Design and Analysis of Shortened Digital Signature Algorithms Based on Complex Public Key Cryptosystem

'MS' Research Thesis

By

Subhanullah

(571-FBAS/MSCS/F09)

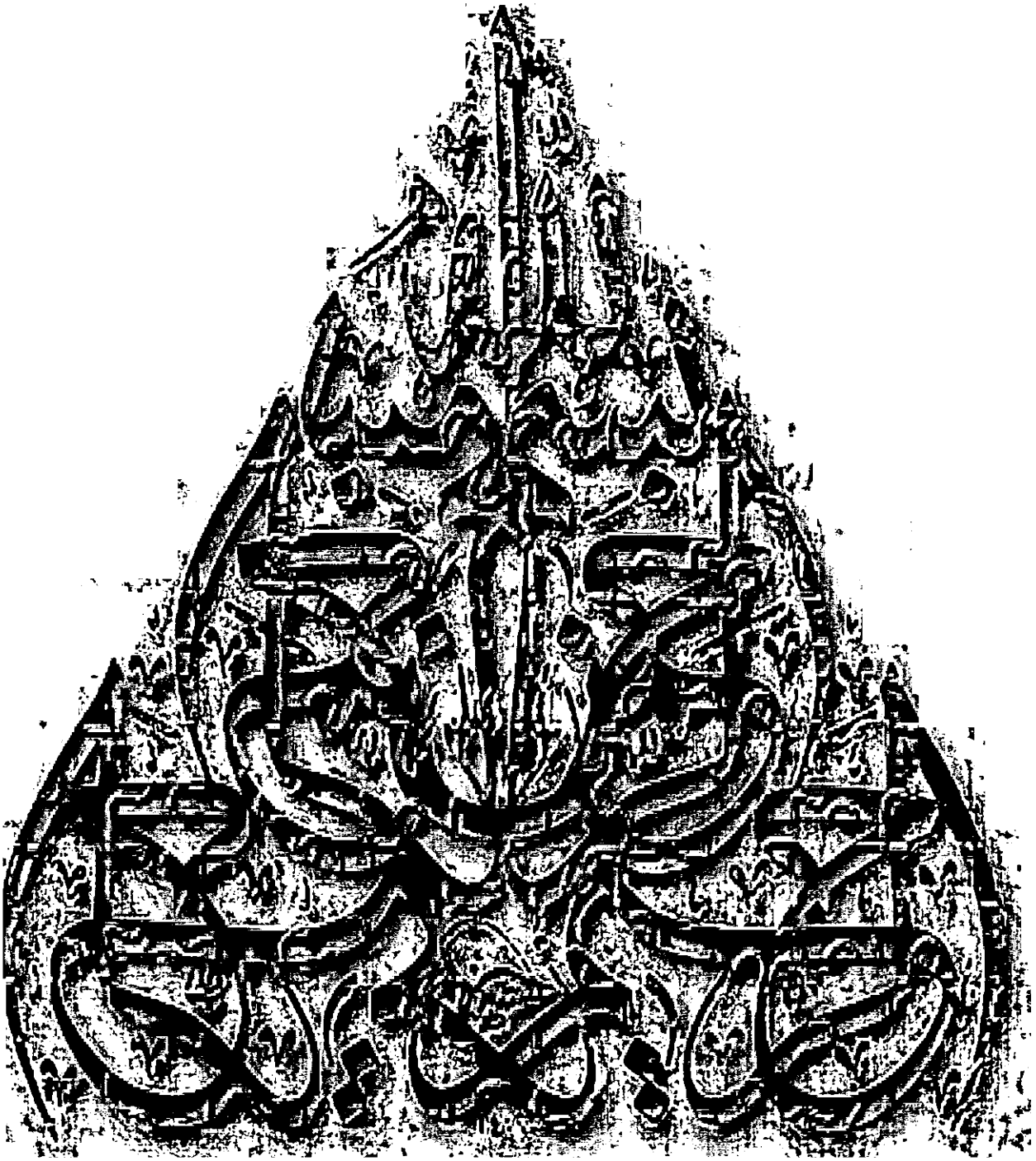
Supervisor

Prof. Dr. Muhammad Sher
Dean Faculty of Basic and Applied Sciences

Department of Computer Science & Software Engineering
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad

2013

1- Digital supercomputers



International Islamic University, Islamabad

Faculty of Basic & Applied Sciences, Department of Computer Science & Software Engineering

Dated: April 15, 2013

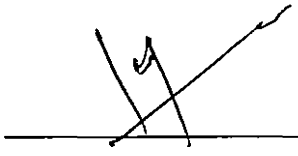
FINAL APPROVAL

It is certified that we have read the thesis, entitled **"Design and Analysis of Shortened Digital Signature Algorithms Based on Complex Public Key Cryptosystem"**, submitted by Subhanullah, Reg. No. 571-FBAS/MSCS/F09. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for MS Degree in Computer Science.

THESIS EVALUATION COMMITTEE

External Examiner:
Dr. Qaisar Abbas Naqvi
Associate Professor
Department of Electronics, Quaid-i-Azam University,
Islamabad, Pakistan

Internal Examiner:
Mr. Syed Muhammad Saqlain
Assistant Professor
Department of Computer Science & Software Engineering
International Islamic University, Islamabad, Pakistan



Supervisor:
Prof. Dr. Muhammad Sher
Dean FBAS and Chairman,
Department of Computer Science & Software Engineering
International Islamic University, Islamabad, Pakistan

ABSTRACT

Discrete Logarithm Problem and Integer Factorization Problem based Digital Signatures are using very large numbers to provide enough security. These Digital Signatures are not applicable for devices having small memory size and less computational power. In this thesis four shortened Complex digital signature algorithms has implemented that are using small numbers and provide enough security. These Shortened Complex Digital Signature Algorithms using hard mathematical Complex Discrete Problem which is more difficult to solve as compare to the Discrete Logarithm or Integer Factorization Problem's based digital signature. This Shortened Complex Digital Signature Algorithm will be compatible for devices having less memory size and small computational capability. These Algorithms take less time during signing and verification process by comparing with previous digital signatures.

DECLERATION

I hereby declare that this present research work has been carried out by me under the sincere supervision of Prof. Dr. Muhammad Sher. It is further declared that this work, neither as a whole nor as a part has been copied out from any source. If any part of this research work is proved to be copied out from any source or found to be reproduction of some other research work, I shall stand by the consequences. The presented work in this dissertation has not been submitted elsewhere for support of any other degree, diploma, fellowship or any other similar title.

Date: 15 April, 2013

SUBHANULLAH

571-FBAS/MSCS/F09

DISSERTATION

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of

The degree of

MS in Computer Science

DEDICATION

This thesis is dedicated to my parents for their endless love, support and encouragement. This thesis also dedicated to my beloved wife for her love and patience.

ACKNOWLEDGEMENT

All praise and thanks to Almighty Allah, the most Gracious, the most Merciful. Peace and mercy be upon His Prophet (Peace Be upon Him).I am grateful to my Supervisor Prof. Dr. Muhammad Sher Chairman Department of Computer Science and Software Engineering, who spares his valuable time in guiding me for my research work. He encourages me always. I am short in word to express his contribution to this thesis through criticism, suggestions and discussions. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project. I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance, help and for their views which helped me in improving the proposal. There is no word to express my feeling for my family members and relatives, especially to my parent for their hidden cooperation and to my wife for her enthusiastic inspirations, round the clock cooperation and help me in many ways. Really, it is not possible to express the love and affection to sweet and little children whose are drivers of my success, to make the path for my MS Research work. My sincere thanks are to Mr. Nizamuddin for their kind suggestions. I am also thankful to my classmates Mr. Zahid Mehmood Ch, Mr. Yasir Shabir, for their result oriented discussions. Special thanks to Mr. Kafeel Ahmed, Mr. Syed Qiam Ali Shah and Mr. Hazrat Jan, who are always being there for me whenever I needed them for their help, generosity and moral support.

SUBHANULLAH

571-FBAS/MSCS/F09

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIUGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CDLP	Complex Discrete Logarithm Problem
DLP	Discrete Logarithm Problem
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm
IFP	Integer Factorization Problem
MD	Message Digest
PDA	Personal Digital Assistant
RFID	Radio Frequency Identification
SDSS	Shortened Digital Signature Scheme
SHA	Secure Hash Algorithm
SCDSA	Shortened Complex Digital Signature Algorithm
www	World wide web

CHAPTER 1

INTRODUCTION

1.1Introduction

Internet isdefinitely become the largest public data network, enable and facilitate both personal and business transmissions and communications worldwide. It has also broughta lot of improvement, accessibility and liberties in every field of life, especially in business, online bank transaction, online correspondence and exchange of sensitive personal information. The transmission and communication over the Internet and corporate networks is increasing day by day. These communication is taking place through E-mail, mobile network, telecommunications as well as organizations are remotely connect to their branch offices networks through Internet, and commercial transactions are accomplishedover the internet, via the World WideWeb [16]. Undoubtedly Internet has transformed and brought a lot of improvement in business world however these applications are at risk to fraudulent activists like Hackers, viruses and individual or human error to change, duplicate or intercept the data.Due to this perception some questions are arises that need proper attention.

- How secrecy maintain during transmission, so that nobody get unauthorized access to the informationof the transmitted message?
- How can the sender of the message ensure that the transmitted message exactly received by the intended recipient?
- How can the recipient of message ensure himself that this is the message sent by the intended sender?

