A NOVEL BLIND SIGNATURE BASED UPON ECDLP

A THESIS SUBMITTED IN PARTIAL FULLFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

BACHELORS OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

BY

ABHIJIT SAMAL (107CS025)
ANIMESH CHHOTARAY (107CS033)

Under the Guidance of
Prof. SUJATA MOHANTY

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

National Institute of Technology

Rourkela

CERTIFICATE

This is to certify that the thesis entitled, **A BLIND SIGNATURE SCHEME BASED UPON ECDLP** submitted by Abhijit Samal, Roll No: 107CS025 and Animesh Chhotaray, Roll No: 107CS033 in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Computer Science and Engineering at the National Institute of Technology, Rourkela is an authentic work carried out by them under my supervision and guidance. To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other university / institute for the award of any Degree or Diploma

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other university / institute for the award of any Degree or Diploma

Prof. Sujata Mohanty

Dept. of Computer Science and Engineering

National Institute of Technology Rourkela - 769008

ACKNOWLEDGEMENT

We avail this opportunity to extend our hearty indebtedness to our guide **Prof. Sujata Mohanty**, Computer Science Engineering Department, for her valuable guidance, constant encouragement and kind help at different stages for the execution of this dissertation work.

We also express our sincere gratitude to **Prof. A.K. Turuk**, Head of the Department, Computer Science Engineering, for providing valuable departmental facilities.

Submitted by :

Animesh Chhotaray
Roll no: 107CS033

Abhijit Samal
Roll no:107CS025

Abstract

Encryption and decryption techniques protect the confidentiality of information exchanged in a network whereas digital signature is electronic signing of data that provide senders authentication using its secret key and verification using its public key and other domain parameters. A combination of encipherment and digital signing of message immunes it from most of the active attacks such as modification of data, masquerading and repudiation Elliptic curve discrete logarithmic problem (ECDLP) is the problem of finding the scalar multiplier knowing the corresponding points on an elliptic curve. ECDLP is very complex and difficult to solve compared to any standard inverse operation of a one-way-trapdoor function such as Discrete Logarithm Problem or Factorization problem. Blind signature allows a user to obtain a signature from an authority on any document, in such a way that the authority learns nothing about the message that is being signed. The blindness is an important property which distinguishes the blind signature from other signature schemes. Blind signature is an important cryptographic primitive used in protocols such as electronic voting systems and cash payment systems. Since an ECDLP enjoys a large space and time complexity and blind signature ensures anonymity of clients message while obtaining a signature from a trusted party, we aim at designing a blind signature scheme based upon ECDLP which is supposed to have a low computation cost and low communication overhead. The signature should be such that it has a small size, it is highly secured and is resistant to elliptic curve cryptography based attacks such as forgery attack, MOV attack etc.

Contents

List of Figures

Chapter 1

Introduction

1 Introduction

In present world anonymous digital signature has got a vast field of applications like electronic voting system,e-banking etc for which the only solution is blind signature strategy.

1.1 Digital Signature

Signature is a method to authenticate any document. It is a proof to the recipient that the document comes from the correct entity (sender). In the present world most of the documents are electronic due to the cult usage of the computer and its applications like email, e-banking, e-voting, etc. Thus the message, data, documents or any other materials in electronic format has to be signed electronically. This signature that is done electronically is known as Digital Signature.[1,2]

1.1.1 Why Digital Signature Is Required ???

The need and importance of Digital Signature can be explained by the following example:-
Suppose that J sends an authenticated message to M. The following disputes may arise:
1. M tries to forge another message and claims that it came from J. M has to create a message and append an authentication code using J and M shared key.
2. It may so happen that J denies sending the message. Because it is very much possible for M to forge a message, it cannot be proved that J in fact sent the message.
Both scenarios are of equal concern. For example in the first scenario, a transfer of electronic funds takes place, and the receiver increases the amount of funds transferred and claims that the larger amount had arrived from the sender.[2]

An example of the second scenario is that an electronic mail message contains instructions to a stockbroker for a transaction that subsequently turns out badly. The sender pretends that the message was never sent. If there is lack of complete trust between sender and receiver authentication is not alone sufficient and the best possible solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature.

1.1.2 Properties Of Digital Signature

• It should be able to authenticate the author, date and timestamp of the signature.

• At the time of the signature it should be able to authenticate the contents of the message.

• To resolve disputes it should be verifiable by third parties.

Thus, the digital signature function includes the authentication function.[2]

1.1.3 Requirements Of Digital Signature

A digital signature must fullfill the following requirements:

• Depending on the message to be signed, the signature should be a bit pattern.

• The signature should use some information unique to the sender so that forgery and denia of service attack can be prevented.

• The digital signature should be relatively easy to produce.

• Recognition and verification of the digital signature should be relatively easy.

• Forgery of a digital signature should be computationally infeasible.

Thus the services that a Digital Signature provides are as follows[1,2] :

• Authentication

• Integrity

• Nonrepudiation (by using a trusted party)

1.1.4 Digital Signature Schemes

A digital signature scheme is a complicated mathematical scheme for proving the authenticity of a message. A valid digital signature makes the recipient believe that the message was created by an authentic sender. Digital signatures are commonly useful in e-commerce world and areas suc as software distribution and defence system and in cases where forgey detection is very important. [1,2]

1.2 Blind Signature

Chaum introduced the concept of blind signature in 1982.In the initial scheme, the protocol was such that the requester is allowed to obtain a valid signature s(m) for his/her message m from a signer.The signer knows nothing about the message. Every blind signature protocol has two properties, blindness and intractableness(difficult to manipulate). All previously prposed blind signature schemes are based on a trapdoor function such as the integer factorization problems(IFP), discrete logarithm problems(DLP).But most of the schemes fail to meet the above two fundamental properties Therefore, we aim to design an ECDLP-based blind signature scheme that possesses both the above properties . Further our scheme is intended to be immune against attacks like MOV, Baby Step Giant Step etc , and optimized in both space and time complexity by using various techniques. [5,13]

2 Objective

The objective of the proposed project is to design a blind signature scheme.Since blind signatures are the best and the most appropriate method of preseerving the anonymity they can be efficiently used in any e-commerce application that gives anonymity utmost importance.Moreover since it is a ECDLP-based blind signature it assures more security and efficiency.

