such that $a + a^{-1} = e$
- V. Commutative under addition: For all $a, b \in G$, $a + b = b + a$
- VI. Closed under multiplication: For all $a, b \in G$, $a * b \in G$
- VII. Associative under multiplication: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$
- VIII. Distributive over addition: For all $a * (b + c) = a * b + a * c$
- IX. Commutative under multiplication: For all $a, b \in G$, $a * b = b * a$
- X. Multiplicative Identity: There is exist an element identity $e, g \in G$ such that $g * e = e * g = g$
- XI. Non zero divisor: For all $a, b \in G$, $a/b \in G$ such that $b \neq 0$

XII. Multiplicative Inverse: For all $a \in G$, there is an element $a^{-1} \in G$ such that $a * a^{-1} = e$

3.2.2 Algebraic Structures

Group $(G, +)$ is an algebraic structure formed by a set under one binary operator, while Ring and Field are algebraic structures $(G, +, *)$ under two binary operators satisfying certain axioms. The figure below demonstrates such algebraic structure.

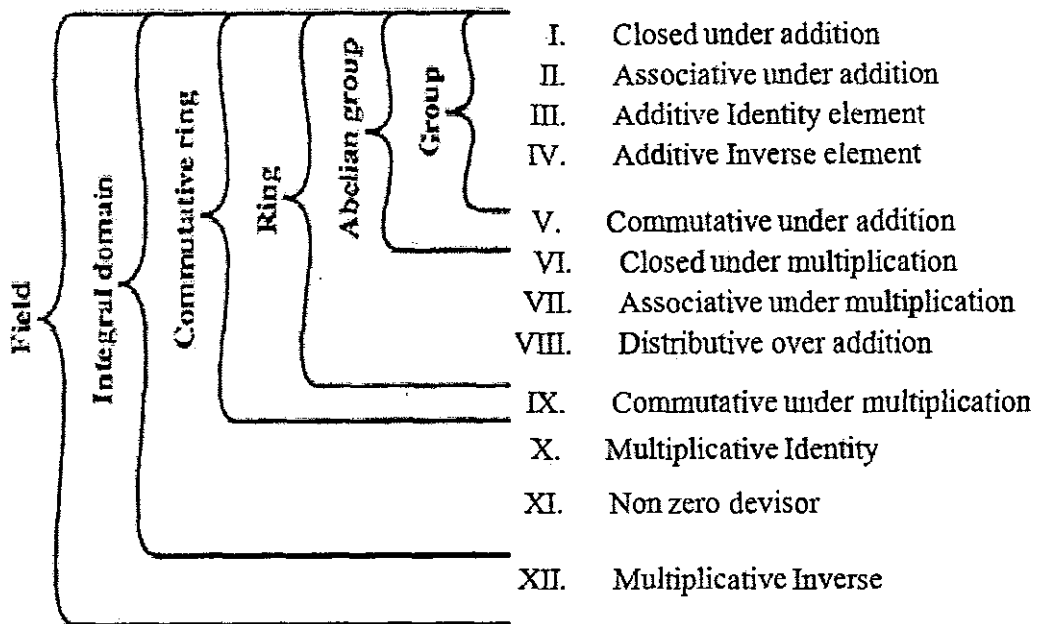


Figure 3.1 Algebraic structure

3.3 Hard Problems and Public Key Cryptosystems

Public key cryptography is based on mathematical function, which use two types of parameters' public and secret. Deriving secret parameters from public is equivalent to solving a mathematical problem. Complex problems leads to difficult derivation of secret parameters from public and provide stronger security. Two hard problems are popular for usage in cryptography.

3.3.1 Integer Factorization Problem

The splitting down of composite number into non trivial divisors such that when multiplied together equal to original composite number is called integer or prime factorization.

Integer factorization problem state that “given a composite integer n product of two prime number a and b , finds its two prime factors a, b

RSA cryptosystem based on IFP, as in RSA encryption public key is derived by multiplying two large prime numbers. To date, IFP is hard and there is no polynomial time algorithm available to solve.

3.3.2 Discrete Logarithmic Problem

Let Z_p be a group of prime order p , $x, y \in Z_p$ such that x is the generator of Z_p . Discrete logarithm problem: $x, y \in Z_p$ such that $y \neq 0$ and x is the generator of Z_p , find a unique integer k , $0 \leq k \leq p - 1$ such that $y = x^k \text{ mod } p$, integer k is called discrete logarithm of y to the base x .

3.3.3 Elliptic Curve Discrete Logarithm Problem

Let F_q be a finite field of order q , where q is either prime or in the form 2^m . E is an elliptic curve defined over F_q . Elliptic curve discrete logarithm problem: P and Q are points on E such that order of P is n , find an integer k , $0 \leq k \leq n - 1$ such that $P = kQ$.

3.3.4 Hyper Elliptic Curve Discrete Logarithm Problem

Let F_q be a finite field of prime order q . \mathbb{C} is a Hyperelliptic curve defined over F_q , \mathcal{J} is the Jacobian of \mathbb{C} . Hyperelliptic curve discrete logarithm problem: D_1 and D_2 are divisor in the Jacobian \mathcal{J} such that order of D_1 is n , find an integer k , $0 \leq k \leq n - 1$ such that $D_2 = kD_1$.

3.4 Hyper Elliptic Curve

Classifying on the basis of genus hyperelliptic curves are generalization of elliptic curve, having genus $g \geq 2$.