Therefore the authentication and integrity as well as confidentiality of the information are the ultimate requirement for these applications [18].

In this thesis I will examine the variant of El-Gamal signature scheme which is known as Digital Signature Standard [39] which is based on Discrete Logarithm problem.

1.2Network Security Concepts

Network security is used to prevent fraudulent attacks and ensure that the data traveling across the network is secure.Network security comprises on detection, prevention and response, is called security trinity [17]. See Figure 1.1.

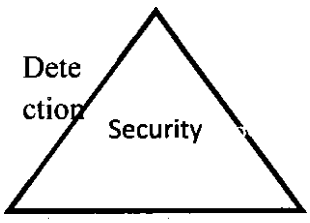


Figure 1.1: security Trinity

1.2.1 Prevention

Prevention is the base of security trinity used to measure the prevention of the exploitation of vulnerabilities. To design network security schemes, preference should be given to Preventative measures over detection and response [17].

1.2.2 Detection

After preventative measures some procedures are need to detect potential problems where preventative measure failure occur [17].

1.2.3 Response

A proper plan is required to be developed by organization toidentifyan appropriate response tosecurity breach [17].

1.3 Cryptography

Cryptography is the field of network securityto designProtocols, technique and algorithms to achieve thesesecurity goals [18].

1.3.1 Cryptosystem

Cryptographic scheme using a key to encrypt and decrypt information called cryptosystem [18]. The keys used for encryption and decryption will be same, or one key is used for encryption and its derived key will be used for decryption.

1.3.1.1 Symmetric Cryptosystem

Cryptosystem is called symmetric if the same key is used for encryption and decryption between the two communicating parties.Consider A and B are two communicating parties, and M is a message sending from A to B. The communicating party A will encrypt the message M by its secret key k and then send to other communicating party B. The same key will be used by B to decrypt the message and recover M. It is fastest cryptosystem but the management of key exchange and security in a large network is more difficult, because the communicating parties must first agree on a session key for a certain time to encrypt all communications. It will required $n\ (n-1)/2$ session keys for n users.

1.3.1.2 Asymmetric Cryptosystem

An asymmetric keycryptosystem is also called Public key cryptosystem, using different keys for encryption and decryption operation. In this technique, the message has encrypted by sender A with a secret key E_k and sends toB. To recovers the message, B using the derived or public key (D_k), of the sender A. It best for key management but very slow as compare to symmetric cryptosystem. If there is n communicating parties then it required 2n session keys.

1.4 One Way Functions

One-way functions are those functions which are easily calculated in one direction but very difficult to calculate in the reverse direction. It means that millions of years will take a function to get in reverse direction. It has many examples like computing Square Roots, Discrete Logarithm Problem and Integer Factorization Problem in a finite field.

1.5Digital Signature

As physical signature is used for the purpose of authentication in real world, similarly when the agreements and all decisions are electronically communicated, we need digital signing. Public key cryptography presented this service by using digital signature scheme. For the authentication purposes an electronic message has signed with digital signature by sender before sending to intended recipient. Thus the authenticities of the message and sender will be provided by the digital signature scheme. A digital signature is an asymmetric cryptographic scheme through which an extra piece of information is attached with the message to detect illegal modifications and also authenticate the identity of the entity who signed the massage. Digital signature algorithm is used for E-mail, transmission of electronic funds, interchange of data, distribution of

software, storage of data, and all other application that required the assurance of data integrity and signatory's authentication. Digital signature's security depends upon the message and on the private key of the signer. Digital signature generated by using one way mathematical hash functionand private key of the singer for both stored as well as transmitted data.

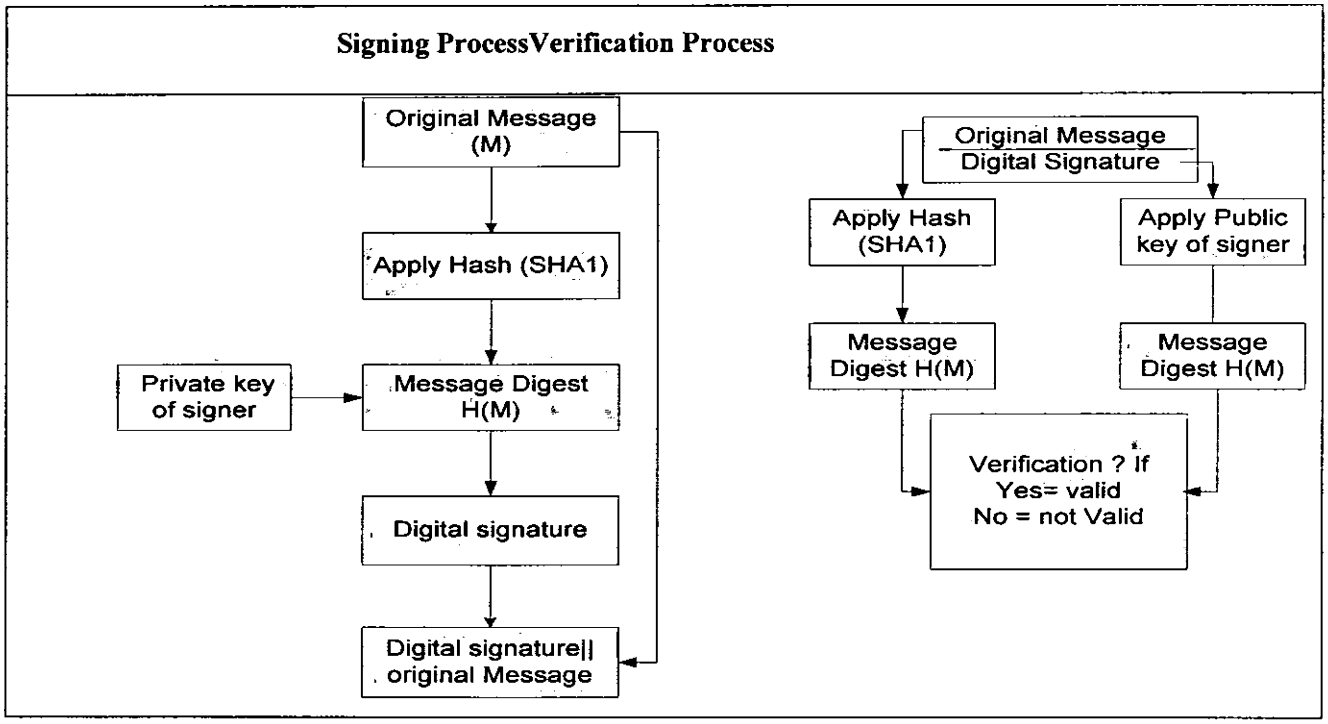


Figure 1.2: Summery of Digital Signature

A digital signature consists on the signature generation and verification algorithms. Private Key of the signer is used for signing and Public key of the signatory is used to verify the signature by the recipient. Comparing with the physical signature, digital signature has the capability that, it cannot be changed nor copied by someone else, and also the signers of the signature cannot repudiate his signature later. These properties of integrity and authenticity of the message ensure

the non-repudiation of the signature for example the signer cannot deny signature of the message in future. The process of Digital Signature generation and verification is shown in figure 1.2.

1.5.1 Types of Digital Signature

There are two main types of Digital signature scheme are used.

1.5.1.1 Direct Digital Signature Scheme

Sometime signed message is sensitive to the receiver, like signature on tax information, personal and business transactions are such type of situations in which a user A signed a message and send to user B for whom it is sensitive and also concerns to remaining users. For this purpose Direct Digital signature scheme is used in which only B can directly verify the signature and also prove the signature validity to any other users. In this scheme the receiver B has full control over the verification process of signature. In Direct Digital SignatureScheme the public key of the receiver is used to encrypt the entire message or the hash digested message by sender to sign a message. The receiver's private key is used to ensure the confidentiality of the encrypted message and signature [18].

1.5.1.2Arbitrated Digital Signature Scheme

In this scheme the signed message firstly send to a trusted third party called arbiter to check the authenticity and integrity of that message. After complete verification it is forwarded to intended receiver.

Signature Generation Process

The signature generation process used one-way hash function to obtain message digest which is used as input for the digital signature. Private Key must be kept secret and is used to generate the

signature by the intended signatory. The digital signatures are designed in such a way that they cannot be forgeable.

Signature Verification Process

Digital signature can be verified by using the public key of the claimed signatory and same hash function that was used in the signature generation process. Public key has required nosecrecy but must be maintains its integrity. Digital signature also used other information like secret random number per-message. The recipients of a signed message used digital signature for the verification of claimed signatory of the message to any third party.

1.6 Classes of Digital Signature Scheme

Digital signatures are divided in two main classes, signature with appendix and message recovery.

1.6.1 Digital Signature with Appendix

In this scheme the original message is required as input for the verification algorithm and depend on the cryptographic hash function. Digital Signatures with appendix are applied to messages having arbitrary lengths. The following are the examples of Digital signatures with appendix.

1.6.1.1 El-Gamal Digital Signature Scheme

ElGamal Digital Signature Scheme is a signature with appendix requires a hash function having $h : \{0,1\}^* \rightarrow Zp$,where each user selects a large prime modulus p, a number g the generator of $Zp^*$and a one-way collision free hash function h.

ElGamal Digital Signature scheme also selectsprivate keyx_A , where$1 \leq x_A \leq p-2$ and public key$y_A = g^{x_A} \bmod p$.

Signature Process of Message m by user A

User A selects the following parameters for signing of message m having arbitrary length.