3 Motivation

In e-commerce world such as an e-voting system authentication is very important as well as anonymity and confidentiality. The answer to this problem is a blind signature that is based upon a very difficult trapdoor function which is obviously elliptic curve discrete logarithm problem.So we intend to design such a scheme that is immune against most of the common cryptographic attacks.

Chapter 2

Cryptographic Background

4 What Is Cryptography?

Cryptography(covered text) is a technique of converting ordinary or plain text to cipher text.This is also called as encryption. In decryption the cipher text is converted back to the plain text. In earlier days cryptography referred to message encryption and decryption by using a common secret key. But in moderrn times the following mechanisms are proposed. They are [1, 2]

- Symmetric Key cryptography
- Asymmetric Key cryptography
- Hashing

4.1 Cryptographic Techniques

4.1.1 Symmetric Key Cryptography

In this technique, the sender uses an encryption algorithm and a secret key known to both sender and receiver to encrypt the message. Then the receiver oafter receiving the message uses the decryption algorithm and the shared secret key to decrypt the message.

4.1.2 Asymmetric Key Cryptography

This technique also known as public-key-cryptography invlolves the use of 2 keys - public key and private key. By using the public key the sender first encrypts the mesage and the receiver uses its private key to decrypt the message as shown in figure1[1, 2]

4.1.3 Hashing

A fixed length message digest is created out of the variable length message in hashing. The digest is of very small size than that of the message(if the message is very large). Usually both the message and the digest are sent to the receiver. Hashing helps in providing check values for the message$'s$ integrity.The hardware requirement for hashing is more than any operation. Compression function may be used by a set of cryptographic hash functions. These hash functions include RSA, MD etc the most poular being MD5/SHA-1 algorithm for message compression

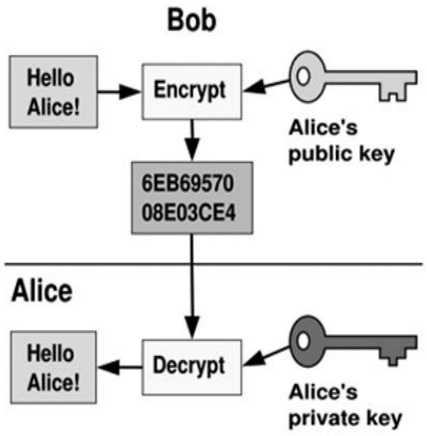

Figure 1: Asymmetric Key Cryptography

which converts a message to a 128 bit/512 bit hexadecimal form. [1, 2]

4.2 Cryptanalysis

Cryptanalysis is the study of methods to obtain the meaning of encrypted information(cipher text), without requiring the access to the private parameters. Usually, this involves a pattern study of the working methodology of the system and hence deriving the secret key. "Cryptanalysis" is also used to refer to any attempt to overcome the security of any cryptographic algorithm and protocol in general, and not only encryption. However, cryptanalysis does not involve methods of attack that do not primarily target weaknesses in the actual cryptography.But these types of attack pose an important concern and often are more effective than traditional cryptanalysis. [1, 2]

4.3 Security Services

Some security services and some mechanism to implement those services are provided by the International Telecommunication union-Telecommunication standardization Sector . The security services include: [2]

- Authentication
- Non repudiation

- Access Control
- Data Confidentiality
- Data Integrity

4.3.1 Authentication

This service gives a proof of authentication of the sender to the reveiver or vice-versa. In peer entity authentication,during the connection establishment phase of connection-oriented communication it provides the authentication of the sender or receiver . In data origin authentication i.e in connectionless communication it authenticates the source of data .[1,2]

4.3.2 Non-repudiation

To avoid repudiation(denial) by either the sender or the receiver of the data non-repudiation service is advisable.The receiver of the data can later prove the identity of the sender along with help of the proof of origin in case of denial of service. In non-repudiation, the sender can confirm the delivery to the receiver with the real proof of delivery[1, 2].This security service is extensively used in the verification phase of digital signatures.[2]

4.3.3 Access Control

Access control enables an authority to gain control and access to areas and resources in an information system. An access control system provides security against unauthorized access and usage of data. The term access in this context can mean reading, writing, modification or execution of programs [1, 2].

