A NEW CONVERTIBLE AUTHENTICATED ENCRYPTION SCHEME WITH MESSAGE LINKAGES

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

Bachelor of Technology

in

Computer Science and Engineering

by

K S Subramanyam
(111CS0114)
&
Dhananjay Rout
(111CS0086)

Department of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela-769008, Odisha, India

A NEW CONVERTIBLE AUTHENTICATED ENCRYPTION SCHEME WITH MESSAGE LINKAGES

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

Bachelor of Technology

in

Computer Science and Engineering

by

K S Subramanyam
(111CS0114)
&
Dhananjay Rout
(111CS0086)

under the guidance of

Dr. Sujata Mohanty
NIT Rourkela

Department of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela-769008, Odisha, India

May 2015

Department of Computer Science & Engineering
National Institute of Technology, Rourkela
Rourkela-769008, Odisha, India.

May 11, 2015

DECLARATION OF AUTHORSHIP

We hereby declare that the thesis we are submitting is entirely our own original work except where otherwise indicated. We are well aware of the Institute's regulations concerning plagiarism, including those regulations concerning disciplinary actions that may result from plagiarism. Any use of the works of any other author, in any form, is properly acknowledged at their point of use.

K S Subramanyam
111CS0114
B.Tech
Department of CSE, NIT Rourkela

Dhananjay Rout
111CS0086
B.Tech
Department of CSE, NIT Rourkela

ABSTRACT

The digital signature provides the signing message with functions like authentication, integration and non-repudiation. However, in some of the applications, the signature has to be verified only by specific recipients of the message and it should be hidden from the public. For achieving this, authenticated encryption systems are used. Authenticated Encryption schemes are highly helpful to send a confidential message over an insecure network path. In order to protect the recipients benefit and for ensuring non-repudiation, we help the receiver to change the signature from encrypted one to an ordinary one. With this we avoid any sort of later disputes. Few years back, Araki et al. has proposed a convertible authenticated scheme for giving a solution to the problem. His scheme enables the recipient to convert the senders signature into an ordinary one. However, the conversion requires the cooperation of the signer. In this thesis, we present a convertible authenticated encryption scheme that can produce the ordinary signature without the cooperation of the signer with a greater ease. Here, we display a validated encryption plan using message linkages used to convey a message. For the collector's advantage, the beneficiary can surely change the encrypted signature into an ordinary signature that which anyone can check. A few attainable assaults shall be examined, and the security investigation will demonstrate that none of the them can effectively break the proposed plan.

ACKNOWLEDGMENT

We are highly obligated to our advisor Dr. Sujata Mohanty for providing for us a chance to work under her direction. Like a genuine guide, she persuaded and motivated us through the whole length of time of our work, without which this venture couldn't have seen the light of the day.

We pay our respects to the faculty of Computer Science and Engineering Department, National Institute of Technology, Rourkela for their precious direction and advice in the fitting times. We also want to thank our companions for their help and support all through this venture.

Last but not the least, we express our heartfelt gratitude to the Almighty and our guardians for their favors and backing without which this assignment could have never been fulfilled.

K S Subramanyam
111CS0114
B.Tech
Department of CSE, NIT Rourkela

Dhananjay Rout
111CS0086
B.Tech
Department of CSE, NIT Rourkela

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER I: INTRODUCTION

There is a great need for security of information nowadays mainly during transmission. A few problems are harder to fathom than others as in producing an answer requires more resources, for example, time, space, energy, etc. Consequently, there exists a quantifiable "complexity gap" in the middle of problems, and it bodes well to recognize “easy” problems and “hard” problems. However, where complexity theory is all about quantifying and exploring the distinction between easy and hard problems, cryptography is all about exploiting it. All the more particularly, cryptography is the study of developments where a portion of the computations included are deliberately easy, while others are hard [1]. This sort of cryptography can offer various other services like

Integrity - reassuring the recipient that the message has not been altered.

Authentication - verifying someone’s (or something’s) identity.

Confidentiality - Security from divulgence to unauthorized persons.

Non-repudiation - Originator of communications can’t deny it later.

These are the essential security objectives a message passing framework must fulfill for an effective correspondence. Before, cryptography mostly concerned with the privacy component [2]. At that point, the most use of encryption was in the division of guard or other association to gather and report mystery data on a foe or contender. In the most recent decade, the other security objectives like respectability check, client validation, computerized marks and so forth have been added to the privacy component. Indeed in antiquated times cryptography was utilized on the premise of some basic figures like the Caesars figure and going the keys through a secured messenger framework [3].

Introduction to Cryptography

Strangely, cryptography is considered to be the art of secret writing. It's a science of utilizing the mathematics for encryption and decryption of data. Encryption helps us in storing the sensitive information or in transmitting the same across networks which are insecure such as the Internet. Then, it can be read only by the supposed person who receives it and nobody else. While cryptography is dealing with data security, cryptanalysis deals with analysis of secure communication and breaking it. Classical cryptanalysis includes a combination of mathematical tools and their applications, analytical reasoning, patience, pattern finding, luck and determination. Another name for the cryptanalysts is attackers. So, cryptology includes both cryptanalysis and cryptography. Here, we are using encryption where information is represented as numbers and then it is manipulated. Previously, people used symmetric key encryption, but it's too old now, because of much more advancements in this field and acquaintance with check of prime numbers generated. Asymmetric cryptography is more popular nowadays [3]. Hence, cryptography is classified in two parts:

Symmetric Key Cryptography

Asymmetric Key Cryptography

Symmetric Key Cryptography

It is an encryption scheme in which the receiver and sender share a common key that is used for the decryption and encryption of the message. This system is simpler and faster, but the main disadvantage in this scheme is that the two parties must exchange the common key somehow or other very confidentially. It is also called as secret-key cryptography. Data Encryption Standard (DES) is a common example for this type of cryptography. In symmetric key cryptography let us suppose that the sender sends the message by encrypting with a key k and the receiver after receiving the encrypted message decrypts it with the same common key k. The supposition is based upon the way that here, the sender and the beneficiary utilize the same key and the transmission of the message and the key of cipher text is done in an unreliable channel. This framework is defenseless and defective if the key k is spilled and it is known to the enemy [1].

Asymmetric Key Cryptography

Asymmetric key is also known as public key cryptography. It is a kind of cryptography in which a instead of one, two keys are used to decrypt and encrypt the message to ensure its secure arrival. In the beginning, a user gets a public and private key pair from the certificate authority board. Any other network user interested in sending an encrypted message to the first user can get his public key from the public directory. Using this key, he has to ecrypt the message and then send to the recipient. After getting the message, the recipient decrypts it with his own private key, which no one else can access. We use asymmetric key cryptography in order to overcome the problems existing in symmetric key cryptography. It is same as the former with slight difference. Here, we have a pair of keys instead of one. Diffie and Hellman were the first to outline Asymmetric Key Cryptographic methods that are used for key agreement and are also used in application of other cryptographic problems [3]. Diffie and Hellman initially delineated the Public Key Cryptography strategy, which could be utilized for key agreement and had an application in the other cryptographic issues [3]. Diffie and Hellman did not give solid developments to how this idea of public-key cryptography could be complemented by and by. It was not until the major work of Adlemen, Shamir, and Rivest that the first public-key cryptosystem was acknowledged [4]. The idea of Public Key Cryptography was a major break-through in the field of Digital Signature. Digital signatures are similar to the signatures done on handwritten documents. They have the same properties of real signatures. They are easy to be produced but difficult to be forged. This was achieved by using the public key to encrypt and private key to decrypt. With passage of time, several new inventions and developments came up and proved better than the older ones.