Let $h(x), f(x) \in Fq[x]$, $\text{deg } h(x) \leq g$, $f(x)$ is monic polynomial and $\text{deg } f(x) = 2g + 1$

A hyperelliptic curve \mathbb{C} of genus $g \geq 2$ over the field Fq is the set of points $(x, y) \in F \times F$ satisfy the equation

$$\mathbb{C}: y^2 + h(x)y = f(x) \quad (1)$$

And there are no points which simultaneously satisfy equation (1) and the partial derivate equations $2y + h(x) = 0, h(x)'y - f(x)' = 0$ of equation (1)

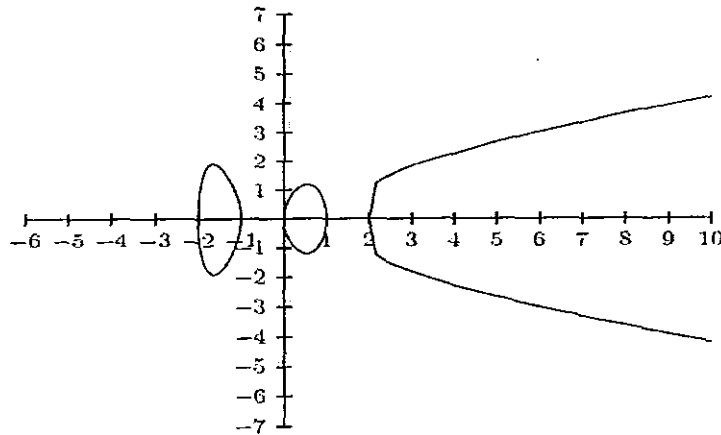


Figure 3.2 Hyperelliptic curve \mathbb{C} of genus $g=2$ $\mathbb{C}: y^2 = x(x^2 - 1)(x^2 - 4)$

3.4.1 Points on Hyper Elliptic Curve

The set of rational points is the set of points $p = (x, y) \in F \times F$ satisfy (1)

Point at infinity ∞ is a point in the projective plane lying on the line at infinity that satisfies the homogenized Hyperelliptic curves equation.

An extension field of F is K which contain all the finite points and point at infinity on \mathbb{C} . Opposite of a point $p = (x, y)$ denoted by $\tilde{p} = (x, -y - h(x))$ (\tilde{p} is on \mathbb{C}), the opposite of ∞ is $\tilde{\infty} \ni \tilde{\infty} = \infty$. A point p is special if $p = \tilde{p}$ otherwise ordinary.

3.4.2 Divisors

A divisor D is a finite formal sum of points $P_i = (x_i, y_i) \in \mathbb{C}, D = \sum m_i P_i, P_i \in \mathbb{C}, m_i \in \mathbb{Z}$.

The degree of the divisor $deg D = \sum_i m_i, suppD = \{P_i \in \mathbb{C} | m_i \neq 0\}$

Let a divisor $D = \sum_i m_i P_i, P_i \in \mathbb{C}, m_i \in \mathbb{Z}$ the set of divisor of degree zero are divisors such that $deg D = \sum_i m_i = 0$, form a group $\ni D^0 \subset D$. The set formed by the divisors of rational functions form the principal divisor denoted by $P \ni P \subset D^0$

A Jacobian J is the quotient of the group D^0 by P , formally $J = D^0 / P$. The Jacobian is finite quotient group and every element in the Jacobian is an equivalence class of

reduced divisor. The order of the Jacobian J according to [45] is calculated by the following inequality

$$|(\sqrt{q} - 1)^{2g}| \leq \#J/F_q \leq |(\sqrt{q} + 1)^{2g}|$$

A reduced divisor $D = \sum_i m_i P_i - (\sum_i m_i) \infty$ such that P_i are finite points on \mathbb{C} and ∞ is a point at infinity, if $P_i \in \text{supp} D$ then $\tilde{p} \notin \text{supp}(D)$ and $\sum m_i \leq g$

3.4.3 Representations of Divisors

There are different representations of reduced divisor but for implementation point of view the most popular representation is Mumford [46] representation

A reduced divisors $D = \sum m_i P_i - (\sum m_i) \infty$ where $P_i = (x_i, y_i)$ is a point on \mathbb{C} and m_i is the order of P_i is represented as a pair of polynomials $a(x), b(x)$, as $D = (a(x), b(x))$

Where

1. $a(x) = \prod (x - x_i)^{m_i}$ is monic polynomial
2. $b(x_i) = y_i$ and $\deg b(x) < \deg(a(x)) \leq g$
3. $a(x) | (b(x)^2 - h(x)b(x) - f(x))$

In case of genus $g = 2$

$$a(x) = x^2 + a_1 x + a_0$$

$$b(x) = b_1 x + b_0$$

Where $a_0, a_1, b_0, b_1 \in F_q$

3.4.5 Addition of Divisors

Divisor of hyperelliptic curve of genus one (elliptic curve) is a single point, using tangent and chord method we perform elliptic curve point addition as

We have elliptic curve defined by $y^2 = x^3 + ax + b(x - 2)(x - 4)$, P and Q are two points on the curve, to add these point we draw a line passing through P, Q and a third point R on the curve. The sum of P and Q is reflection of point R on x-axis is \tilde{R} , $\tilde{R} = P + Q$.

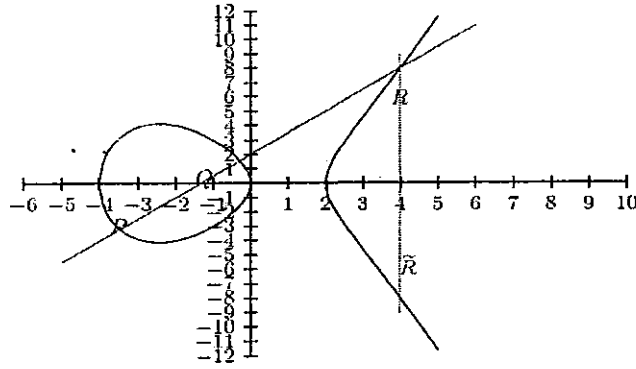


Figure 3.3 Elliptic curve point addition

3.4.5.1 Geometrically Addition of Divisors

Let $D_1 = \sum m_i P_i - (\sum m_i)\infty$ and $D_2 = \sum m_i Q_i - (\sum m_i)\infty$ be two divisors, $D_3 = D_1 + D_2$ is the sum of D_1 and D_2 , P_i and Q_i are points on hyperelliptic curve for ease of explanation $D_1 = P_1 + P_2 - 2\infty$, $D_2 = Q_1 + Q_2 - 2\infty$, D_1 is represented by blue curve, D_2 by red curve, we draw a third curve which passes through six points $P_1, P_2, Q_1, Q_2, R_1, R_2$, the projection of R_1, R_2 are $\widetilde{R}_1, \widetilde{R}_2$ which give divisor D_3 such that $D_3 = \widetilde{R}_1 + \widetilde{R}_2 - 2\infty$