Random secret integer k, r and $s$where

- $k, 1 \leq k \leq p-2$,With$(k, p-1) = 1$
- $r = g^k \bmod p$ And$k^{-1} \bmod p-1$
- $s = k^{-1}\{h(m) - x_A.r\} \bmod p-1$
- $signature = (r, s, m)$

Verification Process of Signature(r, s, m), by any user B

- Verifies the component r, if $1 \leq r \leq p-1$, then accept otherwise reject the signature
- Verifies the component $v1 = y_A{}^r.r^s \bmod p$
- Verifies $h(m)$ and $v_2 = g^{h(m)} \bmod p$
- Signature will be accepted if $v1 = v2$

1.6.1.2 Digital Signature Algorithm

The Digital signature Algorithm is a Digital signature scheme with appendix. DSArequired the following parameters.

Parameters

- Prime modulus p having L bits length where $512 \leq L \leq 1024$, L is the multiple of 64.
- Prime devisor q of $p-1$ having length of 160 bits.

- $g = \alpha^{(p-1)/q} \, mod \, p$ Where$\alpha \in Zp^*$ and g is in the order of q in Zp^*.
- An Integer x_A where $0 < x_A < q$.

Signature process

- $y_A = g^{x_A} mod \, p$.
- h= one way hash function
- Public parameters are p, q, h, g.
- y_A is user public key and x_A is user private key
- Compute k^{-1}mod q by selecting random number k
- $r = (g^k mod \, p) \, mod \, q$.
- $s = k^{-1}\{h(m) + x_A.r\} \, mod \, q$

The (r, s) pair is the signature of the user A for the message m. New value k will be generated for each time when new signature is generated.

Verification Process

- The signature will be accepted if, $1 \leq r \leq p - 1$ and $1 \leq s \leq p - 1$ otherwise rejected.
- Computes $w = s^{-1} \, modpandh \, (m)$
- Computes $u1 = w.h \, (m) \, mod \, q$ and $u2 = r \, . w \, mod \, q$.
- Computes $v = g^{u1} {y_A}^{u2}$ mod q
- The signature will be accepted if v = r.

1.6.1.3 Feige–Fiat–Shamir Signature Scheme

This is digital signature scheme with appendix. One-way hash function h is required for fixed integer k. In this scheme all users having same modulus $n = p.q$ and a key distribution center is used to generate the p, q and also private and public keys for each users.

1.6.2 Digital Signature with message recovery

In this scheme the message can be obtained from the signature and these are useful for short length messages and there is no need to know about the original message in advance for verification algorithm. Digital signature schemes with message recovery are mostly applied to fixed length messages and can be converted to Digital signature scheme with appendix by taking cryptographic hash function and then signing the hash value.

1.6.2.1 The RSA Signature Scheme

The first digital signature with message recovery is the RSA digital signature scheme which is most applied and adaptable technique. All the spaces of message, signing, cipher-text and signature are belonging to $Zn = \{0,1,2,\ldots.n-1\}$ where n is the product of two prime numbers p and q [21].

Signature process

- Any user A compute Cypher text of the message $m^* = h(m)$
- By applying his private key, user A computes$S^* = (m^*)e \bmod n$ whereS^*, is the signature for message m.

Verification Process

- Any recipient B apply the public key e of the sender A and compute $m^* = (s^*)^e \bmod n$.

- Verify that m^* belong to $h(m)$ if yes accept, otherwise reject the signature.
- And recover the message from $h(m)$.

1.6.2.2 Nyberg- Rueppel Digital Signature Scheme

This is also the digital signature scheme with message recovery technique. The space of key generation and signing is $Ms = Zp$, where $p$and q are prime numbers and s is the signature space $S = zp \times zq$.

Signature Process

- Any user A compute $m^* = h(m)$.
- Select a random secret integer k $\in zq$ and compute $r = g^{-k} \bmod p$.
- Compute $e = m^* r \bmod p$ and $s = e.xA + k \bmod q$.
- The signature of the user A will be the pair (e, s).

Verification Process

- Any user B, verify that $e \in zp^*$ and $s \in zp^*$ if yes accept otherwise reject the signature.
- Compute $v = g^s y_A{}^{-e} \bmod p$ and $m^* = v.e \bmod p$.
- Verify that $m^* \in M_h$ if yes then accept otherwise reject the signature.
- Message m will be recovered from $m^*$by computing $h^{-1}(m^*)$.

1.7 Digital Signature Schemes with additional functionalities

Some situations required additional functionalities which is not possible to achieve by implementing the basic digital signature scheme. For this purpose the basic RSA and El-Gamal digital signatures schemes are combined with a specific protocol to achieve the supplementary

features. Some distinguished digital signatures with additional and specific functionalities are described below.

1.7.1 Multi-Signature Scheme

When a digital signature required more than one key for signing a same message is called multi-signature scheme. This type of signature scheme is used in some commercial organizations where a document is required to sign by more than one person in a collaborative and simultaneous manner. For example when a company issued cheque, it required the signature of more than one authorized persons [19, 20].

1.7.2 Group Signature Scheme

In group signature scheme every member of some specific group has the authority to sign the required document on the behalf of that group. The receiver of the signature can verify the validity of the group signature but cannot identify the member of the group who signed the message. A trusted designated entity identifies the signer of the message in case of any disputes [22,23].

1.7.3 Threshold Signature Scheme

In some situation decision has taken by a group of members on the behalf of an organization, for example a large bank transaction which required signatures from more than one member. A separate digital signature is used for every signer to solve such type of problems but this policy make the verification process very difficult for recipient of the digital signature. Threshold digital signature is the alternative method used to share a secret key among a group of people in such a way that a certain number of people can work collectively to recover the secret. This type

of key distribution scheme is used to protect bogus fellow of the group and unintentional disclosure of secret [24, 25].

1.7.4 Undeniable Signature Scheme

Undeniable signature is a number issued by a signer which depends on the message. In this scheme the signature can only be verified with the help of a signer and protect the distribution of the signature without the knowledge of the signer. The main problem of this scheme is that, a dishonest signer may refuse to authenticate a genuine document.For the solution of this problem a new component called disavowal protocol is added with the other normal components of signature and verification. Undeniable signature scheme is implemented using public-key cryptography based hard mathematical discrete logarithm problem (DLP) [26, 27].

1.7.5 Blind signature scheme

This is a two-party protocol between the sender A and the signer B. In this scheme the sender A send a message to signer B for signing. Signer B signs that message and return to A. Now user A is capable to compute the B's signature on a message m of his choice. After the completion of this process B not capable to know the message m or the signature associated with it. So blind signature is used to prevent the signer B from seeing the message it sings and the signature.

Blind signature used in situation like online bank transactions, where the customer A does not want the bank B to be capable of associating a signature and message with a certain instance of the protocol [28, 29].

1.7.6 Proxy signature scheme

Proxy signature is used in situation where the head of the organization is absent due to some reasons, and he delegates the authority of signature to his deputy to sign on the behalf of the organization. In these techniques the private key of the head cannot provide directly to the deputy due to the digital signature security policy but delegate the signing capability without knowing the private key in such a way that the receiver can validate the signature of the head of the organization with the help of proxy signer [30, 31].

1.7.7 Shortened Digital Signature Scheme

The traditional Digital signatures are not suitable for situation of small storage size, low-bandwidth communication, and less computational capability. A SDSS is used to provide authentication and integrity for these small and less computational capability devices.SDSS is important when signature is printing on postage stamp, bank bill or commerce invoice andalso desirable where signatures are entering manually. The signature is shorter and there is no need to do inversion in verification. SDSS is used to provide the authenticity for small size, limited battery timing and less computationalcapabilitiesdevices like cell phone, wireless nodes and RFID chips[5].

Already some trusted short signature schemes based on DLP and IFPhas been developed. Short signature scheme having short signature length while provides same security as provided by DSA. This reduction of signature size is very important for small size and limited computational capable devices because it saved the power and also increased the life of the battery [15].

1.8 Hash Functions

RSA and El-Gamal signature schemes have the problem that the length of the signaturesbecomes same or may be largefrom the messages that aresigned by the signer. Cryptographic hash functions are used to overcome this problem. Hash function is used to produce message digest of fixed length from message m of arbitrary length. Hash should be calculated for the whole message. Hash function is assumed to be public and not keyed. The hash value length should be proposed in the range of 128-bits to 512-bits to resist birthday attacks.The calculation of Hash function should be very fast, one way and strongly collision free. One way hash means that it is infeasible to obtain the message (m) back from the message digest h(m). Infeasible means that it would take millions of years to get the message by intruders [38] and by Collision free means that it should be computationally impractical that the hash of two messages willbe same. For this purpose Revest proposed an MD4 hash function and later on another strengthened version MD5 having message digest length 128-bit size for arbitrary message are presented.

In 1994 federal governed presented Secure Hash Standard of SHA1 which is used to produce 160-bits of message digest. Hash function is very fast but there is no verification available that it is collision free and computationally one way function. It is complicated and analysis is difficult but in practice it work very well.

Message digest will be public and signature algorithm is applied to the message digest obtained from hash function and then the combination of message digest and signature are sending. The verification process is applied to the signed digested message and compared with message digest that is obtained from the message. The signature that is produced by using hash function will be

very shorter and capable to prevent forgery attack. MD5 is not suitable for digital signature and for Secure Sockets Layer certificates, because it has no collision resistant.SHA1 is suitable for light weight devices and produced 160-bits message digest for a given message.