Digital Signature

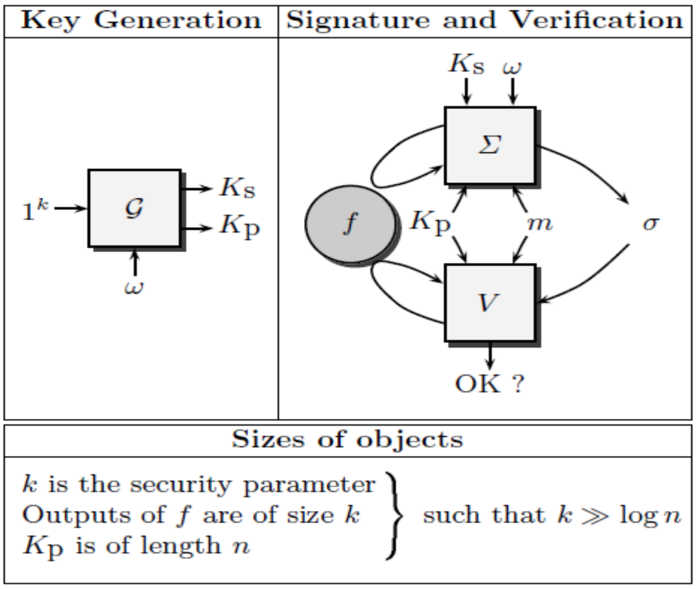
For a document the most important security goal is its Authenticity. In the physical world conventionally the signature is included in the document as a part of it, which is not in case of digital signature as the signer or the sender sends the message and the signature as two separate documents to the receiver which receives both documents and starts the verification process of checking whether that the signature actually belongs to the sender. If verified then the document is accepted else rejected. Digital signature was proposed by Diffie and Hellmen for the first time [3]. We give a more accurate definition for the signature scheme which is based on [5]. The figure 1.1 is from [6].

Signature Scheme: A signature scheme consists of these three algorithms of polynomial time:

- Keygen (Key generation) algorithm: For an input 1k , let k be a security parameter, it produces public and private keys, say (K_p, K_s). It forms a pair of keys. This algorithm is highly probabilistic one.

- Signing algorithm: This produces a signature, say S, when a message, M and a set of public and private keys are supplied to it. Let the set of keys be (K_p, K_s). This algorithm may be probabilistic and may receive some other inputs in other schemes.

- Verification algorithm: It checks whether S is the right signature for m corresponding to K_p or not when supplied with a message m and a signature S and a public key K_p. This algorithm not necessarily be probabilistic in nature.



Sizes of objects

k is the security parameter
Outputs of f are of size k
K_P is of length n
such that $k \gg \log n$

Figure 1: Signature Scheme Diagram from [1]

The digital signature paradigm only provides the Authenticity part of the security goal. To enhance the security to include Confidentiality along with the Authentic- ity we make use of both signature and encryption. It can be done in two separate simple steps of signing the document using some signing schemes and the encrypt- ing it based on some predefined encryption schemes. The various steps can be written as the follows;

- Signing is done using a Public key DS (Digital Scheme) scheme.
- With the help of an existing secret key encryption algorithm, encrypting the message m, along with the signature and this happens under chosen encryption key of a message.
- Using the public key of receiver, encrypt the message encryption key once again.
- Send the message.

Convertible Authenticated Encryption Scheme

A convertible authenticated encryption scheme helps a sender to generate a cipher-text in such a way that only a specific receiver will be able to decrypt and verify it. So as to avoid later disputes because of repudiations this scheme helps the receiver to convert the signature from an encrypted one to an ordinary signature [2]. In 2009, Lee et al. came up with another Convertible Authenticated Encryption scheme which is based upon El-gamal's scheme, in 2009. It also provides notions of security like integration, authentication, non-repudiation and confidentiality. In this scheme, the sender signs the message with an authenticated cipher-text signature. Only the receiver is enabled to decrypt the message using his own private key and thus verify the message with his own public key. If at all a dispute arises, the receiver will be capable of converting the cipher-text into an ordinary signature which is simple enough to be verified by one and all [4].

Convertible

The word 'Convertible' means the receipient can convert the encypted digital signature to an ordinary signature which anyone can verify. Even if the signature is repudiated by the signer, his dishonesty can be proved by the receipient with a great ease as the signature can be verified by anyone [6].

Discrete Logarithms

In mathematics, suppose there is an equation bk=g, where b and g belong to a finite group, then an integer k which solves the above equation is referred to as discrete logarithm. Let b be the base of log and g be the element whose logarithm is being calculated. The discrete algorithms are finite-group theoretic analogue of simple ones that solve the equation with real numbers g and b. [8].

No efficient method is known till date, which can compute discrete logarithmic problems on conventional computers. Computing discrete log problems is quite difficult as per past knowledge. Since there is no efficient solution for Discrete Logarithmic problems, many popular algorithms in public key cryptography have their security based upon this DLP.

Let G be any group in general. Let multiplication be the group operation. Let g and b be any elements belonging to G. Suppose there is a solution k to solve the equation $b^k=g$, then the integer k is called as discrete Logarithm of g with base b. As we know that k=$\log_b$(g). it is quite possible that no such discrete log exists based upon g and b, or that more than one solution exists. Suppose, H is a subgroup of G. In this case, H is cyclic group and for all g in H, we have integral $\log_b$g for sure. If H is infinite, the Discrete logarithm amounts to group isomorphism and then $\log_b$(g) is also unique [4].

$$\log_b : H \to Z.$$

But if H is of finite size n, till modulo n $\log_b$g is unique and the discrete logarithm results in a group isomorphism.

$$\log_b : H \to Z_n.$$

Here Zn indicates the circle of integers modulo n. but the ordinary logarithms base change formula remains the same: If c is another generator of H, then

$$\log_c(g) = \log_c(b).\log_b(g).$$

Message Linkages

A complex message contains multiple message blocks which are linked with one another. If buffer size is not sufficient or when the message is extended due to running processor ,many message blocks are created in the message, as shown in Figure 1. When a message contains so many message blocks overall message type is determined by the first message type even if the type of attached message blocks are different. If the content of the buffer is less than the original content of the message so many message blocks are formed in the message as shown in the diagram below. Suppose a large message say of 1000 kb then it is broken into small message bodies of size 100 kb,