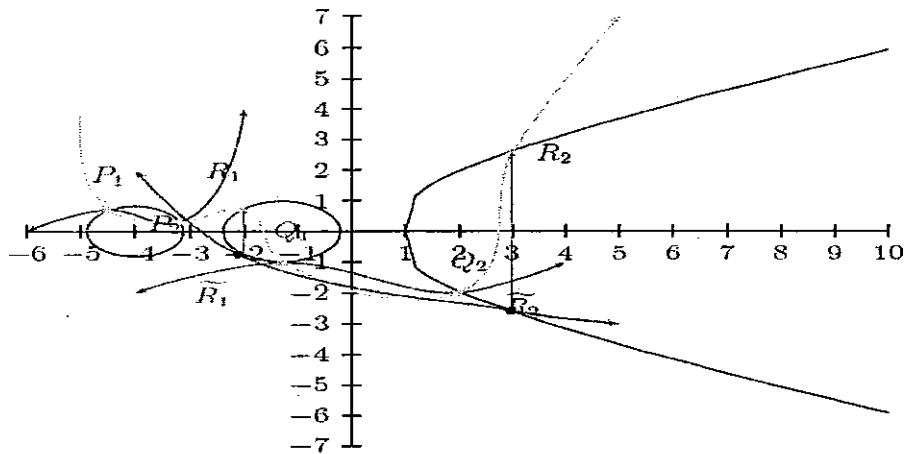


Figure 3.4 Hyperelliptic curve divisor addition

3.4.5.1 Algebraically Addition of Divisors

Geometric method is more complex to implement. In practically algebraic methods are used to add divisor, mostly using Mumford representation of divisor. Cantor [45] first proposed algorithm for addition of reduced divisor known as cantor algorithm.

3.5 Hyper Elliptic Curve Cryptosystem

HECC is prioritized over other cryptosystem due to High efficiency and shorter key size

Table 3.1: NIST recommended key size

Symmetric Cryptosystem	RSA and Diffie-Hellman	Elliptic Curve	Hyper Elliptic Curve
80	1024	160	80
112	2048	224	112
128	3072	256	128
192	7680	384	192
256	15360	512	256

Chapter 4

Proposed Signcryption Schemes

TH-8828

4.1 Proposed Signcryption Schemes

In this thesis we propose three signcryption schemes based on hyperelliptic curve cryptosystem having security features of message confidentiality, authenticity, integrity, non repudiation, public verifiability and forward secrecy. All the schemes have three phases; Initialization, Signcryption and Unsigncryption. In case of dispute between sender and receiver judge verification phase will be included. The proposed work is divided in three sections; in section one, proposed scheme has fulfill the security parameters of signcryption, in section two proposed scheme has additional feature of forward secrecy and in section three proposed scheme has properties of forward secrecy and direct public verifiability.

Parameters setup and notation guide is same as section 3.4.1

For secure communication Alice and Bob will generate their own private and public keys:

Alice selects private key $d_a \in \{1,2,3 \dots \dots q - 1\}$ randomly and compute public key $P_a = d_a D$

Bob selects private key $d_b \in \{1,2,3 \dots \dots q - 1\}$ randomly and compute public key $P_b = d_b D$

Alice and Bob exchange There public keys

4.2 Signcryption Scheme

4.2.1 Signcryption

Sender obtained receiver public key P_a from certificate authority and

Signcryption (k, P_b, P_a, d_a, m) technique is use to generate signcrypted text for message m .

Signcryption (k, P_b, P_a, d_a, m)

1. Select a Random integer $k \in \{0, 1, 2, 3 \dots \dots n - 1\}$
2. Compute kP_b
3. Compute $(K_1, K_2) = h(\varphi(kP_b))$
4. $c = E_{K_1}(m)$

5. Compute $r = h(c||K_2)$
6. Compute s

$$s = \left(\frac{k}{(r + d_a)} \right) \text{mod } n$$

7. Signcrypted text for message m is (c, r, s)

4.2.2 Unsignryption

Receiver obtain sender public key from certificate authority. Unsignryption (P_b, P_a, d_b, c, r, s) technique is use to obtain message "m" from signcrypted text (c, r, s) .

Unsignryption (P_b, P_a, d_b, c, r, s)

1. Compute $u = sd_b \text{mod } n$
2. Compute $u(P_a + rD)$
3. Compute $(K_1, K_2) = h(\varphi(u(P_a + rD)))$
4. Compute $r' = h(c||K_2)$
5. Compute $m = D_{K_1}(c)$
6. Check $r = r'$, if satisfied accept the message, otherwise reject

4.2.3 Correctness Proofs of the Proposed Scheme

Proof of decryption phase:

$$\begin{aligned} u(P_a + rD) &= sd_b(P_a + rD) = \left(\frac{k}{(r+d_a)} \right) d_b(P_a + rD) = \frac{kd_b(P_a+rD)}{(r+d_a)} \\ &= \frac{kd_bP_a + kd_b rD}{(r+d_a)} = \frac{d_a kP_b + kd_b rD}{(r+d_a)} = \frac{d_a kP_b + rkd_b D}{(r+d_a)} \\ &= \frac{d_a kP_b + r kP_b}{(r+d_a)} = \frac{kP_b(d_a + r)}{(r+d_a)} = kP_b \end{aligned}$$

4.2.4 Security Analysis of Proposed Scheme

Security analysis is one of the important aspects of any signcryption scheme. Table shows the security analysis of our proposed schemes along with existing schemes. The analysis is based on the assumption that HECDLP is hard and infeasible to solve

4.2.4.1 Confidentiality

To be confidential, information should be only intangible to unauthorized access and non intangible to eavesdropper/ interceptor [48]. If an adversary want to get session key k ; he/she need to calculate d_b from $p_b = d_b D$ or d_a and r from $p_a = d_a D$ and $R = rD$ which is equivalent to solving one and two HCDLP.