4.3.4 Data Confidentiality

International Organization for Standardization (ISO) in ISO-17799 defined confidentiality as "ensuring that information is accessible only to those authorized to have access" .In many cryptosystems confidentiality is one of the major design goals to protect data from disclosure attack. As defined by X.800 the service is very broad and includes confidentiality of the total message or

part of a message and also ensures protection against traffic analysis. In other words it prevents traffic analysis and snooping.[1, 2]

4.3.5 Data Integrity

Data integrity is requiredTo protect data from unauthorized insertion, deletionmodification and replaying by an attacker . It can protect the total message or the part of message.[1,2]

4.4 Security Mechanism

Security mechanisms include

- Encipherment
- Data Integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization
- Access Control
- Digital Signature

Chapter 3

Literature Review

5 ECC [Elliptic Curve Cryptography]

Elliptic Curve Cryptography is based on a special type of elliptic curve which is of the form

$$y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3$$

ECC makes the existing cryptosystems more secured and more efficient as these cryptosystems have smaller public-key certificates,smaller system parameters,faster implementations and other factors such as lower power consumption etc. Therefore, ECC cryptosystem is the most preferred cryptosystem.[7]

Elliptic Curve Cryptography (ECC) is an assymetric key cryptography. In asymmetric key cryptography each user generally have a pair of keys(a public key and a secret private key) . The private key is the secret parameter of a particular user whereas the public key is distributed among all users taking part in the communication.Public key algorithms require a set of constants that should be predefined .For example Domain parameters in ECC. Asymmetric key cryptography, unlike symmetric key cryptography, does not require any shared secret key between the sender and receiver but is quite slower than symmetric key cryptography.[7]

The mathematical operations of ECC is defined over an elliptic curve over real numbers

$y^2 = x^3 + ax + b$,

where $4a^3 + 27b^2 = 0$(non-singular elliptic curves)

Each value of the a and b gives a different elliptic curve.The points which lie on the curve are all points (x, y) which satisfying the above equation along with the null point(a point at infinity). The secret key is a random number whereas public key is a point on the curve obtained by multiplying the private key with the base point G of the curve.Domain parameters of ECC include the base point G, the curve parameters a and b,along with some other constants. [5]

6 Elliptic Curve Discrete Logarithm Problem [ECDLP]

The classical or general DLP(discrete logarithm problem) is the following:

If $b \equiv a^k \pmod p$, where p is prime and k is any random integer.

DLP is the problem to find k.

Similarly, ECDLP is the discrete log problem for elliptic curves.

i.e.If kP = Q, where P, Q are points on the curve E_p(a,b) and k is an integer such that Q lies on the curve

ECDLP is the problem of finding k knowing P and Q.

Notations:

E(F_q) is the set of all points on E whose all coordinates lie in F_q .

F_q denotes $F_p{}^n$.

Difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) decides the security of ECC-based signature. The high computational complexity of ECDLP is the reason of ECC-based signatures being more secured than other cryptosystems-based signature.Since ECDLP is muc tougher to solve than DLP ,the attacker first converts the ECDLP to DLP in most of the attacks. These attacks have been discussed in further pages .[7]

7 Operations On Elliptic Curves

7.1 Point Addition

On an elliptic curve, point addition is the addition of two points J and K to obtain another point L on the same elliptic curve.

For the points J (x_J, y_J) and K (x_K, y_K) and the resultant point L (x_L, y_L) has the coordinate values as[6,7] :-

$x_L = m^2 - x_J - x_K$

$y_L = m(x_J - x_L) - y_J$

where slope $m = (y_k - y_J)/(x_k - x_J)$

7.2 Point Doubling

If both the points J and K are same the coordinates of L are given as follows[6,7]:-