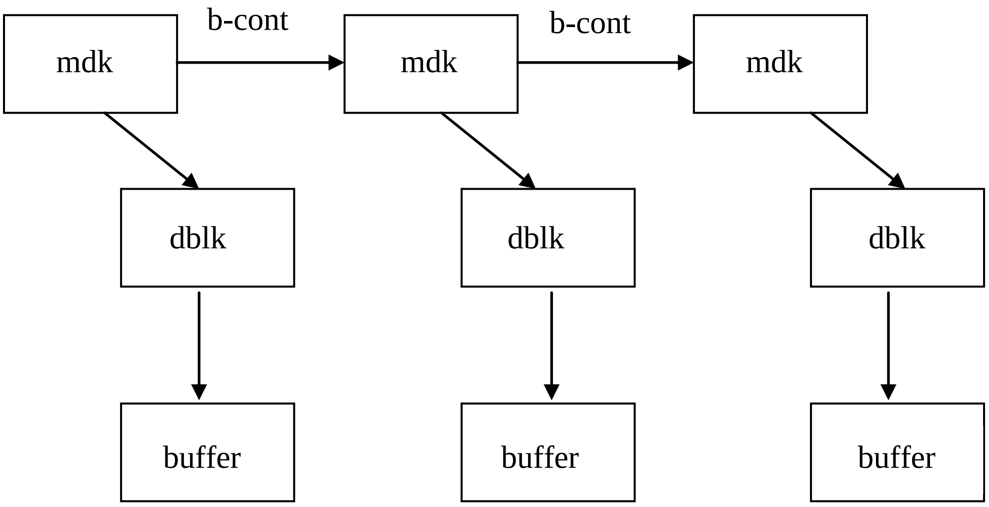


Figure 2: Message linked blocks

Need of the scheme and application

This scheme which is authenticated encryption is filled with so many facilities like message authentication, integrity of the message and repudiation free message.

Message authentication means to make the message like the originally provided with.

Integrity means loyalty just like no unkown person is allowed to change the original message.

Non-repudiation means the person who is signing should have a open view on the message coming afterwards. [1].

E-commerce has become a hub for online digital content transactions. They are growing at a very faster rate. For this to continue we have to take into account the sophisticated electronic payment schemes as well as high quality digital materials.[11]. The electronic cash schemes are able in order to pay e-cash to merchants for the customers only due to privately protected communication networks.

So there is a great challenge before the engineers to necessitate for the application of new electronic payment method with very powerful algorithms of cryptography and security that is going to replace paper based cash schemes in the generations to come. In 1983 the first electronic cash system was proposed by CHAUM[12].

Motivation

In the scheme of Convertible Authenticated Encryption Scheme using message linkages, we observe that the complexity (such as computational cost and communication overhead) is very high for practical applications and sure enough there is a possibility to reduce it. So, we are interested in developing a convertible authenticated encryption scheme with message linkages with a low computational cost and communication overhead than the existing scheme.

Objective

To develop a new convertible authenticated scheme using message linkages with a low computational cost and communication overhead than the existing scheme.

Work done so far

In this thesis, we contribute the following:

Implementation of the existing scheme: Convertible authenticated encryption scheme with message linkages.

Design of convertible authenticated encryption scheme with low computation cost and communication overhead.

Implementation of the proposed scheme.

Comparison and analysis between the two schemes.

Organization of thesis

In Chapter 2, we have given the literature survey which includes the review of a convertible authenticated encryption scheme. At the end we have given the mathematical preliminaries which have been used throughout the thesis.

In Chapter 3, we have proposed our new convertible authenticated encryption scheme. Also the security analysis has been given in this chapter.

In Chapter 4, we have shown all the implementation results.

In Chapter 5 we provide conclusion of this thesis and future research directions.

CHAPTER II: BACKGROUND AND LITERATURE REVIEW

The first persons to put forward an idea about a scheme on digital signatures with discrete logarithm based message recovery technique were Nyberg and Rueppel [10, 13]. In order to decrease computational and communication costs of their method, Hoster et al. [4] proposed his scheme on authenticated encryption system, following which a number of such schemes were presented. In all of their methods, the signer would generate an encrypted signature and send it to the recipient. Once the signature is received, the recipient would verify the signature and generate the message.

In the recent times, Tseng et al. [15] have presented two schemes based on an authenticated encryption system using message linkage with more efficiency. One is a general one which would allow the recipient to get back the message as soon as the partial signature is received. The second one is a basic scheme which is better than all the old schemes in comparision to communication overhead and computational costs.

Further, consider the later dispute condition. For example, the signer repudiates. It means that he has actually signed the signature but he denies. In this way the recipient suffers from a danger of repudiation. He will be left helpless if he can’t prove the dishonesty of the signer. He needs the help of others to do it. That means even others should be able to verify the scheme. It may be necessary to reveal the actual information along with its signature for verification. In a situation of later dispute, to protect the benefit of receiver, we have to enable the receiver to convert the signature into an ordinary one which anyone and everyone can verify. By this the receiver can prove the dishonesty of the sender as he will be able to expose his mischief.

For this reason, Araki et al. [2] proposed a limited verifier method based on the convertible authenticated encryption scheme. However, it could fail in case of the signer is not ready to cooperate with the recipient. He actually signs the message but denies it. Hence, the signature conversion would require another parameter from the sender. Then Wu and Hsu [15] proposed another scheme based on the same convertible encryption method. When the sender does repudiation with the signature in this scheme, the recipient would be able to prove his dishonesty as he can reveal the ordinary version of the original signature which anyone can verify without any need of cooperation of the signer.

Review of Tseng et al.'s convertible authenticated encryption scheme

In this section, we shall present the Tseng et al.'s scheme: A convertible authenticated encryption scheme using message linkage [14]. In the presented scheme, in any normal case the signature has to be retrieved and checked by the specific recipient. Afterwards, the recipient reveals the ordinary signature for verification purpose, if in any case the signer would repudiate the signature. The Tseng et al.'s scheme consists of 4 phases namely System initialization, signature generation, message recovery and conversion phases. The following diagram illustrates the signature generation and message recovery phases of the existing scheme.

$Alice(U_a)$ $Bob(U_b)$

make $\mathrm{r}_0=0$

select a random integer $k \in GF(q)$

$r_i = M_i \,.\, h(r_{i-1} \oplus y_b^k) \bmod p$

$r = h(r_1 \| r_2 \| \ldots \| r_n)$

$R = h(M, r, h(g^k \bmod p)) \bmod q$

$S = k - Rx_a \bmod q$

$$\xrightarrow{(R,S,r,r_1,r_2,....,r_n)}$$

$r' = h(r_1 \| \mathrm{r}_2 \| \; . \; . \; . \; \| r_n)$

confirm $r' = r$

$M_i \ = \mathrm{r}_i.\mathrm{h}(\mathrm{r}_{i-1} \oplus (\mathrm{g}^S \mathrm{y}_a^R)^{x_b})^{-1}\mathrm{mod\ p}$

$R = h(M, r, h((g^S \mathrm{y}_a^R \mathrm{mod\ p}))\mathrm{mod\ q}$

Figure 3: Flow chart for the signature generation phase and message recovery phase [1]

System Initialization phase

These are the parameters used in the existing system. Let p be a large prime, q be a large prime factor of $p-1,\ g$ be a generator with an order q in galois field, $GF(p)$, and let $h(.)$ be a one-way hash function. Each user U_i has a secret key $x_i \in Z_q^*$. Each user then calculates his own corresponding public key using the equation $y_i = g^{x_i} \bmod p$. Let U_a be the sender $p-1,\ g$ and U_b be the receiver.