4.2.4.2 Integrity

Integrity check insures that the data has not been changed and is that one send by the sender. As due to the property of Random Oracle Model "it is infeasible that two different messages have same digest/hash value" [50]. In our schemes the receiver calculates digest/hash value r of c and checking integrity by comparing $rD = R$, if attacker changes c to c' then $rD \neq R$ due to property of Random Oracle Model.

4.2.4.3 Authenticity

The property that we associate with entity from where it came is called authenticity. In our proposed schemes s is used to calculate K_1 which is used to calculate r and the authenticity is checking by $rD = R$. In case of dispute judge can verify the authenticity of the message by involving in zero knowledge protocol with Bob in case of schemes of type one or directly in schemes two.

4.2.4.4 Unforgeability

Unforgeability means it is infeasible for an attacker to create valid signature without secret key [49]. The proposed signcryption schemes are unforgeable as that is based on unforgeable HECDSA.

4.2.4.5 Non repudiation

Non repudiation restricts sender from denying the signcrypted text he/she sent. Unforgeability insures non repudiation [51]. If sender denies, recipient send signcrypted text to judge. By using verification technique judge can decide that the message is sent by he/she.

4.3 Signcryption Scheme with Forward Secrecy

In this section we proposed four signcryption schemes public verifiable through zero knowledge protocol.

4.3.1 Signcryption

Signcryption (k, P_b, P_a, d_a, h, m) technique is used to generate signcrypted text for message m .

Signcryption (k, P_b, P_a, d_a, h, m)

1. Select an integer $k \in \{0, 1, 2, 3 \dots \dots n - 1\}$ randomly
2. Compute kP_b
3. Compute $(K_1, K_2) = h(\varphi(kP_b))$
4. $c = E_{K_1}(m)$
5. Compute $r = h(c \parallel K_2)$
6. Compute $s = \left(\frac{k}{r+d_a}\right) \bmod n$
7. Compute $R = rD$
8. Send Signcrypted message as (c, R, s)

4.3.2 Unsigncryption

Bob receive signcrypted text, to obtain plain text and verifies, the following Unsigncryption (P_b, P_a, d_b, c, R, s) technique is use to obtain message "m" from signcrypted text (c, R, s) .

Unsigncryption $(k, P_b, P_a, d_b, h, c, R, s)$

1. Compute $u = sd_b$
2. Compute $(K_1, K_2) = h(\varphi(u(P_a + R)))$
3. Compute $r = h(c \parallel K_2)$
4. $m = D_{K_1}(c)$
5. Check $rD = R$ if satisfied accept the message, otherwise reject

4.3.3 Correctness Proofs of the Proposed Scheme

Proof of decryption phase:

$$\begin{aligned}
 sd_b(P_a + R) &= \left(\frac{k}{(r + d_a)} \right) d_b(P_a + R) = \frac{kd_b(P_a + R)}{(r + d_a)} = \frac{kd_bP_a + kd_bR}{(r + d_a)} \\
 &= \frac{d_a k P_b + kd_b r D}{(r + d_a)} = \frac{d_a k P_b + r k d_b D}{(r + d_a)} = \frac{d_a k P_b + r k P_b}{(r + d_a)} \\
 &= \frac{k P_b (d_a + r)}{(r + d_a)} = k P_b
 \end{aligned}$$

4.3.4 Security Analysis of Proposed Scheme

Proposed scheme in this section fulfill all the security parameters of Scheme presented in section 4.2 and have additional property of Forward Secrecy.

4.3.4.1 Forward Secrecy

Forward secrecy implies that session key used in communication would not be compromised even if a long term private key is disclosed [52]. In our proposed schemes if an adversary gets d_a for calculating session key k need r . Calculating r is equivalent to solve computational hard problem HECDLP or finding the value of two unknown from one equation.

4.4 Signcryption Schemes with Forward Secrecy and Public Verifiability

In this section we have proposed two signcryption technique based on hyperelliptic curve cryptosystem which are directly verifiable.

4.4.1 Signcryption

Signcryption (k, P_b, P_a, d_a, m) technique is used to generate signcrypted text for message m .

Signcryption (k, P_b, P_a, d_a, h, m)

1. Select an integer $k \in \{0, 1, 2, 3 \dots \dots n - 1\}$ randomly
2. Compute kP_b
3. $(K_1) = h(\varphi(kD))$
4. $(K_2) = h(\varphi(kP_b))$

5. $c = E_{K_2}(m)$
6. Compute $r = h(m \parallel K_1)$
7. Compute $s = \left(\frac{k}{(r+d_a)}\right) \bmod n$
8. Compute $R = rD$
9. Signcrypt text for message m is (c, R, s)

4.4.2 Unsignryption

Bob receive signcrypt text, to obtain plain text and verifies, the following Unsignryption (P_b, P_a, d_b, c, R, s) technique is used to obtain message "m" from signcrypt text (c, R, s) .

Unsignryption $(k, P_b, P_a, d_b, h, c, s)$

1. Compute (K_1, K_2)

$$(K_1) = h(\varphi s(P_a + R))$$

$$(K_2) = h(\varphi(sd_b(P_a + R)))$$
2. $m = D_{K_2}(c)$
3. Compute $r = h(m \parallel K_1)$
4. Check $rD = R$ if satisfied accept the message, otherwise reject

4.4.3 Proofs of the Proposed Scheme

Proof of decryption phase:

$$\begin{aligned} sd_b(P_a + R) &= \left(\frac{k}{(r+d_a)}\right) d_b(P_a + R) = \frac{kd_b(P_a + R)}{(r+d_a)} = \frac{kd_bP_a + kd_bR}{(r+d_a)} \\ &= \frac{d_a kP_b + kd_b rD}{(r+d_a)} = \frac{d_a kP_b + rkd_b D}{(r+d_a)} = \frac{d_a kP_b + rkP_b}{(r+d_a)} \\ &= \frac{kP_b(d_a + r)}{(r+d_a)} = kP_b \end{aligned}$$

4.4.4 Security Analysis of Proposed Scheme

Proposed scheme in this section fulfills all the security parameters of Scheme presented in section 4.3 and have additional property of direct public verifiability.