$x_L = m^2 - 2x_J$

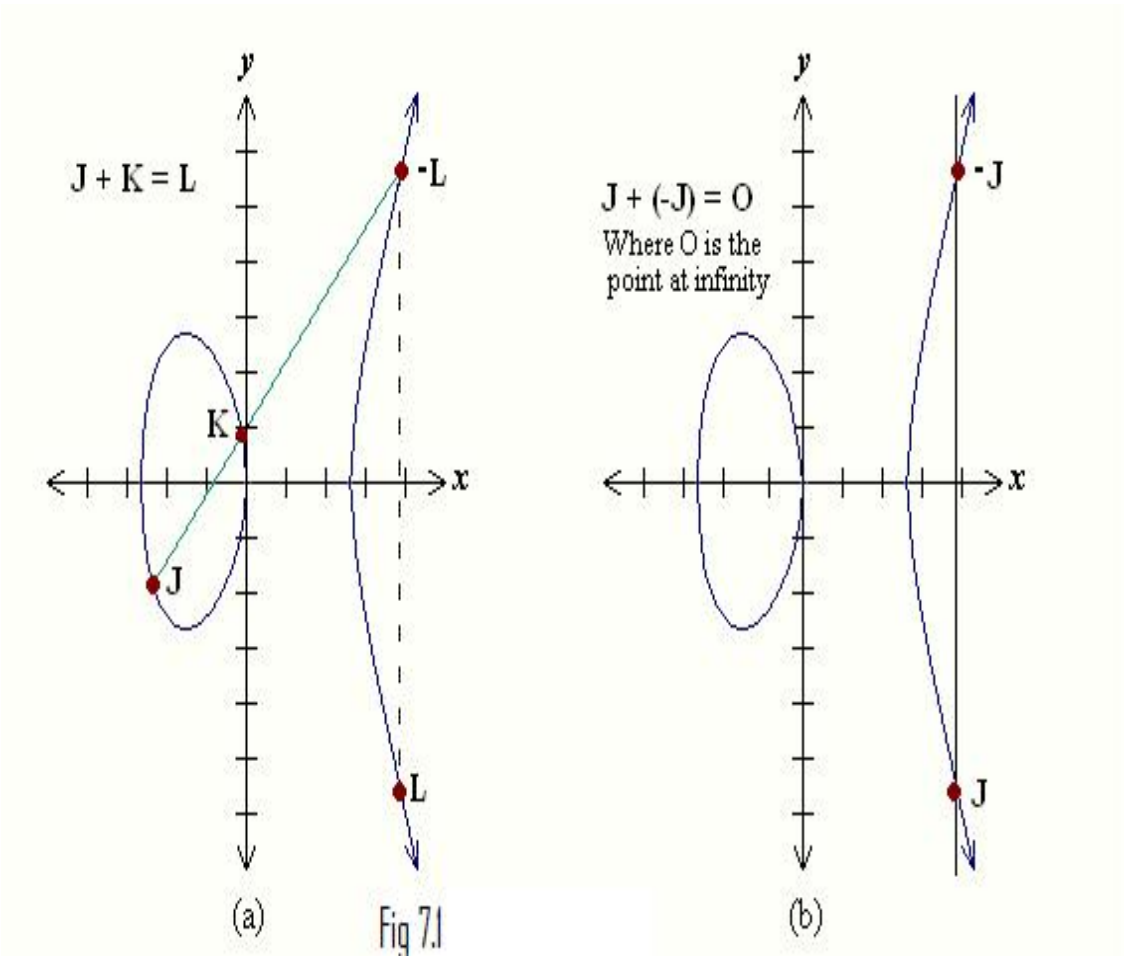

Figure 2: Point Addition

$y_L = m(x_J - x_L) - y_J$

where Slope $m = (3x_J^2 + a)/2y_J$

7.3 Point Multiplication

In point multiplication, a point P on the elliptic curve is multiplied with a scalar(integral value) k using elliptic curve equation to obtain another point Q on the same elliptic curve i.e. kP=Q Point multiplication is achieved by two basic elliptic curve operations[6,7]

1. Point addition, adding two points J and K to obtain another point L i.e., L = J + K.

2. Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J.

Point addition and doubling are explained above.

Here is a simple example of point multiplication.

Let P be a point on an elliptic curve. Let k be a scalar that is multiplied with the point P to obtain another point Q on the curve. i.e. to find Q = kP.

If k = 11 then kP = 23.P = 2(2(2P) + P) + P.

Thus point multiplication uses point addition and point doubling repeatedly to find the result. The above method is called double and add method for point multiplication. There are other efficient methods for point multiplication such as NAF (Non Adjacent Form) and wNAF (windowed NAF) method for point multiplication [3]

8 ECDSA - Elliptic Curve Digital Signature Algorithm

This is one of the algorithm that is used for authentication of a message between 2 clients(Let the clients be A and B).A has to sign the message using its private key to authenticate a message sent by A. A sends the message and the signature to B. This signature can be verified only by using the public key indeed send by A .[1]

ECDSA is a variant of the Digital Signature Algorithm (DSA).It operates on elliptic curves. Both the clients have to agree up on Elliptic Curve domain parameters to send a signed message from one to the other. Sender A has a key pair - a private key d(a randomly generated integer

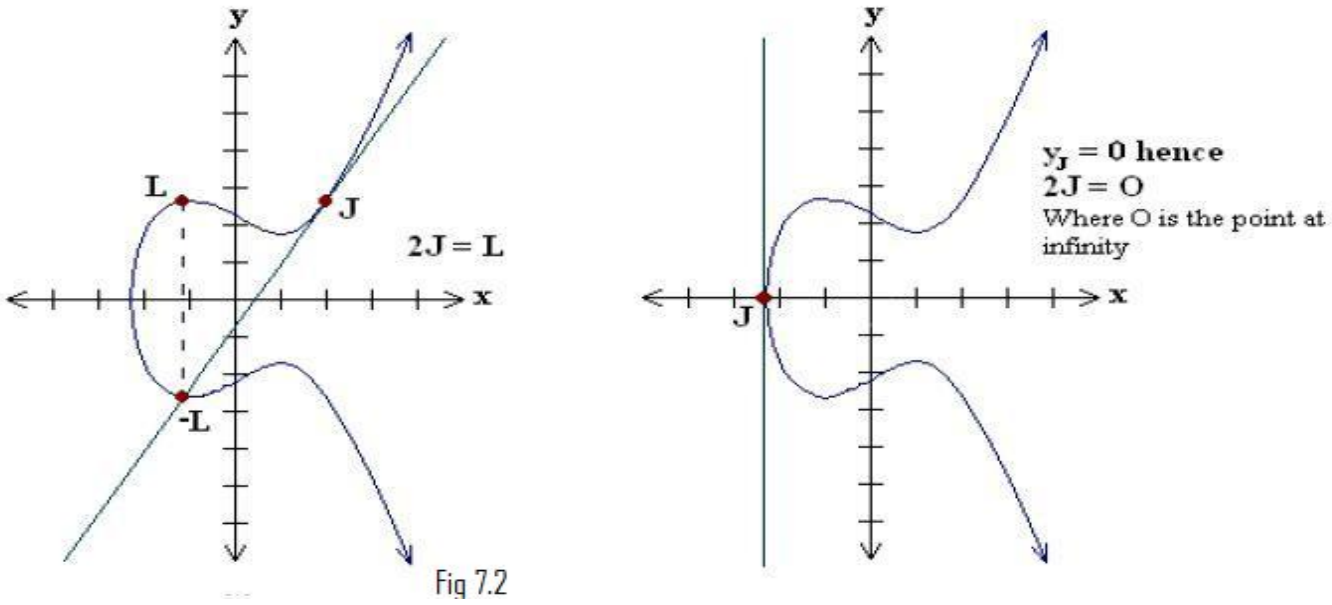

Figure 3: Point Doubling

less than n, where n is the order of the curve) and a public key Q = d * G(G is the base point). An overview of ECDSA process is defined below.