Signature generation phase

Let us consider that the sender, U_a is interested in delivering a large message M to the particular receiver, U_b. Let us assume that the message M is divided into small message blocks in the sequence $\{M_1, M_2, \ . \ . \ . \ , M_n\}$, where $M_i \in GF(p)$. After this, U_a executes the following steps for creating the signature blocks for the corresponding message blocks $\{M_1, M_2, \ . \ . \ . \ , M_n\}$.

Step I: Let $r_0 = 0$ and choose a random integer $k \in GF(q)$.

Step II: Compute $r_i = M_i . h(r_{i-1} \oplus y_b{}^k)\ modp$ for all i = 1,2,. . . ,n, where "$\oplus$" refers to the exclusive operator.

Step III: Compute $r = h(r_1 \| r_2 \| . . . \| r_n)$, where ‘‘||’’ refers to concatenation operator.

Step IV: Compute $R = h\left(M,\ r,\ h\left(g^k mod\ p\right)\right)\ mod\ q$.

Step V: Compute

$$S = k - Rx_a mod\ q. \qquad (1)$$

U_a sends the generated blocks of signature $\left(R, S,\ r,\ r_1,\ r_2,\ . . ,\ r_n\right)$ to the recipient U_b through an open transmission medium. r_i is the message linkage parameter in between the $\left(i\ +\ 1\right)^{th}$ & i^{th} blocks of message.

Message recovery phase

Once the signature blocks are received, ie; $U_b, \left(R, S,\ r,\ r_1,\ r_2,\ . . ,\ r_n\right)$ can retrieve the original blocks of message $\left\{M_1, M_2,\ . . . , M_n\right\}$ by executing these steps:

Step I: Compute $r_0 = h(r_1 \| r_2 \| . . . . . .r_{n-1} \| r_n)$ and check whether $r' = r$ or not. If it matches proceed to next step.

Step II: Retrieve the original blocks of message $\left\{M_1, M_2,\ . . . , M_n\right\}$ in the given way:

$$M_i = r_i .\ h(r_{i-1} \oplus \left(g^S y_a{}^R\right)^{x_b})^{-1} mod\ p, \qquad (2)$$

for all $i\ =\ 1, 2, . . . , n$ as well as $r_0 =\ 0..$

Step III: Verification of the signature should be done using this equation:

$$R = h\left(M,\ r,\ h\left(g^S y_a{}^R\right)^{x_b}\right)^{-1} mod\ p))\ mod\ q: \qquad (3)$$

If it is matching, then the signature is considered valid and then conversion is done.

Conversion phase

If the signer, U_a is found repudiating the signature, then then receiver, U_b is capable to prove the dishonesty of U_a by just exposing the ordinary signature $\left(R, S,\ r\right)$ generated for message M. Using this ordinary signature which we got from converting the original signature, anybody can validate it using Eq. (3). So, let us prove the correctness of the existing scheme:

In message recovery phase, the receiver U_b recovers the message using *Eq.* (2).

Proof . According to *Eq.* (2), we have

$$
\begin{aligned}
& r_i \cdot f(r_{i-1} \oplus (g^S y_a^R)^{x_b})^{-1}, \\
& = r_i \cdot f(r_{i-1} \oplus (g^{k-Rx_a} y_a^R)^{x_b})^{-1}, \\
& = r_i \cdot f(r_{i-1} \oplus (g^k y_a^{-R} y_a^R)^{x_b})^{-1}, \\
& = r_i \cdot f(r_{i-1} \oplus (g^k)^{x_b})^{-1}, \\
& = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1}, \\
& = M_i \bmod p.
\end{aligned}
$$

In conversion phase, the ordinary signature is verified using *Eq.* (3).

Proof . According to *Eq.* (3), we have

$$
\begin{aligned}
& h(M, r, h(g^S y_a^R \bmod p)), \\
& = h(M, r, h(g^{k-Rx_a} y_a^R \bmod p)), \\
& = h(M, r, h(g^k y_a^{-R} y_a^R \bmod p)), \\
& = h(M, r, h(g^k \bmod p)), \\
& = R \bmod q.
\end{aligned}
$$

Security analysis of the Tseng et al. scheme

The existing scheme is similar to the digital signature scheme when security is considered. It is very difficult in finding solution to a discrete logarithmic problem [4.6] and a one-way hash function [9]. The security of the existing scheme is primarily based upon these two features which it imbibes. Let us take into consideration some common possible attacks against the existing scheme and try to analyze how the scheme responds to theme and how it withstands the attacks.

The existing scheme is successful in providing all the four functions of security i.e confidentiality, non-repudiation, integrity and authentication. In this section we will see how the existing scheme will satisfy the above mentioned attributes:

Attack 1: Eve already has information of one of the small message blocks M_i and thus he attempts for obtaining the common key ${y_a}^{x_b}$ and in turn the rest of the message blocks.

Analysis of attack 1: Eve can compute the equation $h(r_{i-1} \oplus y_b{}^k) = M_i^{-1}.\, r_i \; mod\; p$. Let us consider that he can get the value of $y_b{}^k$, which goes to show that $y_a{}^{x_b}$ can be derived using $y_b{}^k = \left(g^S y_a{}^R\right)^{x_b} mod\; p$. In any case, breaking the one way hash function and getting the value of $y_b{}^k$ is very difficult. Eve can never be able to obtain the rest of the blocks of message using Equation 2 because of non-availability of the value of $y_b{}^k$.

Attack 2: Eve tries to get the secret key, x_i of the user from all the available information publicly.

Analysis of attack 2: Let us assume, Eve intends to get the U_a's private key x_a using the corresponding public key of U_a, $y_a = g_a{}^x mod\; p$. It is very difficult because of usage of discrete logarithms. Hence to get U_a's secret key x_a is highly impossible. Eve cannot get secret key of U_a, x_a simply from exisiting signature using Equation 1, because we already know that Equation 1 has two unknown variables namely k and x_a. As we can see, even k is based upon discrete logarithmic problem as well as one-way hash function.

Attack 3: Eve tries to forge the ordinary converted signature so as to pass Equation 3.

Analysis of attack 3: It's not so easy to determine R and r, given S, as we already know that discrete logarithm values as well as one-way hash function are quite difficult to be solved as we can observe from equation 3. Just similar to this, suppose R and r are given, then it is also highly infeasible to derive the value of S in such a way that it satisfies Equation 3.

Attack 4: Eve tries to forge the signature blocks delivered by Alice.

Analysis of attack 4: Eve should have information of the key $y_b{}^k$ in order to build up the signature to satisfy the equation 2. Eve would encounter lot of difficulty just similar to Attack 1.