1.8.1 Why we need hash functions?

Hash functions are used because public-key signature algorithms are very slow if we sign the whole message. Therefore the signing of the resulting Hash Digested value of a message is much more efficient than signing the whole message. Secondly the signing of whole message without hashing result a many times large size of a signature for that message. And if signature has applied to the hash value of a message than only small overhead like 320 bits in case of the DSS would be added.Thirdly due to the collision free property of a hash function, any change in a message will result in a different hash value, and signature verification will be failed [40].

1.8.2 The Secure Hash Algorithm

NIST used SHA-1 for DSS which is having 160 bits fixed length for any message less 2^{64} bits. It originally based on Ron Rivest Message Digest MD4. Ron Rivest also enhanced MD4 message digest to MD5 algorithm. According [38] there is no cryptographic attack exists against Secure Hash Algorithms.

CHPATAR 2

LITERATURE REVIEW

2. Literature Review

The literature survey consists on existing Digital Signature and Shortened Digital Signature based on these three hard mathematical problems like DLP, CDLP, and IFP.

2.1 Key Distribution Scheme Based on DLP

Hellman[1] proposed a key distribution scheme on the basis ofDLP in which each participant has its own secrete key. Each key consist on public and private key part called key pair also. He had first time presented the idea of public key cryptosystem on the basis of DLP. It allows participants to exchange private keys over an insecure channel without prior sharing of secret information. This scheme is limited only to the exchange of keys and no practical cryptosystem has presented. Due to no authentication for the participants, Man-in-the-middle attack is possible in this scheme.

2.2 First Public Key Cryptosystem Based on IFP

Rivest et al [2] Proposed firstpractical public key cryptosystem schemewhich is based onthe difficulty of factoring large numbers. It provides authentic encryption scheme without the needs of Private Keyexchange separately. In this scheme the encryption key of intended recipient is publically known to every one and only that recipient decrypt the message by its private key. Minimum key length is 1024 bits.Security breaking is challenging and difficult as factorization of n. Author used Richard Schroeppel's methodfor 200 digits, so 1.2×1023 number of operations is required and if each operation having one microsecond then 3.8×109 years are required for factorization.The limitations of this scheme is that, p and q values must be enough

large that direct guessing is impossible, the value of $p$and q are recommended to be prime numbers. No proper Digital signature scheme has been designed.

2.3 First Digital Signature based on DLP

El-Gamal [3] proposed first DSA scheme based on the difficulty of computation of DLP over finite field. He used same public key for encryption of message and for signature verification. He has developed signing and verifying procedures of proposed signature scheme. Its security breaking is difficult like solving the DLP. Proposed scheme security will be non-breakable if large prime numbers and strong exponents are used. Random encryption exponent $k$must be different for each message.The limitation of this scheme is that, it doubled the size of the transferred message and the security may be compromised if random encryption exponent $k$is repeated.

2.4 Shortened Digital Signature Based on IFP

Moldovyan [4] proposed a short digital signature scheme based on the difficulty of factorization of a composite number which is the product of two large prime numbers. New improved digital signature schemes having small size are developed. This signature scheme provides security of minimum security level group operations estimated as 2^{80} which is requiredto forge a digital signature.Due to choosing of large prime numbers attack on this scheme is computationally infeasible.Limitation of this scheme is that if we use prime numbers smaller than 1024 then the security has compromised.

2.5 Shortened Digital Signature Algorithm based on DLP

Z. Shao [5] proposed a short signature scheme on the basis of DLP which provides better security then existing signatures and has one forth reduction in the length of signature and in the computation of verification to original DSA. Its security breaking is difficult like the difficulty of discrete logarithms problems. Pairing is not used in this scheme due to which efficiency is high and implementation is easy. This scheme is secure in the random oracle model from signature copying by adaptive chosen-message attack. The proposed scheme will have signature length of 240 bits if 160 bits key length and SHA-1 or SHA-512 hash functions are used. If small sizes of prime numbers are used then the security of the scheme has compromised.

2.6 Digital Signature Based on the Hybrid of DLP and IFP

Ismail et al [6] proposed a new digital signature based on the hybrid of two hard problems namely DLP and IFP. In which two secret keys are used for signing and two public keys for verification. This scheme has less than $1203\,T_{mul} + T_h$ time complexity for both signaturegeneration and signature verification. As compare to other signature scheme based on single hard problem, this signature scheme is more secure because no intruder can solve two hard problems simultaneously. It has less than $5T_{exp} + 3T_{mul} + T_h$ computational complexity both for signing and verification. The communication cost of this scheme is 3|n| + 4|P|. It has less number of operations for signing and verification.

2.7 Short Signature scheme based on IFP

Moldovyan [7], Proposed a short signature scheme based on the difficulty of IFP. This scheme consists on a pair of two numbers which provide same security like RSA and the length is

reduced to 320-bits. This scheme provides complete security if the order number valued is greater than 160 and the length of prime numbers which is used to generate n to be chosen very large. If prime numbers having values less than 160 bits then security may be compromised.

2.8 Blind Signature Scheme based on IFP and DLP

Tahat et al [8] proposed a new blind signature scheme based on both IFP and DLP. It has less computational complexity for signatures and who demand the signature. This scheme is secure than the signatures scheme based on single hard problems. In this paper some possible attacks are also defined and the security of the proposed scheme has proved. This scheme has high computational overhead as compared to single hard problem.

2.9Cryptosystem based on Complex Discrete Logarithm Problem

Sagheer et al [9] uses complex numbers to present existing public key cryptosystem with hard mathematical problem known as CDLP. His scheme has shorter key length due to which the overall calculation is easy than schemes based on DLP. As comparing to DLP, The CDLP using of complex numbers whichprovides double securityfor very smaller bit size of the key. The proposed scheme is applied for Diffie-Hellman Key exchange, El-Gamal, Massey-Omura public-key cryptosystems and proved that the security based on CDLP is strong then based on DLP. Repeated squaring and multiplication algorithms are used to compute complex numbers exponentiation in the complex field group. If we calculated value of the CDLPis q-bit then it requiredsquare times operation to solve it.Operation complexity of CDLP is immediately increased with the increases of size as compared with DLP. Hence due to these reason the CDLP base cryptosystem is more secure than DLP.

2.10 Digital Signature based on applying hash round function before signing

Chen et al [10] proposed a new digital signature scheme in which hash round function is applied before the signature. To overcome the active attacks author used a new digital signature scheme Hash Round Function and Self-Certified Public Key System Digital Signature Algorithm. H-S DSA is similar as ELGamal digital signature algorithm in the format and it is more secure and having less time complexity. Its security depends on one-way hash function, discrete logarithm problem and integer factorization problem. H-S DSA has presented in four steps like initialization, user registration, signing and verification of signature. Author conducts performance analysis and proved that this scheme has batter security and also secure from all type of password attacks.

2.11 Digital Signature Based on Bitwise and Multiply Hash Function

Noorouzil et al [11] used a new digital signature, which is better for such applications which using small size file for sending and want simple and fast algorithm for generating digital signature. A new method of bitwise and multiply function are used for hashing. This hash functions generate smaller and dynamic size of bits which depends on each bytes (size) of the message. If original file is changed then the hashed file will also be changed. This scheme is limited to applications which have transferred smaller size of files.

2.12 Digital Signature Based on IFP and DLP

Verma et al [12] proposed a digital signature scheme on the bases of two hard mathematical problems, IFP and DLP. He analyzes the security of the proposed scheme for different attacks and proved that the proposed scheme is more secure than the previous schemes. Because

calculating two hard problem is not easy to break security. The limitation of this scheme is double communication and computation overhead because of two hard problems.

2.13Overcome Security Weaknesses of El-Gamal Digital Signature

Zhang et al [13] address the security weakness of the El-Gamal Digital signature [1] that the repeated usage of random number makes the possibility of security breaking, and proposed an improved El-Gamal digital signature scheme with the pairs of private keys (x, d). For this scheme there is no need to remember the value of k so the overall computational operation of comparisons and storage space is minimized. El-Gamal digital signature is improved by the introduction of a random number t with the signature and applying modular inversion. This scheme is secure from forgery attack. Limitation is increase in length of signature due to addition of the value of t with the signature.

2.14 Digital Signature based on DLP and Biometric string input

Parida [14] proposed a short signature scheme based on DLP and Biometric String. It takes DLP and biometric string as input.It reduces the length as well as the computation of the verification algorithm while the level of the security is remaining the same. It is more secure because the private key not determined due to discrete logarithm problem. Due to less verification cost it is easily apply in the real life applications like e-commerce and e-voting etc. This scheme provides security for the use of random number and increased the life cycle of a private key. It minimizes the overall operation and save the storage space because of auto random number k.it is secure from forgery and plaintext attack. Extra computation devices for biometric data analysis and calculation are the limitations of the scheme.

2.15 New Digital Signature based on DLP with designated verifier

HAN-YU [15] proposed a new digital signature scheme based on discrete logarithm problem. In this scheme the signature is not verified without the designated verifier, only designated verifier apply his private key and find out the verification. Any third person or signer by self also is not able to verify the signature. It is efficient and short signature scheme. It has low computation cost. Its security is proved in the random oracle model.

CHAPTER 3

PROBLEM ANALYSIS

3.1 Hard Mathematical Cryptographic Schemes

Digital signatures are based on the difficulty of some hard mathematical problems like DLP [32, 33] and IFP [34, 35] or on the combination of these two problems [36, 37]. The security breaking of these Digital signatures based on hard problems is as difficult as breaking of discrete logarithm or integer factorization of large prime numbers is difficult. These hard mathematical problems are discussed as following.