4.4.4.1 Public Verifiability

The property; when Alice denies his sign the recipient Bob can prove in a secure way that just Alice has signed the message [53]. In our proposed schemes one for public verification the receiver need to engage with judge in zero-knowledge protocol [54] while in schemes two the signcrypted text is directly verified by judge.

4.4.4.1 Verification by Judge

When dispute occurs between sender and receiver the trusted third party or judge can resolve the dispute as:

In case of dispute Bob provide (P_a, m, R, s) to judge

Verification process:

Compute $(K_1) = h(\varphi s(P_a + R))$

Compute $r = h(m \parallel K_1)$

Check $rD = R$ if satisfied the signcrypted text is valid, otherwise not

4.4.4.2 Proof of Verification Phase:

$$\begin{aligned} s(P_a + R) &= \left(\frac{k}{(r + d_a)} \right) (P_a + R) = \frac{k(P_a + R)}{(r + d_a)} = \frac{k(d_a D + rD)}{(r + d_a)} \\ &= \frac{k(d_a D + rD)}{(r + d_a)} = \frac{kD(d_a + r)}{(r + d_a)} \\ &= \frac{kD(r + d_a)}{(r + d_a)} = kD \end{aligned}$$

4.5 Cost analysis of Proposed Schemes and Results

Cost is one of the major parameters of any cryptographic technique. We presented two type of cost analysis computation cost and communication overhead of the proposed signcryption schemes and existing signature-Then-Encryption scheme.

Table 3.2: Environment settings

Operating System	Window Vista 32 bit
System RAM,	RAM 3GB
Processor	Core 2 Duo 1.83 GHZ
Programming Language	V C++ (Visual Studio 2008)
Hyperelliptic Curve \mathbb{C} $y^2 = x^5 + 153834295433461683634059x^3 + 1503542947764347319629935x^2 + 1930714025804554453580068x^1 + 790992824799875905266969$	
Divisor $D = (x^2 + 4044270522993724839132540x + 9302566344691261900012434, 8758011889586115776259440x + 11434287076605500196003050)$ $q = 15502234002335423222711631$ $n = 9833557797934760928301623$	
Asymmetric Encryption/Decryption	HEC-El-Gamal
Symmetric Encryption/Decryption	AES
Digital Signature	S-HECDSA
Hash Function	SHA-128
Data Set	128 bits (Session key) 1280 bits (a text message 160 Character) 7168 bits (An E- mail)

4.4.5.1 Computation Cost Analysis of Proposed Schemes and Results

Computation cost is calculated as the time taken in ms by existing signature-Then-Encryption and proposed signcryption approaches. The Figure 4.1 shows the Comparative computation cost of Sign-then-Encryption Vs Signcryption and Figure 4.2 shows the Comparative computation cost of Decryption-Then-Verification Vs Unsigncryption.