Attack 5: Eve attempts to verify the authenticated encryption signature before even converting it.

Analysis of attack 5: Eve badly needs the message, M in order to perform the verification of authenticated encryption signature in Equation 3. Eve will not be able to retrieve the message block M_i, just as in case of Attack 6. Hence, there is no possibility of verification of the signature.

Attack 6: Eve tries to retrieve a small message block M_i from the encrypted signature.

Analysis of attack 6: Eve can retrieve message block, M_i from Equation 2, only if he has the secret key of either bob or Alice i.e. x_a or x_b. It's quite difficult to break the discrete logarithm problem and find out the secret key of user, just as in case of Attack 1.

Attack 7: Eve tries to modify, reorder and replicate or remove the blocks of message.

Analysis of attack 7: The signature $R = h\left(M, r, h\left(g^k mod\ p\right)\right) mod\ q$ will undergo a change if Eve modifies, reorders, replicates or deletes even one of the signature blocks. Since, the relation $r = h(r_1 \| r_2 \| . . . . \| r_n)$ is not going to exist any more, the signature blocks can never pass the verifying equations. Hence, the changes will be definitely detected by the recipient.

Setup

The parameter 1 of security when given as input to the setup algorithm, the public parameters are formed by the following results.

Let, $q, p:$ two prime numbers, which are large, in such a way that the q is a prime divisor of (p – 1) . Let g be an element of Z_p^* of the order, q.

$H : \{0,1\} * \in Z_q^* :$ It is a collision resistant one-way hash function.

Key generation function

The KeyGen algorithm generates the public and secret key pairs of signer and receiver.

Bobs Public key $y_B = g^{x_B} \bmod p$.

Bobs Private Key $x_B \in Z^*$

Alice's Public key $y_A = g^{x_a} \bmod p$

Alice's Private Key $x_a \in Z^*$ q

Mathematical preliminaries

We used the following basic notation, definitions and models used throughout this thesis.

Notation and terminology

All the discussed groups in the project are considered abelian groups. Groups of prime order have useful properties and are widely used in cryptography. All groups of prime order are p cyclic. If there exists an element $g \in G$, group G is considered cyclic. For each $g_0 \in G$, there exists an integer a with $g_0 = g_a$. Such an element $g \in G$ is referred to as generator of G. The integers field mod p is denoted as Z_p, for any prime, p. The multiplicative cyclic group of all the non-zero elements in the field of integers mod p, Z_p is denoted as Z [27].

Discrete Logarithmic Problem (DLP)

To be specific and more focused discrete logarithms are considered analogous to the normal ones group theoretically. If h and g are the elements of one finite cyclic group called G then a solution to the equation, $gx = h$, let it be x, is referred to as discrete logarithm for the base g of h in G. Similarly, over the complex or real numbers, the simple logarithm, $log(a,b)$ is a solution to the equation, $ax = b$. To be concise, if G is a finite group, the problem discrete logarithm in group, G is the following computational problem: given elements β and α in G, determine an integer x is considered in such a way that the equation, $\alpha^x = \beta$ is satisfied, provided x exists [11].

Computational Diffie-Hellman problem

If g is generator of a group (more specifically we are talking about the multiplicative group of any finite field) and x, y are randomly choosen integers. Let us consider one group G of order q, where G is cyclic. Then the Computational Diffie Hellmen method says that, if given a set (g, g^a, g^b) for any randomly choosen generator, say g and $a, b \in \{0, ..., q-1\}$ it is incompatible computationally to compute the x, y values [6]. This is the Computational Diffie-Hellmen problem.

The Integer Factorization Problem

Definition: Given an integer n which is positive, the problem of integer factorization says that to find its prime factorization, we need to use the equation $n = p_1^{e1} p_2^{e2} .. p_n^{ek}$. Here, p_i is a distinct prime and each ei ≥ 1.

Safe Primes

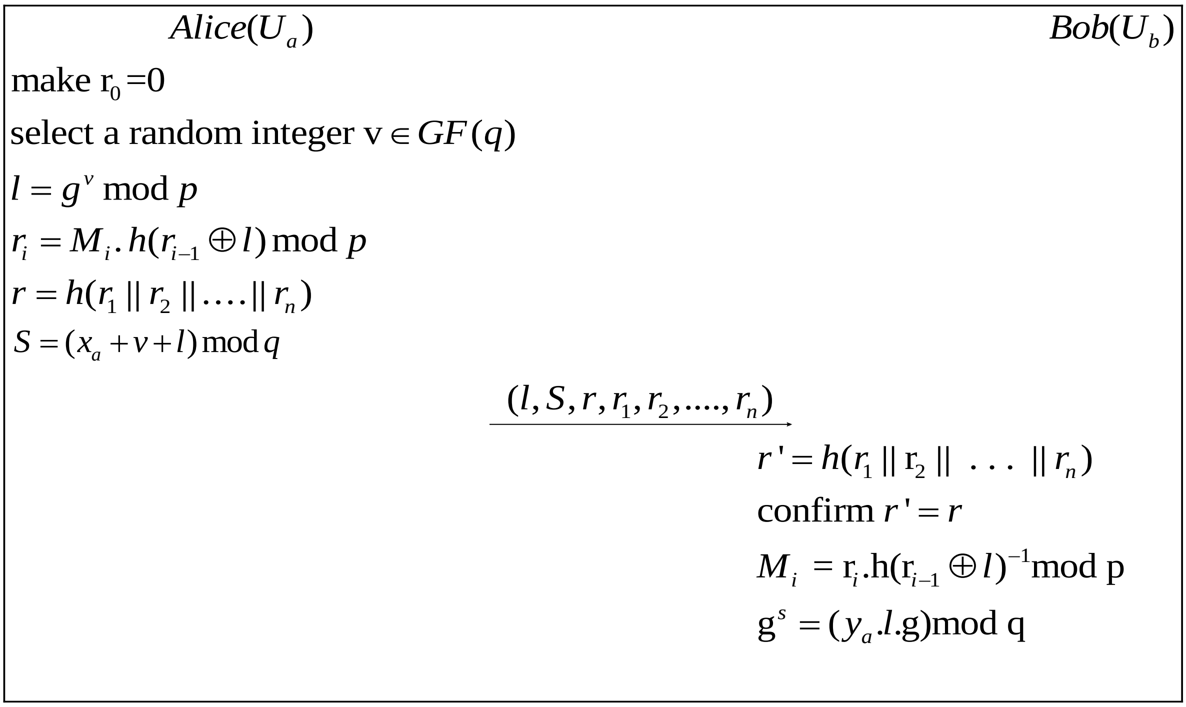
These primes are also known as safe primes because they have a very good relation with the stronger ones. Let q be a number that is a prime, then it is considered a strong prime whenever q-1 and q+1 will possess large prime factors. For a safe prime, the equation q = 2p + 1 should satisfy, then p is considered to be a large prime factor according to the equation. Since the safe primes are used extensively in discrete logarithmic techniques such as Diffie Hellmen key exchange, they are considered very important especially in the field of cryptography. [23].