3.1.1Discrete Logarithm Problem

This is hard mathematical problem used to design Digital Signature, because the breaking of such hard problems is very difficult and more operations required for solution if we used numbers in the range of 100 to 200 digits. The ordinary Algorithm $log_a^{(b)}$ is the solution for the equation $a^x = b$, similarly if g and h are two elements of cyclic group G then solution of x in the equation $g^x = h$ is called DLP. A group of G with an operation "*" is defined on pairs of elements of G. The operation will satisfy the following basic properties.

1. Closure Property: $a * b \in G \quad for\ all\ a, b \in G.$

2. Associative Property: $a * (b * c) = (a * b) * c \in G \quad for\ all\ a, b, c \in G.$

3. Multiplicative Identity: There are exists an element $I \in G$ called Identity such that $I * a = a * I = a\ for\ all\ a \in G.$

4. Multiplicative Inverse: For $a \in G$ there is an element $b \in G$ such that, $a * b = b * a = e$ thus the element b is called the inverse of a.

Consider the equation $y = x^a$ where x and y are two real numbers and a is an integer then y will be easily calculated if x and a are known, but when the values are largeit is very hard to determine the value of a from the known values of x and y. DSA, Diffie-Hellman and El-Gamal are based on discrete problem [32].

3.1.2Integer Factorization Problem

This is another hard mathematical problem used to design the DSA and SDSA. This is based on factorization of two large prime numbers. Consider the equation $n = p * q$ where p and q are two large prime numbers. So the calculation of n is easy if $p\ and\ q$ are known but the factorization of n back into p and q is a hard problem when the values of $p\ and\ q$ are large. It is called IFP [35]. One of the famous Algorithms based on Integer Factorization problem is RSA algorithm. RSA Algorithm security depends on the difficulty of factorization of two large prime numbers. In literature different researchers has used DLP or IFP and some are used the hybrid of these two problems to design DSA and SDSA [37].

3.1.3 El-Gamal Digital Signature Scheme

[3] ElGamal first time in 1985 proposed a Signature scheme known as El-Gamal Digital Signature which is nondeterministic signature because it is use a random number k,therefor this signature is used only for signing not for encryption. El-Gamal Signature scheme is the basis for DSA, and its security is based on DLP.[41]Describe the following public parameters p, g, y and private key x. $p$is prime number chosen from a finite field and g is a generator $mod\ p$,x is a private key less than p and y is public key where $y = g^x\ mod\ p$. These parameters will be same throughout the program.If Alice wants to sign the message m, a random number k will be

picked by her, which is relatively prime to $p - 1$. And compute $r = g \bmod p$ and $s = (m - xr)k \bmod (p - 1)$.So the required signature $S = (s, r)$ along with message will send to Bob in order to verify the signature. Bob using r, s and public parameters and compute $y^r r^s = g^m \bmod p$ to verify the signature.

3.1.4 Digital Signature Standard

The DSA was first time proposed in 1991 and belonging to DSS designed by National Institute ofStandards and Technology's. The DSA is used to show the authentication of signatory and integrity of the signed data.The DSA is the modified form of the ElGamal scheme and these modifications are discussed as following. The security of ElGamal scheme is based on DLP and using a very large modulus p must be at least 512bits, but for future guarantee of the security the length of p should be 1024 bits. ElGamal variant DSS using one way hash function which is used to convert the message variant length to fixed length of 160-bit. The modification of ElGamal scheme consist of flipping the "– " sign to "+" sing during the generation of S part of the signature like $s = (m + xr)\, k^{-1} \bmod (p - 1)$ and verification condition changes like $g^{ms^{-1}} y^{rs^{-1}} = r \bmod p$. In DSA signature scheme Alice select a random or pseudorandom number k where $k < q$, and compute $S = (r, s)$ where

$$r = (g^k \bmod p) \bmod q$$

$$s = (k^{-1}(m + xr)) \bmod q$$

And then Alice sends the message along with Signature $S = (r, s)$ to Bob. On receiving the message along with signature, Bob is verifying it for integrity as well as authentication as following.

$$w = (s)^{-1} \bmod q$$

$$u1 = (Hash(m) * w) \bmod q$$

$$u2 = (r) * w \bmod q$$

An then verify that that $r' = ((g^{u1} * y^{u2} \bmod p) \bmod q)$

Now the Bob check that if $r = r'$ then the signature will be valid if $r \neq r'$ then the signature will be modified by someone and the message will be rejected.

3.1.5Mathematical Solution

By computing a small example, we will prove the DSA.

The following parameters are supposed.

Let $q = 11$

$p = 38q + 1 = 3839$, Where q is prime divisor $p - 1$.

$g = 5^{38} \bmod 3839 = 2688$

Suppose Alice select a private key $x = 17$

Hence it public key will be

$y = g^x \bmod 3839 = 2688^{17} \bmod 3839 = 1347$

Alice wants to sign the message $M = 12$, she chooses a random number $k = 25$ and findsthe inverse to be$k^{-1} \bmod 101 = 97$. She then calculates (r, s).

$r = (2688^{37} \bmod 3839) \bmod 101 = 2601 \bmod 101 = 76$

$s = (12 + 17 * 76)\, 97 \bmod 101 = 36$

Alice then sends the triple $(48, 44, 73)$ on to Bob, who performs the following

Computations to verify the signature:

$$w = 36^{-1} \, mod \, 101$$

$$e1 = 12 * 56 \, mod \, 101 = 66$$

$$e2 = 76 * 56 \, mod \, 101 = 14$$

$$r' = ((2688^{66}1347^{14}) mod \, 3839) \, mod \, 101 = 1692 \, mod \, 101 = 76$$

Thus, Bob has compared r with r' and then verifies that the signature came from Alice is authentic or not.

3.2Problem Statement

Traditional Digital Signature Algorithm based on Discrete Logarithm Problem and Integer Factorization Problem having many applications in network security but not suitable for devices having small memory size, limited battery power, low-bandwidth and less computational capability. These Digital signaturesbased on DLP and IFP using larger bits size (512-1024 bits) of computation and communication needs higher energy consumptions for the desired security and privacy for small devices. It follows that the computation and communication complexity of these devices should be as lower as possible and the security can be achieved in a desired level.

Existing Digital Signature Algorithmbased on real number public key cryptosystem producedhigh communication overheadi.e 832 bits per Message,such as(P=512, q=160, h(m)= 160).This cause more memory overheads and having more computational complexity when large numbers are provided.

3.3 Problem scenarios

Existing DSAhaving two different problem scenarios. These problem scenarios are discussed according to the communication overhead and time complexity during signature and verification process. DSA based on the difficulty of DLP consists of three different types of public parameters p, q, g.These parameters will be known to a group of users. A p will be selected as from the range of $512\ to\ 1024$ bit and q is 160 bits such that $q$will divide $p-1$. The parameter g will be selected from $h^{(p-1)/q}\ mod\ p$ where h is between $1\ and\ p-1$, and g must be greater than 1. In the presence of p, q, g user select his private key x randomly and compute his public key y, the hash of the message will be selected and random number k per message will be created. To create Digital signature a user calculate r and s called components of digital signature.

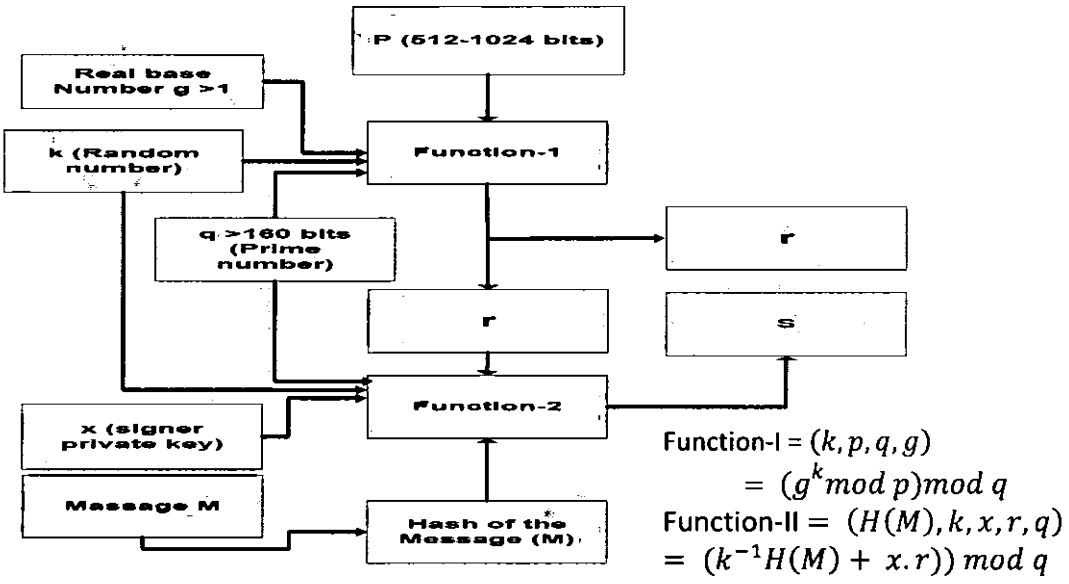


Figure 3.1: Digital Signature Signing Scenario

The problem of the existing DSA is high communication and computation overhead. Because size of p *is* 512 bits and q *is* 160 bits. And the value of base number g will bein the range of 512bits and must be greater than 1. So every message will carry more than 1185 extra bits as digital signature. If we suppose to select small numbers than the DLP will be compromised and the value of private key has easily determined by intruders. If we select large numbers than extra overhead per message will be created.