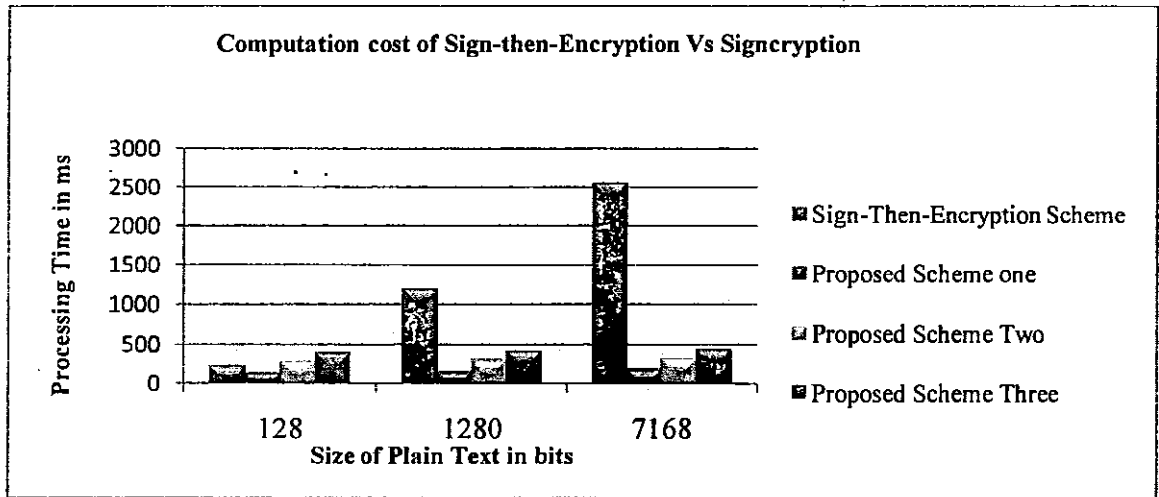


Figure 4.1 Comparative computation cost of sign-then-encryption Vs Signcryption

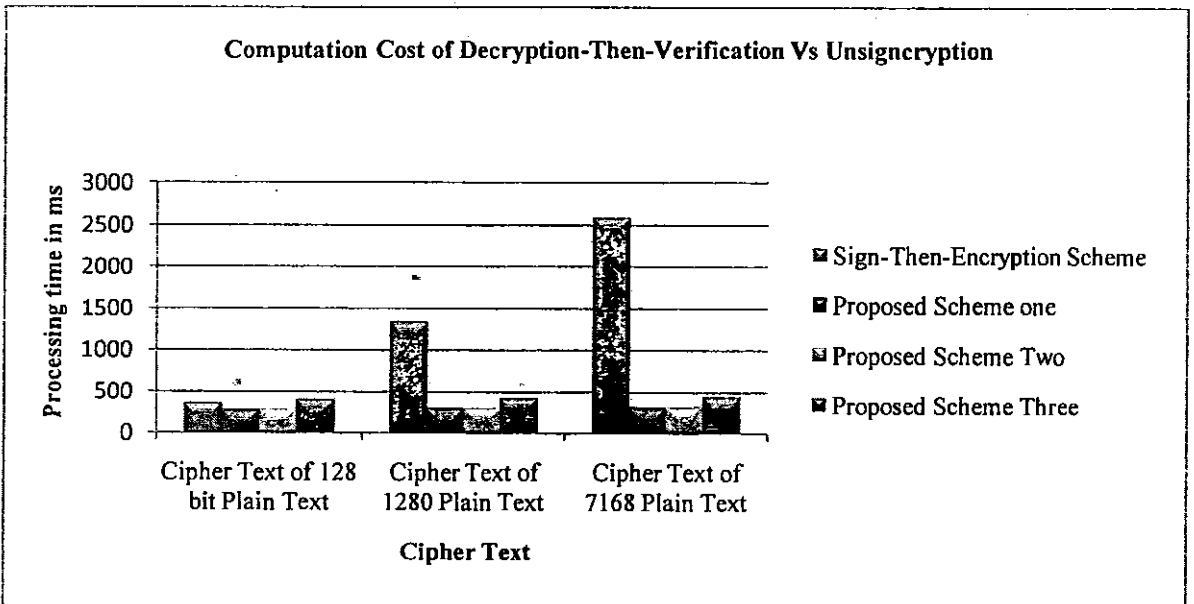


Figure 4.2 Comparative computation cost of decryption-Then-verification Vs Unsigncryption

4.4.5.2 Communication Overhead Analysis of Proposed Schemes

Communication cost depends on the choice of parameters and amount of information. Communication cost is calculated as the size of plain text Vs signcrypted text in bits of existing signature-Then-Encryption and proposed signcryption approaches. The Figure 4.3 shows the Comparative Communication overhead analysis of Sign-then-Encryption Vs Signcryption.

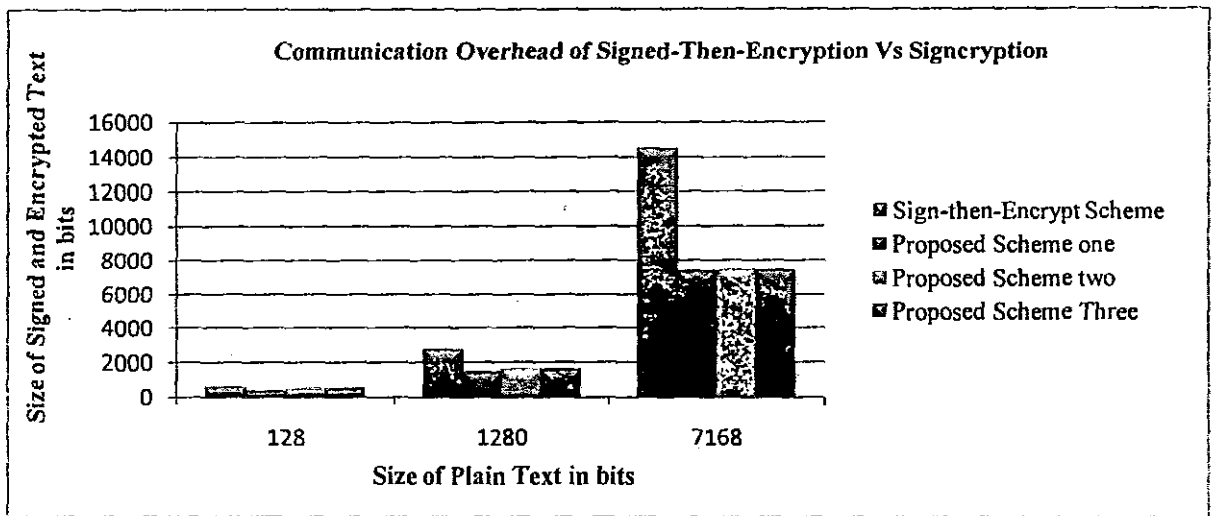


Figure 4.3 Communications overhead analysis

Chapter 5
Conclusion and Future Work

5.1 Conclusion

In this thesis we presented four signcryption schemes based on hyperelliptic curve cryptography for confidential and authenticated message delivery. The proposed schemes fulfill all the security parameters of signcryption and equivalent in function to signature-Then-encryption technique with less computation cost and communication overhead. The proposed schemes provide the functionality of forward secrecy and public verifiability. The schemes are based on the HECDLP which is more difficult than IFP, DLP and ECDLP. Proposed schemes have less computation cost and communication overhead and more suitable for restricted computation devices.

5.2 Limitations of the Proposed Work

Hyperelliptic curve cryptosystem parameters must be chosen in a secure way to make it difficult for an attacker to solve HECDLP. Schemes have limitation of additional special property like proxy group signcryption.

5.3 Future Direction

Elliptic curve points have compressed representation which reduces communication overhead significantly, like ECC point compression divisor in HEC cryptosystem need compressed representation.

Generalized signcryption schemes based on HECC can be developed to achieve confidentiality only, authenticity only and both confidentiality and authenticity.

Secure Sockets Layer (SSL), the Internet security protocol for point-to-point connections provides protection against eavesdropping, tampering, and forgery. SSL was developed by Netscape and its version 3.0 has been implemented in many web browsers (e.g., Netscape Navigator and MS Internet Explorer) and web servers widely used on the Internet. TLS can be viewed as SSL v3.1. SSL Cipher suite contains asymmetric cryptosystem for key exchange, digital signature and symmetric key cryptosystem for encryption. SSL Cipher suite:

RSA, DES (in different modes), RC (4, 5, 6), HASH, MAC, HMAC, ECC, DSA, MD5, DH) [56-59]. Signcryption schemes based on hyperelliptic curve cryptosystem can be used as cipher suite in SSL/TLS.