CHAPTER III: PROPOSED CONVERTIBLE AUTHENTICATED ENCRYPTION SCHEME WITH MESSAGE LINKAGES

In this chapter we propose a convertible authenticated encryption scheme with message linkages based upon the previous scheme, but with improved computational cost and communication overheads.

Proposed Scheme

Let us have a look at the four phases in our proposed scheme. They are namely system initialization, signature generation, message recovery, and conversion phases. The Figure 3 representing the signature generation phase and message recovery phase and description of individual phases is given below.



$Alice(U_a)$ $Bob(U_b)$

make r_0 =0

select a random integer $\mathrm{v} \in GF(q)$

$l = g^v \bmod p$

$r_i = M_i . h(r_{i-1} \oplus l) \bmod p$

$r = h(r_1 \,||\, r_2 \,||\, \ldots \,||\, r_n)$

$S = (x_a + v + l) \bmod q$

$\xrightarrow{(l, S, r, r_1, r_2, ..., r_n)}$

$r' = h(r_1 \,||\, \mathrm{r}_2 \,||\, \ . \ . \ . \ \,||\, r_n)$

confirm $r' = r$

$M_i \ = \mathrm{r}_i.\mathrm{h}(\mathrm{r}_{i-1} \oplus l)^{-1} \mathrm{mod\ p}$

$\mathrm{g}^s = (y_a.l.\mathrm{g}) \mathrm{mod\ q}$

Figure 4: Flow chart for the signature generation and message recovery phase of proposed scheme.

System initialization phase

Let, p be a large prime number, q be large prime factor of (p – 1). Let g be one of the generators with order q in galois field, GF(p). Let, H be one-way hash function in our scheme. Let, U_a be the sender and U_b be the receiver. The Secret key of U_a is x_a, public key of U_a is y_a. Secret key of U_b is x_b and the respective public key is $y_b = g^{x_b} \bmod p$.

Signature Generation Phase

Assume that the Alice, U_a sends a large message, M to Bob, U_b. Here, the message M is composed of a sequence $\{M_1, M_2, \ldots, M_n\},$, where $M_i \in GF(p)$. U_a performs the given operations in order to generate the blocks of signature for M.

Step I : Sets $r_0 = 0$ and chooses V in random from Z_q^*.

Step II : Compute $l = g^V mod\ p$.

Step III : Computes $r_i = M_i.H(r_{i-1} \oplus l)$

$$r = H(n, r_2, \ldots, r_n) \qquad (1)$$

$$S = (x_a + v + l)\ mod\ q \qquad (2)$$

So, U_a uses the public medium to send the blocks of signature $(l, S, r, r_1, r_2, \ldots, r_n)$ safely to Bob, U_b. Here, r_i is the message linkage parameter in between $(i+1)^{th}$ *and* i^{th} block of message.

Message recovery phase

Once the signature blocks, $\left(l,\ s,\ r,\ r_1,\ r_2,\ ...\ r_{n-1},\ r_n \right)$ are received U$_b$ can retrieve the small blocks of message $\left\{ M_1,\ M_2,\ ...\ ,M_n \right\}$ as per the below given steps.

Step I : Computes $r' = H\left(r_1,\ r_2,\ ...\ ,\ r_n\right)$ as well as checks iff $r' = r$.

Step II : Using the equation below, verifies the encrypted signature.

$g^S = y_a .\ l\ .\ g^l$ If the above condition satisfies, then the signature is a valid one.

Step III : Recovers the small blocks of message $\left\{ M_1,\ M_2,\ ...\ ,M_n \right\}$ in the following way:

$M_i = r_i . H(r_{i-1} \oplus l)^{-1}$ for all $i = 1,\ 2,\ ...\ ,\ n\ and\ r_0 = 0.$

Correctness

$$g^S = g_a^{(x+v+l)} = g_a^{\ x} . g^{v+l} = g_a^{\ x} . g^v . g^l = y_a . g^v . g^l = y_a .\ l\ .\ g^l .$$

Comparision

Table 1: Comparison between existing and proposed scheme

	Tseng Et Al’s Scheme	Proposed Scheme
Signature Generation	3H + 2M + 2E	2H + M + E
Message Recovery	4H + 2M + 5E + I	2H + 3M + E + I

Security analysis of the proposed scheme

Our new scheme is found to be as secure as the existing one. The security of all the previous schemes depends upon the complexity in breaking discrete logarithms [4, 6] and one-way hash function [9]. We shall assume common security attacks against the scheme proposed by us and hence we shall prove that our scheme can pass all those possible security attacks which the existing scheme could do.

As we have already seen that our scheme would provide 4 notion of security i.e. non-repudiation, confidentiality, integrity and authentication. In this section, we shall observe how our proposed scheme is going to satisfy all the four attributes:

Attack 1: Eve already has information of one of the small message blocks M_i and thus he attempts for obtaining the common key l and in turn the rest of the message blocks.

Analysis of attack 1: Eve can compute the equation $h(r_{i-1} \oplus l) = M_i^{-1}. r_i \ mod\ p$. Let us consider that he can get the value of l, which goes to show that $y_a^{x_b}$ can be derived using $y_b^k = (l)^{x_b} \ mod\ p$. In any case, breaking the one way hash function and getting the value of l is very difficult. Eve can never be able to obtain the rest of the blocks of message using Equation 2 because of non-availability of the value of l.

Attack 2: Eve tries to get the secret key, x_i of the user from all the available information publicly.

Analysis of attack 2: Let us assume, Eve intends to get the U_a's private key, x_a using the respective public key of U_a, $y_a = g_a^x mod\ p$. It is very difficult because of usage of discrete logarithms. Hence to obtain U_a's secret key x_a is highly impossible. Eve cannot get U_a's secret key, x_a simply from the signature using Equation 1, because we already know that Equation 1 has two unknown variables namely k and x_a. As we can see, even k is based upon the discrete logarithmic problem and the one-way hash function.

Attack 3: Eve tries to forge the ordinary converted signature so as to pass Equation 3.

Analysis of attack 3: Given S, it's not so easy to determine r as we already know that discrete logarithm values and one-way hash function are quite difficult to be solved as we can observe from equation 3. Just similar to this, suppose r is given, then it is also highly infeasible to derive the value of S in such a way that it satisfies Equation 3.

Attack 4: Eve tries to forge the signature blocks delivered by Alice.

Analysis of attack 4: Eve should have information of the key l in order to build up the signature to satisfy the equation 2. Eve would encounter lot of difficulty just similar to Attack 1.

Attack 5: Eve attempts to check the authenticated encryption signature before even converting it.

Analysis of attack 5: Eve badly needs the message, M in order to perform the verification of authenticated encryption signature in Equation 3. Eve will not be able to retrieve the message block M_i, just as in case of Attack 6. Hence, there is no possibility of verification of the signature.

Attack 6: Eve tries to retrieve a small message block M_i from the encrypted signature.

Analysis of attack 6: Eve can retrieve the message block, M_i from Equation 2, only if he has the secret key of either bob or Alice i.e. x_a or x_b. It's quite difficult to break discrete logarithmic problem and find out the secret key of user, just as in case of Attack 1.