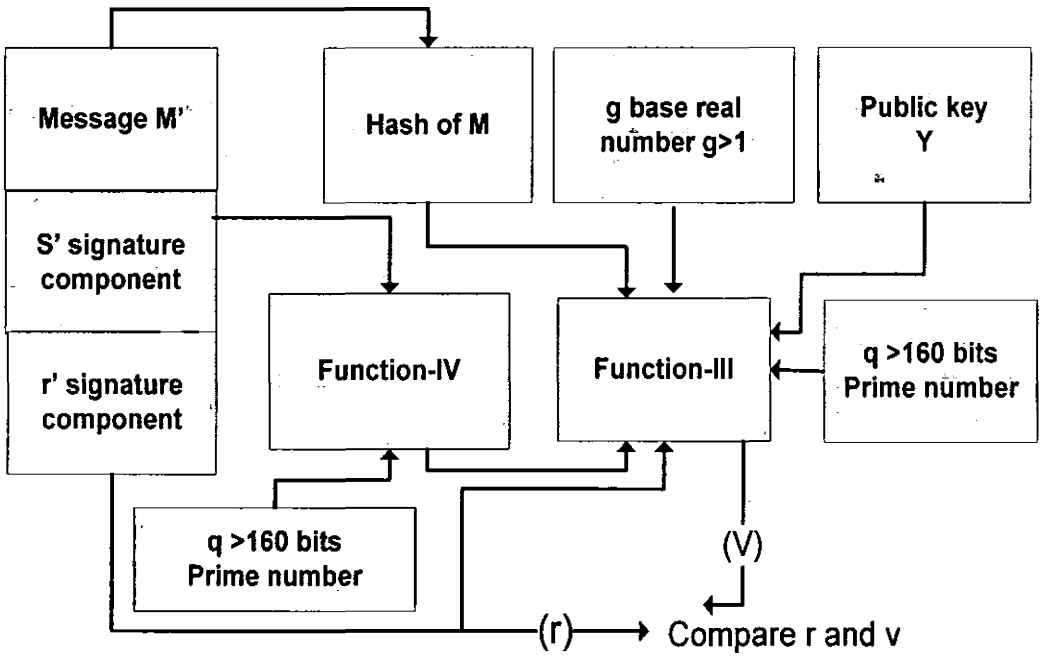


Figure 3.2: Digital Signature Verification Scenario

$$W = \text{function IV } (s', q)$$

$$= (s')^{-1} \bmod q$$

$$V = \text{function-III } (y, q, g, H(M'), w, r')$$

$$= ((g^{(H(M')w), \bmod q} \, y^{r'w \bmod q}) \bmod p) \bmod q$$

This verification scenario usedlarge size of parametersi.e$p \geq 512\ bits$, $q = 160\ bits$and alsousing public key of the sender to verify the signature.

CHAPTER 4

PROPOSED SOLUTION

4.1Proposed Solution

We have proposed Shortened Digital Signature Algorithmswith a new method based on complex number called Shortened Complex Digital Signature Algorithms. These Algorithmsreduces the memory overhead, time complexity, computation and communication overhead comparing with DSA.Complex numbers and hash function used in this scheme are discussed as following.

4.1.1 Complex Number

This thesis has focused on designing and implementation of Shortened Complex Digital Signature Algorithms based on CDLP. This scheme has less communication overhead $(q = 512\ bits, r = 160\ bits)$ per message; approximately reduction is (56%) such as 864 $bits$ per message. Therefore this scheme will provide more security for very smaller bit size as compare to previous signatures schemes based on DLP, IFP. It means that large numbers for example more than $512 - bits$ will be provided for the required parameters to get adequate security by using DLP and IFP. This same security will be acquired by using complex numbers smaller than 512 $bits$.

Complex public key cryptosystem is using Complex numbers instead of real numbers as mathematical hard problems. A Complex number is $C = a + bi$where "a" part is real number and "bi"is an Imaginary part. An imaginary part consist on $i$where$i = \sqrt{-1}$.We have proposed a new shortened digital signature based on complex number instead of real numbers, which is more secure and no intruder can solve it. The use of CDLP for designing of Digital Signatures will be more secure than DLP and IFP's based Digital Signatures.

4.1.2 Secure Hash Algorithm

This algorithm also using one way hash function SHA1,to fixed the size of the one part of Digital Signature"r"to 160 $bits$. Now the length of the signature will be equal to$|hash\ (M)| + |q|$.

4.2Notation Guide of Scheme (SCDSA)

- n:It isa large prime number of bit length, between512 and 1024.
- q:Is a large prime factor of $n\ -1$.
- g: Complex number with large order n.
- k: is a random number per message selected from (0, 1,2,..... n – 1)
- Hash: a one-way hash function
- va: Alice private key, chosen uniformly at random from $[0, 1, 2 \ldots\ n - 1]$
- P_a: Alice's public key $P_a = g^{va}\ mod\ n$
- vb: Bob private key, chosen uniformly at random from $[0, 1, 2 \ldots\ n - 1]$
- P_b: Alice's public key $P_b = g^{vb} mod\ n$

Digital signature consists on a string of bits computed by some rules and set of parameters that are used to identify the signatory and integrity of the message to be verified. SCDSAused public integer (n, g, r)as parameters which is known to a common group of users. The value of n must be enough large that the discrete log will not be easily calculated.The "va"is a private key of the signer used to sign a given message, and corresponding public key is used for signature verification. A random number k which unique to every message is used for the generation of the signature, where greatest common devisor (GCD) of $(k, n\ -\ 1)$ is equal to "1" and "k" must be secretly chosen by signer. The required signature will be $\boldsymbol{S} = (\boldsymbol{r}, \boldsymbol{s})$and

signature length will be |hash (M)| + |q|. Following are different Algorithms used to compute digital signatures on a given message.

4.3.1 SCDSA1 (Signature Process) on a message m

1. **Random number k gernerate**
2. $\mathbf{r = hash\left((g^k \bmod n) \parallel m\right)}$
3. $\mathbf{s = k/(r + va) \bmod q}$

Signature $= (r, s)$

Signature length: $|hash\,(.)| + |q|$

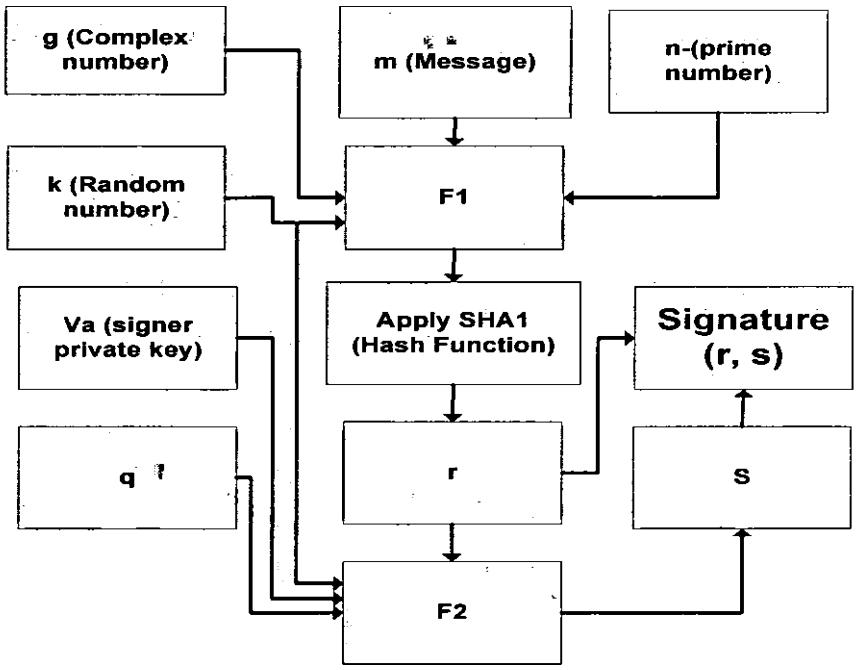


Figure 4.1: Proposed Signing Scenario

(i) F1= g^k ‖ m(ii) F2 = k /(r + va) mod q

In the above Shortened Complex Digital signature Algorithm the required parameters are defined firstly and then generated random number k,then base number g is selected from the finite field and computed $g^k$by using random number k. Required Message has concatenated withg^k and passing through hash function SHA-1 to fixed its length to 160 $bits$, and it is called the r part of digital signature. Similarly the s part of digital signature is generated in F2 by using $r, n, va,$ and k. Now the Shortened Complex Digital Signature $S = (r, s)$ is generated for a message m.