8.1 Signature Generation

[1,6] For signing a message m by sender A, using As private key d

1. Calculate e = HASH (m).
2. Select a random integer k from [1 ,n - 1]
3. Calculate r = x_1 (mod n), where (x_1, y_1) = k * G. If r = 0, go to step 2
4. Calculate s = k^{-1}(e + dr)mod(n). If s=0, go to step 2
5. The signature is the pair (r, s)

8.2 Signature Verification

[1,6] For B to authenticate A's signature, B must have As public key Q

1. Verify that r and s are integers in [1,n - 1]. If not, the signature is invalid

2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate w = s^{-1}mod(n)
4. Calculate u_1 = ew(mod n) and u_2 = rw (mod n)
5. Calculate (x_1, y_1) = u_1G + u_2Q_A
6. The signature is valid if x_1 = r(mod n), invalid otherwise

9 Blind Signature

The concept of blind signature was first introduced by Chaum in 1982.It was mainly introduced to enhance security of automated payment systems and electronic voting systems. Chaum pointed out that the multiplicity and growth of electronic services may have an impact on consumers privacy and extent of criminal use. Thus, blind signature cryptosystem is the need of the hour.Moreover it is a fundamentally different kind of cryptosystem. This new cryptosystem ensures anonymity and protects customers privacy during the use of secure electronic payment systems. [5,8,13]

A blind signature scheme involves basically a group of requesters and a signer. Each requester obtains a valid signature from the signer after sending an encrypted message to him.The signer only signs the message without any idea of the contents of the message i.e. it does not decrypt it. Later, the signer can verify the authenticity of the signature whenever he/she comes across the message-signature pair.However, he/she cannot link the message-signature pair to the particular phase of the signing protocol that has led to this pair.In blind signature the receiver′s identity is always concealed. Therefore, according to Chaum a blind signature scheme should be intractable and blindness property should hold good.[5,8,13]

9.1 Phases of Digital Signature

Most of the digital signature schemes are universally verifiable i.e. anyone using the signers public key can verify whether the signature is authentic or not, and signature forgery is very difficult. A digital signature consists of [5,8,13]
the following phases-
1) Signing phase: A sender first of all uses a hashing function to produce a message digest.Using

private key of the sender the message digest is encrypted to get the digital signature. Then the sender sends his message and its digital signature to a receiver.
2) Verification phase: When the receiver gets the message-signature pair, he inputs the message into the same hashing function to get the first phase of the message digest. Then he decrypts the digital signature by the senders public key to get the second phase of the message digest. And finally he verifies both the message digests. If they are the same, the signature is valid; otherwise, the signature could be forged.

9.2 Blind Signature

The signer signs the requesters message and knows nothing about it; moreover, no one knows about the correspondence of the message-signature pair except the requester. A short illustration of blind signature is described in the following [5,13]:-
1) Blinding phase: The sender chooses a random number called a blind factor to blind his message such that the signer will not be able to view the contents of the message.
2) Signing phase: When the signer gets the blinded message, he encrypts the blinded message using his private key and then sends back the blind signature to the sender.
3) Unblinding phase: The sender uses the blind factor used in (a) to recover the signers digital signature from the blinded signature.
4) Signature Verification phase: Anyone can use the signers public key to verify whether the signature is authentic or not[5,13].

10 Attacks On Digital Signature

Any ECC based signature derives its security from the fact that it is based on Elliptic curve discrete logarithm problem and it is very difficult to solve an ECDLP, more difficult than Integer Factorization problem or discrete logarithm problem.In cryptography, an attack is a method of solving a problem. Specifically, the aim of an attack is to find a fast method of solving a problem on which an encryption algorithm depends. The known methods of attack on the elliptic curve

(EC) discrete log problem that work for all curves are slow, making encryption based on this problem practical. However, several efficient methods for solving the EC discrete log problem for specific types of elliptic curves are known. This means that one should make sure that the curve one chooses for ones encoding does not fall into one of the several classes of curves on which the problem is tractable. Below, we describe the Baby Step, Giant Step Method, which works for all curves, but is slow.[12]

10.1 Baby Step, Giant Step Method

This is one of the fastest general methods of solving the ECDLP. The algorithm has approximately sqrt(p) time and sqrt(p) space complexity, where p = ♯E(Fq).But this is not fast enough to be practical. Ignoring logarithmic factors (sqrt(p)) is already large enough for the problem to be intractable, we find that the running time is on the order of (sqrt(p)). The storage space required is also on the order of (sqrt(p)), This algorithm is too slow to be of practical use in breaking codes, as it is exponential in the length log N of the input. [12]

10.2 Key-Only-Attack

In the key-only-attack, Eve has access only to the public information released by Alice. To forge a message, Eve needs to create Alices signature to convince Bob that the message is coming from Alice. [1]

10.3 Known-Message-Attack

In the known-message-attack, Eve has access to one or more message-signature pairs. In other words, Eve has access to some documents previously signed by Alice. Eve tries to create another message and forge Alices signature on it. [1]

10.4 Chosen-Message-Attack

In the chosen-message-attack, Eve somehow makes Alice sign one or more messages for her. Eve later creates another message, with the content she wants, and forges Alices signature on it.[1]

If the attack is successful, the result is a forgery. There are essentially 2 types of forgery.