IPSec an IP layer protocol used to secure service..... IPSec provide either confidentiality and authenticity or authenticity using RSA, DSA and symmetric encryption technique. Generalized signcryption schemes based on Hyperelliptic curve can be implemented in IPSec to gain efficiency.

MANET and sensor networks have issue of energy and secure communication due to high computation and communication cost public key cryptosystem are not preferred, while symmetric cryptosystem have limitation of key distribution, to handle these problems Signcryption schemes based on HECC can be used which have less computation cost, communication overhead and key distribution problem.

Satellite communication has global application in science, entertainment, information sharing and military task. Secure satellite system is the need of the current age; due to cost effectiveness signcryption schemes based on HECC is good choice and can be implemented in satellite network for secure communication.

References

- [1] Y. Zheng. "Digital signcryption or how to achieve cost (signature encryption) \ll cost (signature) + cost (encryption)" In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pp 165-179, London, UK, 1997.Springer-Verlag.
- [2] Y. Zheng, J. Baek and R. Steinfeld "Formal proofs for the security of Signcryption" *Journal of Cryptology*, 20(2):pp 203-235, 2007.
- [3] G. Daniel and V.Salvador "Topics in the Theory of Algebraic Function Fields" pp 353-375 -2006.
- [4] W. Stallings "Cryptography and Network Security: Principles and Practice" Prentice Hall fifth edition 2010.
- [5] W. Mao "Modern Cryptography: Theory and Practice" Prentice Hall July 25, 2003
- [6] C. Paul and J. Menezes, A. Vanstone "Handbook of Applied Cryptography" CRC Press, 1996.
- [7] T. ElGamal "A public key cryptosystem and a signature scheme based on discrete logarithm" *IEEE transaction on information theory* 31, pp 469-472 1985.
- [8] R. L. Rivest, A. shamer and L. M. adleman "A method for obtaining digital signature and public key cryptosystem" *communication ACM* 21, pp120-126, 1978.
- [9] N. Koblitz "Elliptic curve cryptosystem" *Math computation* 1985.
- [10] N. Koblitz "Hyperelliptic curve cryptosystem" *journal of cryptology* Volume 1, Number 3, pp 139-150 1989.
- [11] S. Gaudry, Pauls and N. smart "Arithmetic of super elliptic curve" *Math computation* 2002.
- [12] T. Okamoto "Cryptography Based on Bilinear Maps" *AAECC 2006, LNCS 3857*, pp. 35-50, 2006.
- [13] S. Akl "Digital signature: A tutorial survey" *Computer* February 1983.
- [14] National Institute of Standards and Technology Digital Signature Standard Federal Information Processing Standard (FIPS) PUB 186, 1993.
- [15] S. Vanstone, "Responses to NIST's Proposal", *Communications of the ACM*, 35, pp 50-52, July 1992.

- [16] Stephen, F. Bush and A. B. Kulkarni, "Advances in Resource Constrained Device Networking" *Wireless Communication and Mobile Computing* pp821–822, July, 2007.
- [17] Y. Han, X. Gui and X. Wang "Multi-Recipient Signcryption for Secure Wireless Group Communication"
- [18] M. Bohio and A. Miri "An Authenticated Broadcasting Scheme for Wireless Ad hoc Network" *IEEE Second Annual Conference on Communication Networks and Services Research* 2004.
- [19] R. Vijayan and S. Singh "A Novel approach for Implementing Security over Vehicular Ad hoc network using Signcryption through Network Grid" *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 4, 2011.
- [20] S. Singh and R. Vijayan "Enhanced Security for Information Flow in VANET using Signcryption and Trust level" *International Journal of Computer Applications* Volume 16– No.5, February 2011.
- [21] A. A. Yavuz1, F. Alagoz and E. Anarim "HIMUTSIS: Hierarchical Multi-tier Adaptive Ad-Hoc Network Security Protocol Based on Signcryption Type Key Exchange Schemes" *ISCIS 2006, LNCS 4263*, pp. 434–444, 2006. Springer-Verlag Berlin Heidelberg 2006.
- [22] A.A. YAVUZ1, F. ALAGOZ and E. ANARIM "A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption" *Turk Journal Electrical Engineering & Computer Science*, Vol.18, No.1, 2010.
- [23] Z. Chuanrong and X. Hong "Threshold Key Management Protocol in Mobile Ad Hoc Networks Using an ID-based Signcryption Scheme" *International Conference*, pp233 – 237, 2009.
- [24] G. Yang1, C. Rong, C. Veigner, J. Wang and H. Cheng "Identity-Based Key Agreement and Encryption for Wireless Sensor Networks" *International Journal of Computer Science and Network Security*, VOL.6 No.5B, May 2006.
- [25] I. T. Kim and S. O. Hwang" An Efficient Identity-Based Broadcast Signcryption Scheme for Wireless Sensor Networks" *6th International Symposium on Wireless and Pervasive Computing (ISWPC)*, pp 1-6, 2011.
- [26] A. Hagra, H. Aly and D. El-Saied "An Efficient Key Management Scheme based on Elliptic Curve Signcryption for Heterogeneous Wireless Sensor Networks"

International Journal of Computer Science and Technology Vol. 1, Issue 2, December 2010.