SCDSA1 (Verification Process):

1. $\mathbf{g^k = (Pa * g^r)^s \ mod \ n}$
2. $\mathbf{r' = hash\ (g^k \parallel m)}$
3. **Check**

$\mathbf{r' = r}$

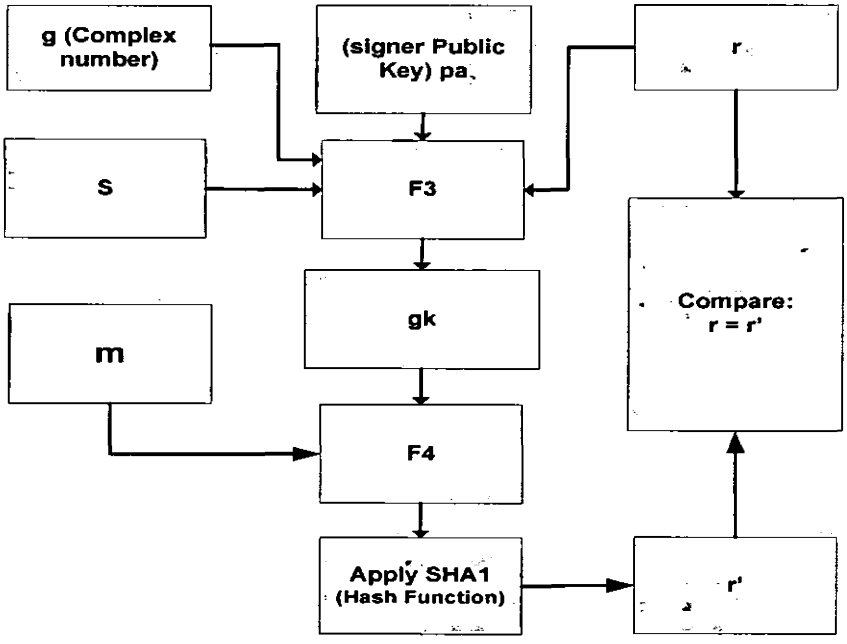


Figure 4.2: Proposed Digital Signature Verification Scenario

(i) $F3=(Pa * g^r)^s$ (ii) $F4=g^k \parallel m$

In the verification process the public key of sender pa, complex base number g, modulus n and signature (r, s) parts are used to calculate g^k. Message m is concatenated with g^k and Hash function is applied to it to get r'. Now r compared r withr' if they are same then signature will be valid otherwise it will be compromised in the middle.

Correctness Proof:

$$(Pa * g^r)^s$$

$$=(Pa * g^r)^{k/(r+va)}$$

$$=(g^{va} * g^r)^{k/(r+va)}$$

$$=(g^{va+r})^{k/(r+va)}$$

$$=g^{k(va+r)/(r+va)}$$

$$=g^k$$

4.3.2SCDSA2: Signature (r, s)Process on a message

1. **Random number k generate**
2. $r = hash((g^k \bmod n) \parallel m)$
3. $s = k/(1 + va.r) \bmod q$

Signature = (r, s)

Signature length: $|hash(.)| + |q|$

Verification Process of (SCDSA2) scheme

1. $g^k = (g * Pa^r)^s \bmod n$
2. $r' = \text{hash}(g^k \parallel m)$
3. **Check**

$$r' = r$$

Correctness Proof:

$$=(g * Pa^r)^s$$

$$=(g * g^{va.r})^s \qquad \therefore pa = g^{va}$$

$$=(g * g^{va.r})^{k/(1+va.r)} \qquad \therefore s = k/(1 + va.r)$$

$$=(g^{va.r+1})^{k/(1+va.r)}$$

$$=g^k$$

4.3.3 SCDSA3 (Signature Process) on a message

1. **Random number k gernerate**
2. $r = \text{hash}((g^k \bmod n) \parallel m)$
3. $s = k/(va - r) \bmod q$

Signature = (r, s)

Signature length: $|hash(.)| + |q|$

4.3.4 SCDSA3 (Verification Process):

1. $g^k = (Pa / g^r)^s \ mod\ n$

2. $r' = hash(g^k \| m)$

3. **Check**

   $r' = r$

Correctness Proof:

$$g^k = (Pa / g^r)^s$$

$$=(Pa * g^{-r})^{k/(va-r)}$$

$$=(g^{va} * g^{-r})^{k/(va-r)}$$

$$=(g^{va} * g^{-r})^{k/(va-r)}$$

$$=(g^{va} * g^{-r})^{k/(va-r)}$$

$$=(g^{va-r})^{k/(va-r)}$$

$$=g^{k(va-r)/(va-r)}$$

$$=g^k$$

4.3.4 SCDSA4: Signature (r, s) Process on a message

1. **Random number k generate**
2. $\mathbf{r = hash\,((g^k \bmod n) \parallel m)}$
3. $\mathbf{s = k/(1 - va.r) \bmod q}$

Signature = (r, s)

Signature length: $|hash(.)| + |q|$

Verification Process of (SCDSA4) scheme

1. $\mathbf{g^k = (g / Pa^r)^s \bmod n}$
2. $\mathbf{r' = hash\,(g^k \parallel m)}$
3. **Check**

$$\mathbf{r' = r}$$

Correctness Proof:

$$=(g / Pa^r)^s$$

$$=(g / g^{va.r})^s \qquad \therefore pa = g^{va}$$

$$=(g * g^{-va.r})^{k/(1-va.r)} \qquad \therefore s = k/(1 - va.r)$$

$$=(g^{1-va.r})^{k/(1-va.r)}$$

$$=g^k$$

4.4 Mathematical Model ofSCDSA1

For the purpose of producing results of proposed SCDSA, we are going to implement our scheme mathematically. And show that the presented scheme is better than existing schemes. We know that the parameters used for digital signatures are consists on very large numbers, which is not easy to calculate by hand. Due to this reason, we are going to select small values for these parameters to calculate and understand it easily. The mathematical implementation is explained by the following example. In this example Alice and Bob choose a finite field Fq and large prime numbers up to 100 or 200 digits. Then publically define a complex number g which belongs to finite field Fq and of order n. On the basis of these parameters Alice chose his Private Key "va" and generate public key "Pa"by using equation, $Pa = g^{Va} \ mod \ n$. Private key will be secrete and only public key will be transferred to Bob. Similarly Bob select his private key "vb" and generate public keyPb $= g^{Vb} \bmod n$. For signature generation "k" is randomly selected from finite field Fn and keeps it secret. Now Digital Signature is generated by Alice as(s,r) . On the other hand Bob will receive the public key Pa, r, and s to verify the digital signature. If the values of $r \ and \ r'$ be same then the message will not be changed, if the $r \ and \ r'$ having different values then the message will be changed by someone else.

4.4.1 Basic Parameters:

Let q beof 10 digits, i.e. q = 1234567899. Then the finite field will be Fq $= \{0, 1, 2, 3, \ldots., 1234567898\}$.

Let n is of 10 digits, i.en = 591558727 and g belong to finite field Fq and of order n.

Consider the complex numbers selected from the above finite field Fq is g $= (11, 12)$

or $g = (11 + 12i)$andfdFn $= \{0, 1, 2, \ldots\ldots\ldots n - 1\}$.

4.4.2 Key generation

Let Alice private key is $Va = 5, g = (11 + 12i), n = 7$ and $q = 3$.

Public key is $Pa = g^{Va} \bmod n$. Put the values.

Hence$Pa = g^{Va} \bmod n = (11 + 12i)^5 \bmod 7$, now solve it by using squaring and multiplying method, in which $va = 5$ is converted to Binary form, i.e$5 = 101$. For first binary bit initialize the value ofg, and for each of the next binary Bit =0, calculate squaring and for Bit =1 calculate squaring and multiplying.

Table 4.1: Squaring and multiplication method for g^5

Binary Representation of va = 5 = 101	Status	Operation
First Binary Bit = 1	Initialization	$g^1 = (11 + 12i)$
Binary Bit =0	Squaring	$g^2 = (11 + 12i)^2$
Binary Bit =1	Squaring and Multiplying	$g^5 = (((11 + 12i)^2)^2(11 + 12i))$

$g^{Va} = g^1 = (11 + 12i)$

$g^2 = (11 + 12i)^2 = (121 + 132i + 132i + 144(-1))$

$= (-23 + 164i)$

$g^4 = (((11 + 12i)^2)^2$

$= (-23 + 164i)^2$

$= (529 - 3772i - 3772i - 26896(-1))$

$= (-26367 - 7544i)$

$g^5 = (((11 + 12i)^2)^2(11 + 12i))$

$= ((-26367 - 7544i)(11 + 12i))$

$= (-199509 - 399388i)$

$Pa = g^{Va} \bmod n = (((11 + 12i)^2)^2(11 + 12i)) \bmod 7$

$= (-199509 - 399388i) \bmod 7$

Public key of Alice $Pa = (-2, -3)$Now calculate the Bob Public key.

Let Bob private key is $vb = 9, n = 7, g = (11,12)$

$$Pb = g^{Vb} \bmod n = (11 + 12i)^9 \bmod 7$$

By using squaring and multiplying method solve the following equation.

Table 4.2: Squaring and multiplication method for g^9

Binary Representation of $va = 9 = 1001$	Status	Operation
First Binary Bit = 1	Initialization	$g^1 = (11 + 12i)$
Binary Bit =0	Squaring	$g^2 = (11 + 12i)^2$
Binary Bit =0	Squaring	$g^4 = (((11 + 12i)^2)^2$
Binary Bit =1	Squaring and Multiplying	$g^9 = ((((11 + 12i)^2)^2)^2(11 + 12i))$

$$Pb = g^{Vb} \bmod n =$$

$$Pb = (11 + 12i)^9 \bmod 7$$

$$g^{vb} = g^1 = (11 + 12i)$$

$$g^2 = (11 + 12i)^2$$

$$= (121 + 132i + 132i + 144(-1))$$

$$= (-23 + 164i)$$

$$g^4 = (((11 + 12i)^2)^2$$

$$= (-23 + 164i)^2$$

$$= (529 - 3772i - 3772i - 26896(-1))$$

$$= (-26367 - 7544i)$$

$$g^8 = (((11 + 12i)^2)^2)^2$$

$$= (-26367 - 7544i)^2$$

$$= (695218689 + 198912648i + 198912648i + 56911936(-1))$$

$$= (638306753 + 397825296i)$$

$$g^9 = ((((11 + 12i)^2)^2)^2(11 + 12i))$$

$$= (638306753 + 397825296i)(11 + 12i)$$

$= (7021374085 + 7659681036i + 4376078256 + 4773903552\,(-1))$

$= (2247470533 + 12035759301i)$

Public key of Bob Pb $= g^9 \bmod 7$

$= ((((11 + 12i)^2)^2)^2(11 + 12i)) \bmod 7$

$= (2247470533 + 12035759301i) \bmod 7$

$= (0, 6)$

Bob Public key is $= (0, 6)$

4.4.3 Signing Process:

k , is randomly selected fromFn. Let k = 4 and message = m.