10.5 Existential Forgery

In an existential forgery, Eve may be able to create a valid message-signature pair, but not the one that she can really use. In other words, a document has been forged, but the content is randomly calculated. This type of forgery is probable but fortunately Eve cannot benefit from it very much. Her message could be syntactically or semantically unintelligible. [1]

10.6 Selective Forgery

In selective forgery, Eve may be able to forge Alices signature on a message with the content selectively chosen by Eve.Although this is beneficial to Eve, the probability of such a attack is very low, but quite detrimental for Alice.[1]

11 Speeding Up Verifications In ECDSA

11.1 Certicom's Proposal

ECDSA signatures are considered and conventionally are significantly faster RSA signatures.But recent research suggest verification with RSA was found to be faster than verification with ECC if considerable key size was used in RSA. Inorder to overcome this shortcoming, Certicom has found a new way to speed up the verification step of ECDSA by nearly 40

11.2 Inverse Operations Minimization using Projective coordinate system

In projective coordinate system the point (X_1, Y_1, Z_1) corresponds to the point (X_1/Z_1, $Y_1/{Z_1}^2$) in gaussian coordinate system and the equation for the elliptic curve becomes ${Y_1}^2 + X_1Y_1Z_1 = {X_1}^3Z_1 + a{X_1}^2{Z_1}^2 + b{Z_1}^4$. In point multiplication, the point (X_1, Y_1) in gaussian coordinate system is converted to (X_1, Y_1, 1) in projective coordinate system. After multiplication is over the result (X_1, Y_1, Z_1) is converted to the gaussian coordinates as (X_1/Z_1, $Y_1/{Z_1}^2$)[11]

(Z cannot be equal to 0 as if Z = 0, then the point is a null point or in other words point at infinity)

11.2.1 Point Addition

In projective coordinate system for adding two points let

$(X_a, Y_a, Z_a) + (X_b, Y_b, Z_b) = (X_c, Y_c, Z_c)$

$A = Y_b Z_{a2} + Y_a$

$B = X_b Z_a + X_a$

$C = Z_a B$

$D = B2(C + aZ_a2)$

$Z_c = C^2$

$E = A.C$

$X_c = A_2 + D + E$

$F = X_c + X_b Z_c$

$G = X_c + Y_b Z_c$

$Yc = E.F + Z_c G$

$Z_b = 1$(in point addition one operand will definitely be the input to a point in point multiplication operation, which is a gaussian coordinate point)[11]

11.2.2 Point doubling

In projective coordinate system for doubling a point let $2(X_a, Y_b, Z_a) = (X_b, Y_b, Z_b)$

$Z_b = X_a^{\ 2} Z_a^{\ 2}$

$X_b = X_a^{\ 4} + bZ_a^{\ 4}$

$Y_b = bZ_a^{\ 4} Z_b + X_b (aZ_b + Y_a^{\ 2} + bZ_a^{\ 4})$[11]

Chapter 4

Proposed Scheme "Blind Signature Based Upon ECDLP"

12 Proposed Scheme

12.1 Participants

The scheme involves 3 participants:

• Sender • Signer(Trusted Authority) • Verifier

12.2 Description

12.2.0.1 Set-up Phase For each message that has to be signed the Signer generates 2 random integers(d_1,d_2) which will be the private keys for the particular session. Then it calculates the public key(Y) as :

$Y = d_1 B_1 + d_2 B_2$,

where B_1 and B_2 are two base points on an elliptic curve(E_p(a,b)) over F_q) and a,b and p are curve parameters.

12.2.0.2 Blinding Phase When the setup phase is over, the sender first of all converts the message to a point on the curve and then generates 2 random integers c_1 and c_2 and blinds the message M as:

$$bm = m(c_1 B_1 + c_2 B_2)$$

where m is x-coordinate of the message(M) After the message is blinded, the sender sends the blinded message to the signer to get signed message(s).

12.2.0.3 Signing Phase The signer on receiving the blinded message generates 2 random integers z_1 and z_2 to give a point on the curve (Q) as:

$Q = z_1 B_1 + z_2 B_2$

Using z_1 and z_2 the signer generates 2 signatures S_1 and S_2 as:

$S_1 = bm + (d_1 + z_1)a B_1$

$S_2 = bm + (d_2 + z_2)a B_2$

where a is a random integer.

Finally point R is calculated as

R = a*Q.

12.2.0.4 Unblinding Phase The signature is un-blinded through the following equations to get X_1 and X_2

$$i = [(c_1 B_1)^{-1} + (c_2 B_2)^{-1}] m$$

$$X_1 = S_1 + i$$

$$X_2 = S_2 + i$$

Here c_1 and c_2 are integers.

12.2.0.5 Verification Now a point N is calculated using the equation :- $N = X_1 + X_2 - aY$ The signature can now be verified by comparing the points N and R.

12.3 Correctness

$$\begin{aligned}
N &= X_1 + X_2 - aY \\
&= S_1 + i + S_2 + i - a(d_1B_1 + d_2B_2) \\
&= bm + (d_1 + z_1)a B_1 + [(c_1 B_1)^{-1} + (c_2 B_2)^{-1}] m \\
&\quad + bm + (d_2 + z_2)a B_2 + [(c_1 B_1)^{-1} + (c_2 B_2)^{-1}] m - a(d_1B_1 + d_2B_2) \\
&= m(c_1 B_1 + c_2 B_2) + (d_1 + z_1)a B_1 + [(c_1 B_1)^{-1} + (c_2 B_2)^{-1}] m \\
&\quad + m(c_1 B_1 + c_2 B_2) + (d_2 + z_2)a B_2 + [(c_1 B_1)^{-1} + (c_2 B_2)^{-1}] m \\
&\quad - a(d_1B_1 + d_2B_2) \\
&= a(z_1 B_1 + z_2 B_2) \\
&= aQ \\
&= R
\end{aligned}$$

13 Security Analysis

13.1 Key-only-attack

For the key-only-attack to be possible, Eve(attacker) has to create a valid signature pair. Let Eve is able to create the signature pair. This implies that the signer is compromised, which is

quite rare. But this will not help as in the unblinding stage, Eve will not be able to unblind the signature pair as it will not be having the required parameters(c_1 and c_2) and extraction of c_1 and c_2 is impossible due to ECDLP.

$$\begin{aligned} bm &= m(c_1B_1 + c_2B_2) \\ &= c'B \end{aligned}$$

To determine c' is cumbersome due to ECDLP and even if c' is known, determination of c_1 and c_2 is nearly impossible and this is the reason for using double parameters.