- [27] N. Sultana and E. Huh "Secure Group Communication in Mobile Wireless Sensor Networks" International Conference on Advanced Communication Technology, 2008. ICACT, pp 136 – 141, 2088.
- [28] P. Chang-yan, Z. Quan and T. Chao-jing "A Secure On-Demand Routing Protocol for LEO Satellite Networks" Signal processing Vol 26, No. 3, March 2010.
- [29] A. A. Yavuz, F. Alagz and E. Anarim "NAMEPS: N -Tier Satellite Multicast Security Protocol Based on Signcryption Schemes" IEEE GLOBECOM, 2006.
- [30] Y. Wang and T. Li "LITSESET/A++: A New Agent-assisted Secure Payment Protocol" IEEE International Conference on E-Commerce Technology 2004.
- [31] Z. Chuanrong and Z. Yuqing "Secure Mobile Agent Protocol by Using Signcryption Schemes" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC '09. pp 108 – 112, 2009
- [32] X. YI, C. K. Siew, X. F. Wang and E. Okamoto "A Secure Agent-based Framework for Internet Trading in Mobile Computing Environments" Distributed and Parallel Databases, 8, 85–117 2000.
- [33] Erickson, Stefan Jacobson, Jr., Michael Stein and Andreas "Explicit formulas for real hyperelliptic curves of genus 2 in affine representation" Advances in Mathematics of Communications 5(4), (2011)
- [34] R, Deng, F, Bao "A signcryption scheme with signature directly verifiable by public key" Proceedings of PKC'98 LNCS 1431, pp 55-59, 1998.
- [35] C. Gamage, J. Leiwo, and Y. Zheng "Encrypted message authentication by firewalls" In Proc. of PKC99, LNCS 1560, pp 69-81. Springer-Verlag, 1999.
- [36] Y. Zheng and H. Imai "How to construct signcryption schemes on elliptic curve" Information processing Letters 68 pp 227-233 1998.
- [37] Ren-Junn Hwang , Chih-Hua Lai, Feng-Fu Su "An efficient signcryption scheme with forward secrecy based on elliptic curve" Applied Mathematics and Computation, 167(2): pp 870 -881, 2005.
- [38] M. Toorani, A.A. Beheshti Shirazi "An Elliptic Curve-based Signcryption Scheme with Forward Secrecy" Journal of Applied Sciences Vol.9, No.6, pp.1025-1035, 2009.

- [39] R. K. Mohapatra and B. Majhi "Signcryption Schemes with Forward Secrecy Based on Elliptic Curve Cryptography" MT Thesis Department of Computer Science and Engineering National Institute of Technology Rourkela Rourke.
- [40] J. A. Beachy and W. D. Blair "ABSTRACT ALGEBRA" Third Edition ISBN 157766-434-4, Waveland Press, Inc. 2005.
- [41] T. W. Judson "Abstract Algebra Theory and Applications" Stephen F. Austin State University August 27, abstract.pugetsound.edu 2010.
- [42] J. H. Silverman "A Friendly Introduction to Number Theory" Third Edition, ISBN: 0-13-186137-9 Pearson Prentice Hall 2006.
- [43] Sandeep Sadanandan "Addition of Jacobian of Hyperelliptic Curves" M Tech thesis Indian Institute of Technology Madras, Chennai 2004.
- [44] W. Fulton "Algebraic curves" Third Edition Addison-Wesley 2008.
- [45] D.G. Cantor "Computing in Jacobian of a Hyperelliptic Curve" In Mathematics of Computation, volume 48 (177), pp 95-101, January 1987.
- [46] D. Mumford. "Tata Lectures on Theta II" Progress in Mathematics, vol 43, Birkhauser, 1984.
- [47] Y. Lin and S. Yong-xuan "Effective generalized equations of secure hyperelliptic curve digital signature algorithms" The Journal of China Universities of Posts and Telecommunications 17(2) pp 100–108 April 2010.
- [48] ISO/IEC 17799.
- [49] K. Kim, I. Yie and D. Nyang "On the Security of Two Group Signature Schemes with Forward Security" Informatica Vol 34 pp 237–242 June 2010.
- [50] Jonathan Katz and Yehuda Lindell "Introduction to Modern Cryptography" Chapman and Hall/CRC 2007.
- [51] Colleen M. Swanson and Douglas R. Stinson "Unconditionally Secure Signature Schemes Revisited" Information Theoretic Security Lecture Notes in Computer Science, Volume 6673/2011, 2011.
- [52] DongGook Park, Colin Boyd, and Sang-Jae Moon "Forward Secrecy and Its Application to Future Mobile Communications Security" Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography 2000.

- [53] Lei Feiyu, Chen Wen and Chen Kefei "A generic solution to realize public verifiability of signcryption" Wuhan University Journal of Natural Sciences Volume 11, Number 6 2006.
- [54] http://wiki.answers.com/Q/What_is_the_average_size_of_email.
- [55] K. Chatterjee, A. De and D. Gupta "Software Implementation of Curve based Cryptography for Constrained Devices" International Journal of Computer Applications pp 0975 – 8887 Volume 24– No.5, June 2011.
- [56] Johann Großschädl "Performance and Security Aspects of Client-Side SSL/TLS Processing on Mobile Devices" First International Workshop on Constructive Side-Channel Analysis and Secure Design COSADE 2010.
- [57] Yunyoung Lee, Soonhaeng Hur, Dongho Won, and Seungjoo Kim "Cipher Suite Setting Problem of SSL Protocol and It's Solutions" IEEE International Conference on Advanced Information Networking and Applications Workshops 2009.
- [58] Luo Qing, Lin Yaping "Analysis and Comparison of Several algorithms in SSL/TLS Handshake Protocol" IEEE International Conference on Information Technology and Computer Science 2009.
- [59] Zhao Huawei, and Liu Ruixia "A Scheme to Improve Security of SSL" Pacific-Asia Conference on Circuits, Communications and System 2009.
- [60] R. Ganesan and K. Vivekanandan "A Novel Hybrid Security Model for E-Commerce Channel" International Conference on Advances in Recent Technologies in Communication and Computing 2009.
- [61] R. Ganesan and K. Vivekanandan "A Secured Hybrid Architecture Model for Internet Banking (e-Banking) Journal of Internet Banking and Commerce vol. 14, no.1 April 2009.
- [62] R. Ganesan, M. Gobil and K. Vivekanandan "A Novel Digital Envelope Approach for A Secure E-Commerce Channel" International Journal of Network Security, Vol.11, No.3, PP.121127, Nov. 2010.