Attack 7: Eve tries to modify, reorder and replicate or remove the blocks of message.

Analysis of attack 7: The signature will undergo a change if Eve modifies, reorders, replicates or deletes even one of the signature blocks. Since, the relation

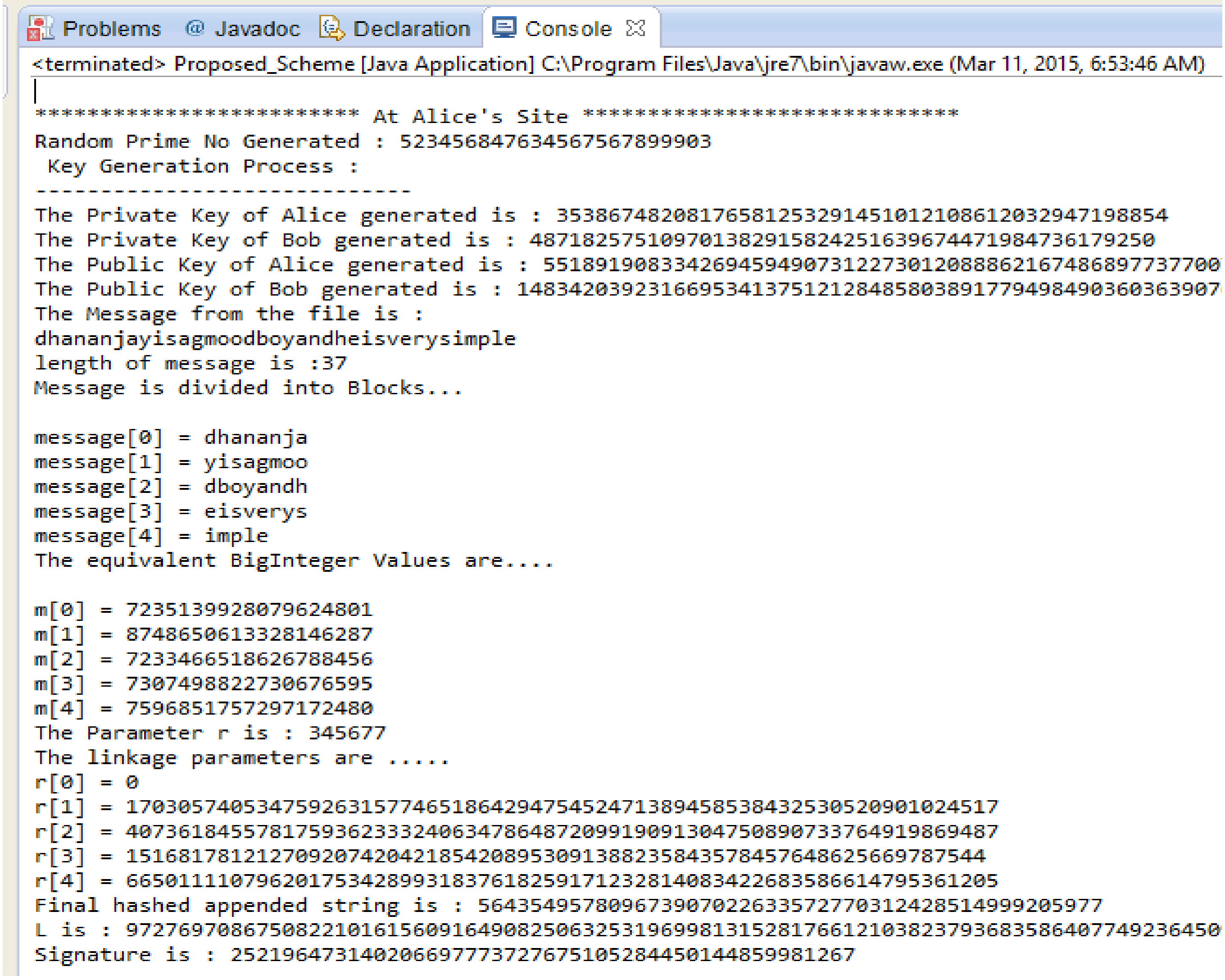
$r = h(r_1 \| r_2 \| . . . . \| r_n)$ is not going to exist anymore the signature blocks can never pass the verifying equations. Hence, the changes will be definitely detected by the recipient.

Attack 8: Eve attempts to select the cipher text, delivers it to Alice, and in return gets the respective plaintext or some part thereof.

Analysis of attack 8: It is well known that a plain RSA is susceptible to CCA Attacks, but in this algorithm, we have a random component introduced which ensures that it is no more a plain RSA. Also, for decryption of any message, Eve needs the private key x_a or x_b. But, breaking the Discrete Logarithm and getting the private key is very difficult. Hence, it is resistant to CCA attacks.

CHAPTER IV: IMPLEMENTATION RESULTS

The proposed scheme is implemented in Java using java.security package. We have taken input as different size of messages and time for the generation of signature and retrieval of message is compared for different message sizes. Here are some screen shots of the output of our program:

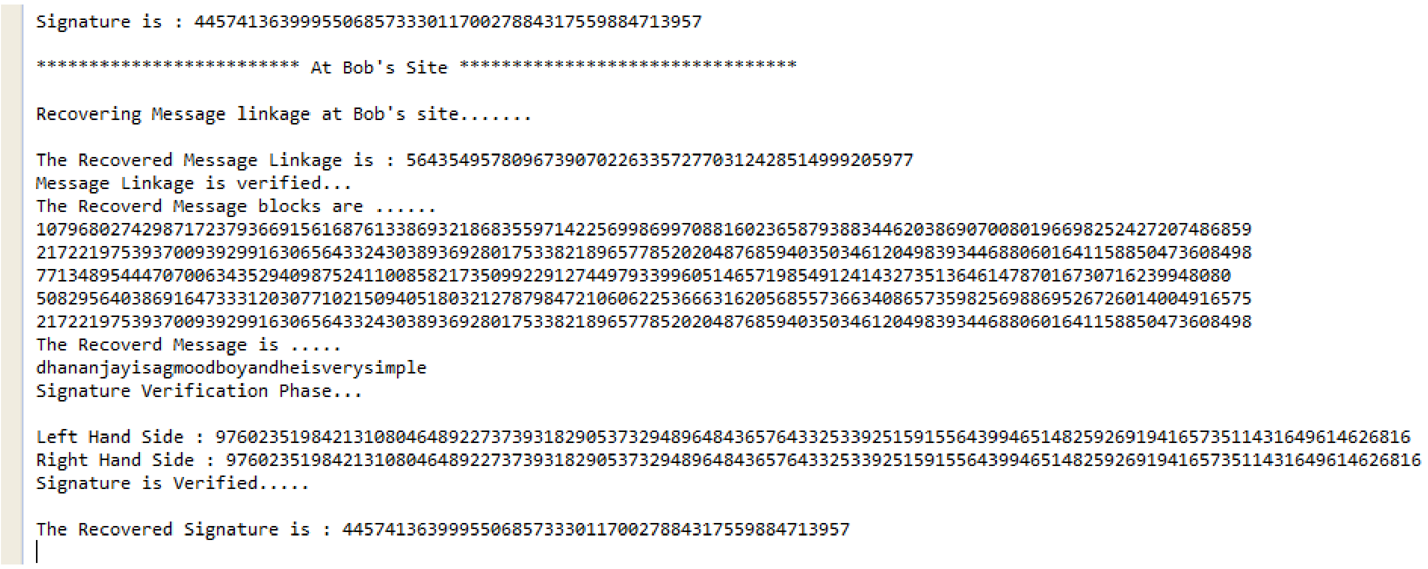


```
<terminated> Proposed_Scheme [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Mar 11, 2015, 6:53:46 AM)
|
************************* At Alice's Site *****************************
Random Prime No Generated : 523456847634567567899903
 Key Generation Process :
-----------------------------
The Private Key of Alice generated is : 35386748208176581253291451012108612032947198854
The Private Key of Bob generated is : 487182575109701382915824251639674471984736179250
The Public Key of Alice generated is : 551891908334269459490731227301208886216748689773770
The Public Key of Bob generated is : 148342039231669534137512128485803891779498490360363907
The Message from the file is :
dhananjayisagmoodboyandheisverysimple
length of message is :37
Message is divided into Blocks...

message[0] = dhananja
message[1] = yisagmoo
message[2] = dboyandh
message[3] = eisverys
message[4] = imple
The equivalent BigInteger Values are....

m[0] = 7235139928079624801
m[1] = 8748650613328146287
m[2] = 7233466518626788456
m[3] = 7307498822730676595
m[4] = 7596851757297172480
The Parameter r is : 345677
The linkage parameters are .....
r[0] = 0
r[1] = 1703057405347592631577465186429475452471389458538432530520901024517
r[2] = 4073618455781759362333240634786487209919091304750890733764919869487
r[3] = 151681781212709207420421854208953091388235843578457648625669787544
r[4] = 6650111107962017534289931837618259171232814083422683586614795361205
Final hashed appended string is : 56435495780967390702263357277031242851499205977
L is : 972769708675082210161560916490825063253196998131528176612103823793683586407749236450
Signature is : 252196473140206697773727675105284450144859981267
```

Figure 5: Screenshot of the output for message at the Alice's Site



```
Signature is : 44574136399955068573330117002788431755988471395 7

************************* At Bob's Site ********************************

Recovering Message linkage at Bob's site.......

The Recovered Message Linkage is : 564354957809673907022633572770312428514999205977
Message Linkage is verified...
The Recoverd Message blocks are ......
1079680274298717237936691561687613386932186835597142256998699708816023658793883446203869070080196698252427207486859
2172219753937009392991630656433243038936928017533821896577852020487685940350346120498393446880601641158850473608498
771348954447070063435294098752411008582173509922912744979339960514657198549124143273513646147870167307162399480 80
5082956403869164733312030771021509405180321278798472106062253666316205685573663408657359825698869526726014004916575
2172219753937009392991630656433243038936928017533821896577852020487685940350346120498393446880601641158850473608498
The Recoverd Message is .....
dhananjayisagmoodboyandheisverysimple
Signature Verification Phase...

Left Hand Side : 97602351984213108046489227373931829053732948964843657643325339251591556439946514825926919416573511431649614626816
Right Hand Side : 97602351984213108046489227373931829053732948964843657643325339251591556439946514825926919416573511431649614626816
Signature is Verified.....

The Recovered Signature is : 445741363999550685733301170027884317559884713957
|
```

Figure 6: Screenshot of the output for message at the Bob’s Site

CHAPTER V: CONCLUSION

In this thesis, we propose a better convertible authenticated encryption scheme with lesser computational cost and communication overhead. This scheme preserves all the required security properties such as integrity, authenticity, confidentiality, non-repudiation, etc. Though modifications were made, the previous advantages and strengths were kept intact without any compromise. Also, our scheme reduces the communicational overheads as well as the computational costs to further extent both in receiver and sender side.

In future research can be done on our scheme to further lower its computation cost and communication overhead. Also research can be done to incorporate this feature to some of the highly proved secured encryption schemes which can be applicable to highly security sensitive application such as e-cash, e-bidding, e-voting, e- transactions etc.

REFERENCES

[1] Behrouz A. Forouzan. Cryptography and Network Security. Tata McGraw-Hill, 2007.

[2] Ting-Yi Chang, “A Convertible Multi-Authenticated Encryption scheme for group communications,” Information Sciences, vol. 178, no.17, May 2008, pp. 3426-3434.

[3] Ting-Yi Chang, “An Computation-Efficient Generalized Group-Oriented Cryptosystem,” Informatica, vol. 21, no. 3, August 2010, pp. 1-14.

[4] L. H. Encinas, A. M. del Rey, and J. M. Masqu´e, “A Weakness in Authenticated Encryption Schemes Based on Tseng et al.’s Schemes,” International Journal of Network Security, vol. 7, no. 2, 2008, pp. 157–159.

[5] Abdel-Hafez Ahmed, Miri A, Orozco-Barbosa Louis. Authenticated group key agreement protocols for ad hoc wireless networks. Int J Network Secur 2007; 4(1):90–8.

[6] Araki Shunsuke, Uehara Satoshi, Imamura Kyoki. The limited verifier signature and its application. IEICE Trans Fundament 2009; E82-A(1):63–8.

[7] Choo KKR. Revisit of mccullagh-barreto two-party id-based authenticated key agreement protocols. Int J Network Secur 2005; 1(3):154–60.

[8] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Informat Theory (IT-31) 1985:469–72.

[9] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs. Electronics Lett 1994;30(15):1212.

[10] Hwang MS, Chang TY. Threshold signatures current status and key issues. Int J Network Secur 2005;1(3):123–37.

[11] Diffie, W., Hellman, M., 1996. New directions in cryptography. IEEE Transactions on Information Theory IT-22 (6), 644–654.

[12] Mangipudi KV, Katti RS. A hash-based strong password authentication protocol with user anonymity. Int J Network Secur 2006;2(3):205–9.

[13] Mangipudi KV, Katti RS, Fu H. Authentication and key agreement protocols preserving anonymity. Int J Network Secur 2006;3(3): 259–70.

[14] He, W.H., Wu, T.C., 1999. Cryptanalysis and improvement of Petersen–Michels signcryption scheme. IEE Proceedings – Computers and Digital Techniques 146 (2), 123–124.

[15] Mitchell, C.J, Piper, F., Wild, P., 2012. Digital signature. In: Simmons, G.J. (Ed.), Contemporary Cryptology: The Science of Information Integrity. IEEE Press, New York.

[16] Petersen, H., Michels, M., 2008. Cryptanalysis and improvement of signcryption schemes. IEEE Proceedings – Computers and Digital Techniques 145 (2), 149–151.

[17] Rivest, R., Shamir, A., Adleman, L., 1978. A method for obtaining digital signature and public-key cryptosystem. Communications of the ACM 21 (2), 120–1.