13.2 Known-message-attack

In the known-message-attack, Eve has to access one or more message-signature pair and then generate a signature for her message. But this is not possible and is explained as below.

Let Eve has a message-signature triplet (m,x_1,x_2) and wants to generate signature for message m' . So first of all she has to generate blind signature pair (s_1', s_2') and then the un-blinded signature pair (x_1', x_2'). Then the signatures are sent to the verifier for verification. But the verifier will not be able to verify the signature because the verifier will be having public key corresponding to the private key used by The Actual Signer for some message m.
But Eve can easily access the public key(Y) issued by The Actual Signer to the Verifier for some message m and use it for her own message(m) instead. But she cannot do this because she will be encountering the ECDLP.

$$\begin{aligned} S_1'' &= bm'' + (d_1'' + z_1'')a'' B_1 \\ \text{or } S_1'' - bm'' &= (d_1'' + z_1'')a'' B_1 \\ \text{or } S_1'' - bm'' &= d_1''' B_1 \\ \text{or } S_1''' &= d_1''' B_1 \end{aligned}$$

To determine d_1''' Eve has to solve ECDLP and then to extract d_1'' from d_1''' is nearly impossible; justifying the use of double parameters.

13.3 Chosen-message-attack

For the same reasons explained for the infeasibility of known-message-attack the chosen-message attack is impossible thereby indicating that this signature is highly secured. Determination of

d_2'' involves similar difficulties.

14 Performance Evaluation

Any digital signature is compared on the basis of number of operations rather on the basis of time complexity. The following notations are used to estimate the operating overhead:

T_{MUL}: the time required for the modular multiplication.

T_{EXP}: the time required for the modular exponentiation.

T_{INV}: the time required for the modular inversion.

T_{ECMUL}: the time required for the multiplication of a scalar and an elliptic curve point.

T_{ECADD}: the required time for the addition of two points over an elliptic curve.

Modular addition operations add negligibly to the operating overhead. The following table compares our scheme with 2 other standard schemes[].

Phase	Proposed Scheme	Scheme1	Scheme2
SetUp	$2T_{ECMUL}$	$3T_{ECMUL}$	$2T_{ECMUL}$
Blinding	$3T_{ECMUL}$ + 1 T_{ECADD}	$2T_{EC_MUL}$ + $10T_{MUL}$+$6T_{INV}$	$2T_{EC_MUL}$
Signing	$5T_{ECMUL}$ + 3 T_{ECADD} + $2T_{MUL}$	$6T_{MUL}$	$2T_{EC_MUL}$
Unblinding	$3T_{ECMUL}$ + $3T_{ECADD}$	$10T_{MUL}$+$2T_{INV}$	$1T_{EC_MUL}$+$3T_{MUL}$
Verification	$1T_{ECMUL}$ + T_{ECADD}	$2T_{EC_MUL}$	$1T_{EC_MUL}$

Though the computational overhead of our scheme is more than Scheme1 and Scheme2,but is much more secure as compared to the 2 Schemes as:

•The attacker has to solve an ECDLP at every stage to get any information

•Even if the attacker is able to get solve the ECDLP,he/she cannot get hold of any private parameter as almost in all stages there is a linear combination of the private parameters.

Chapter 5

Implementation And Results

15 Implementation

15.1 SetUp

Fist of all the signer choose an appropriate but random set of curve parameters:

• p=54167

• a=11

• b=24

• Generating Points::

b1= (2633,66)

b2= (2837,210)

The signer generates d_1 =3 and d_2 =7 as private keys and then computes the public key Y=(41441,2313)

15.2 Message To Point Conversion

Koblitz's Method was used to convert the message to a point.In this method the message is fist converted to a number(m) and then the method is applied to get a point M which is as follows[9]:

• Choose a random integer k≥1280

• For i=0 to k-1

• x=km+i, where x is the x-coordinate of the point(M)

• Find corresponding y-coordinate

• If y exists then break;else continue

The message(animesh chhOtaray== gfgfdfhdgdflgfglldsl122443) is converted to 83614777164082643 7308388 44650185742058121639443062071166695609161480774966140406205249162633123628674792874307055075855626 is converted to M(1902,179)

15.3 Blinding

Then the blinding algorithm was used to get blinded message (14532,37455) which is send to the signer for signing.

15.4 Signing

The signer generates 2 signatures: s_1 = (2946,28451) and s_2= (2560,45286) which are sent to the sender for unblinding.

15.5 Unblinding

The sender generates 2 signatures x_1 = (27135,23571) and x_2 = (45642,45441) using s_1 and s_2 which are sent to the verifier along with some other parameters for verifying.

15.6 Verification

The signature is verified using the verification algorithm and the resultof verification is published as true/false.In this case the resulti is true.

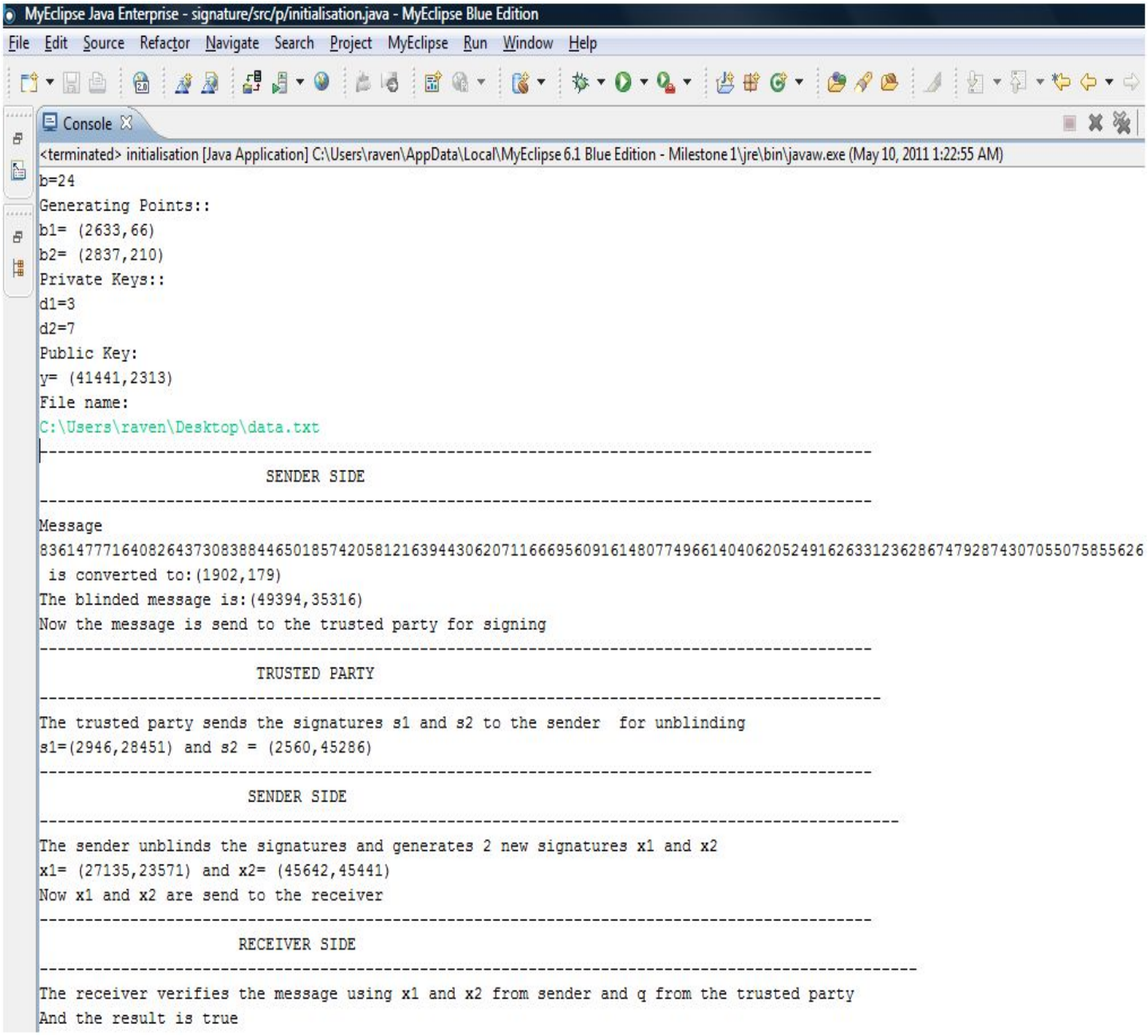

Figure 4: Implementation Screenshot

Chapter 6

Conclusion

16 Conclusion

Public key encryption can be used to eliminate problems involved with conventional encryption. It however has not managed to be as widely accepted as conventional encryption because it introduces a lot of overheads. Therefore it is very important to find ways to reduce the overhead yet not sacrificing on other aspects of security. The ECC has been shown to have many advantages due to its ability to provide the same level of security as any cryptosystem yet using shorter keys. However its disadvantage which may even hide its attractiveness is its lack of maturity, as mathematicians believe that enough research has not yet been done in ECDLP. Thus a blind signature along with ECDSA promises to be a bright prospect in designing secure and efficient systems such as e-voting systems.

Chapter 7

References

References

[1] B Forouzan. *Cryptography and Network Security.* TMH, 2007 edition.

[2] W Stallings. *Cryptography and Network Security.* Prentice Hall, 2005 edition.

[3] D.S.; Ramkrishna B.; Venkataramana Bhandari, A. K.; Nagraj. *Elliptic Curves, Modular Forms and Cryptography.*

[4] David S. Dummit and Richard M Foote. *Abstract Algebra.*

[5] F.G.Jeng T.S.Chen, T.L.Chen. A blind signature scheme based on elliptic curve cryptosystem. *Journal of Networks*, 5:921 – 927, August 2010.

[6] Kefah Rabah. Theory and implementation of elliptic curve cryptography. *Journal of applied sciences*, 5:604 – 633, 2005.

[7] Rob Lambert. Understanding elliptic curve cryptography. *Director of New Technology,Certicom.*

[8] J.M. Camenisch, J. L. Pirereau and Stadler. M.a. blind signature based on discrete logarithm problem, advanced in cryptology. *Journal of Networks*, pages 428 – 432, 1994.

[9] P.Prapoorna Roja Padma Bh, D.Chandravathi. Encoding and decoding of a message in the implementation of elliptic curve cryptography using koblitzs method. *International Journal on Computer Science and Engineering*, 02:1904 – 1907, 2010.

[10] Sanjay Kumar Jena Debasish Jena and Banshidhar Majhi. A novel untraceable blind signature based on elliptic curve discrete logarithm problem. *International Journal of Computer Science and Network Security*, 2007.

[11] Yu-Fang Chung Tzer-Shyong Chen, Kuo-Hsuan Huang. A practical authenticated encryption scheme based on the elliptic curve cryptosystem. *Computer Standards and Interfaces*, 26:461 – 469, November 2003.

[12] S. Vanstone N. Koblitz, A. Menezes. The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, 19:461 – 469, 2000.

[13] D Chaum. Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto*, 82:199–203, 1983.