Now calculate r,

So

$r = \text{hash}(g^k || m)$

By using squaring and multiplying method we calculate $g^k = g^4$.

Table 4.3: Squaring and multiplication method for g^4

Binary Representation of k =4= 100	Status	Operation
First Binary Bit = 1	Initialization	$g^1 = (11 + 12i)$
Binary Bit =0	Squaring	$g^2 = (11 + 12i)^2$
Binary Bit =0	Squaring	$g^4 = (((11 + 12i)^2)^2$

$g^k = (11 + 12)^4$

$g^1 = (11 + 12)$

$g^2 = (11 + 12)^2$

$$= (11 + 12)(11 + 12)$$

$$= (121 + 132i + 132i + 144(-1))$$

$= (-23 + 164i)$

$g^4 = ((11 + 12)^2)^2$

$= (-23 + 164i)^2$

$= (529 - 3772i - 3772i - 26896(-1))$

$= (-26367 - 7544i)$

$g^4 \bmod 7 = (-26367 - 7544i) \bmod 7$

$= (5 + 5i)$

r = hash $g^k||m$ = hash $(5 + 5i)||$ hello = "861f0151cfe95a52173d6faaae0b2708214c84d6"

Now Convert hexadecimal valueinto decimal numbers

861f0151cfe95a52173d6faaae0b2708214c84d6 = 259427964050000000000000000000

Now the other part of signature s calculated as following.

$$s = \frac{k}{r + va} \bmod n$$

$$s = \frac{k}{r + va} \bmod 7$$

$$s = \frac{4}{61 + 5} \bmod 7$$

$$s = \frac{4}{66} \bmod 7 = .0606060607$$

Signature = (.0606060607, 1)

4.4.4 Verification process

$g^k = (pa * g^r)^s$

$$g^k = ((-2 - 3i) * (11 + 12i)^1)^{.6060607}$$

$r' = \text{hash}(g^k || m)$

r′="861f0151cfe95a52173d6faaae0b2708214c84d6"

By converting to it to decimal $r' = 259427964050000000000000000000$

$$r' = 259427964050000000000000000000 \bmod 7 \ \ hence r' = 1$$

CHAPTER 5

SIMULATION AND RESULT

5.1Implementation and comparison of Results

In this chapter the implementation scenarios and the obtained results will be discus and explain in detail. The implementation scenarios are consists on signing and verifying processes of Digital signature for a message. In this thesis I have proposed four different Complex Shortened Digital signature algorithms based on complex numbers and compared each of them with the DSAwhich is based on real numbers. The first comparison has done for the Time taken during signing of a message by DSA and SCDSA. The second comparison has done for the time taken during verification process of a signature. Third comparison has done for the time taken for the solution of DLP and for CDLP. Forth comparison has done for the memory overhead during singing of a message by using DSA and SCDSA

5.2 Comparison of Time taken for signing a message byDSA and SCDSA

In this comparison the time has recorded during signing of a message by using DSA and SCDSA. Everyresulthas taken by applying different values for random number k as power, and keep constant the value of base number g. The base number for SCDSA has considered same as given in DSA but $23i$ is added to make it complex numberlike $(a + bi)$. The resulting table data and graph show that the time taken during signing process by SCDSA is small as compared to DSA.The reason is that computation of digital signature algorithm is straight forward and taking more operations for calculation of Public key P_a and other power containing numbers during signing, but the SCDSA used the method of squaring and multiplying method due to which its number of operations are minimized. And time taking per operation are minimizing.

Table5.1: Time Comparisonof DSA vsSCDSA

DSA based on DLP			SCDSA1 based on CDLP		
Real Base number (g)	Power (k)	Time elapsed for signing per message (msec)	Complex base number (g)	Power (k)	Time elapsed for signing per message (msec)
123235	10	116.1936	(123235+23i)	10	112.2342
123235	16	153.5753	(123235+23i)	16	127.9874
123235	20	310.1649	(123235+23i)	20	305.8963
123235	24	458.4521	(123235+23i)	24	450.8735
123235	28	689.8402	(123235+23i)	28	600.3274
123235	32	928.6666	(123235+23i)	32	713.3475
123235	36	1203.0725	(123235+23i)	36	922.9342
123235	40	1498.8336	(123235+23i)	40	1205.4732

We have performed these experiments multiple of times (average of 20 times) for each signature and the results are shown in the figure 5.1.

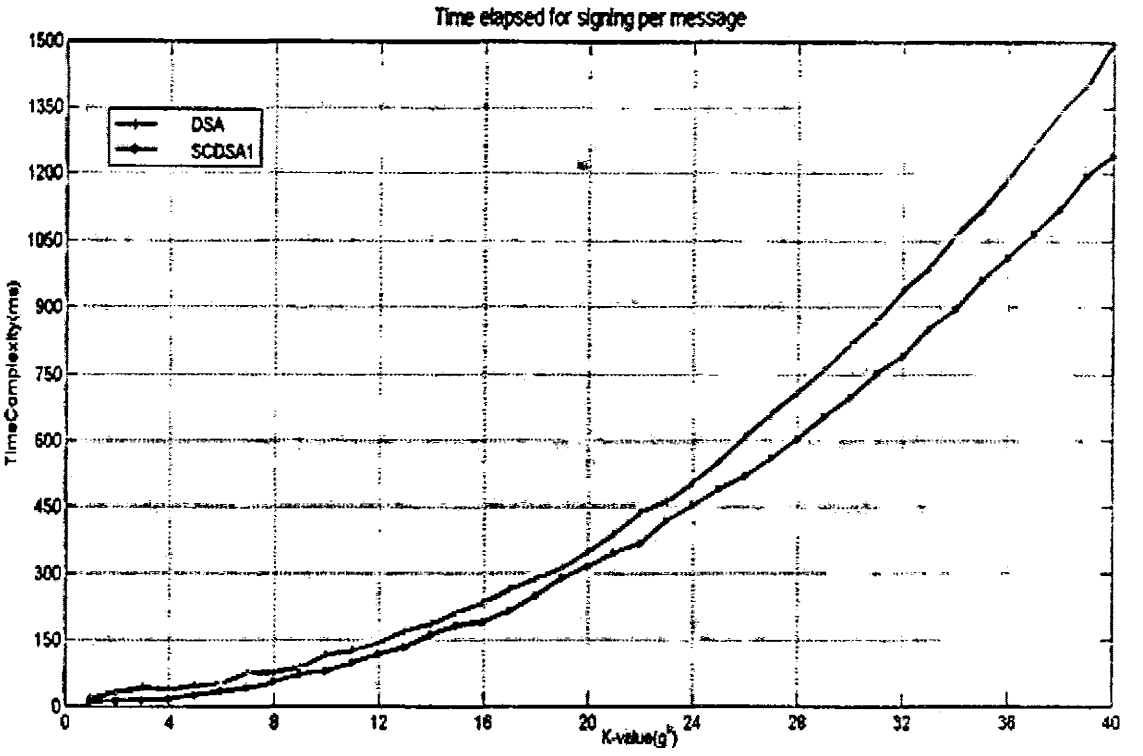


Figure.5.1: Time Elapsed for signing

5.3 Comparison of Time taken for Verifying of DSA and SCDSA

The comparison of time taken during verification process has recorded by changing the number of digits of base number g for DSA and SCDSA and shown the resulting values in a table as well as graphically. It show that the time elapsed during verification is less than that elapsed during the verification process of DSA. This is the reason of using the method, squaring and multiplying for verification method to determine the value of r'.And also the steps required for getting the value of g^k are very simple as compared to DSA.

Table 5.2: Time Comparison of DSA vs. SCDSA

DSA based on DLP		SCDSA1 based on CDLP	
Number of digits (Real number g)	Time elapsed for verification per message	Number of digits (Complex base number g)	Time elapsed for verification per message
8	63.5753	8	13.4673
12	98.9115	12	36.4345
16	189.4523	16	47.5323
20	279.9348	20	55.8475
24	426.9024	24	61.8734
28	598.7458	28	71.9853
32	689.8973	32	83.3471
36	983.8349	36	95.9532
40	1132.8293	40	99.0958

We have performed these experiments multiple of times (average of 20 times) for each verification process of signature and the results are shown in the figure 5.2. The graph of the existing is going up very rapidly because the number of operations during verification process is large and secondly the process of calculation is not simple. In our scheme only two operations are used one for the value of g^k and the other for the comparison computation of r'. Secondly for the power calculation of complex numbers we used the method of squaring and multiplying are used which has also minimize the number of operations.

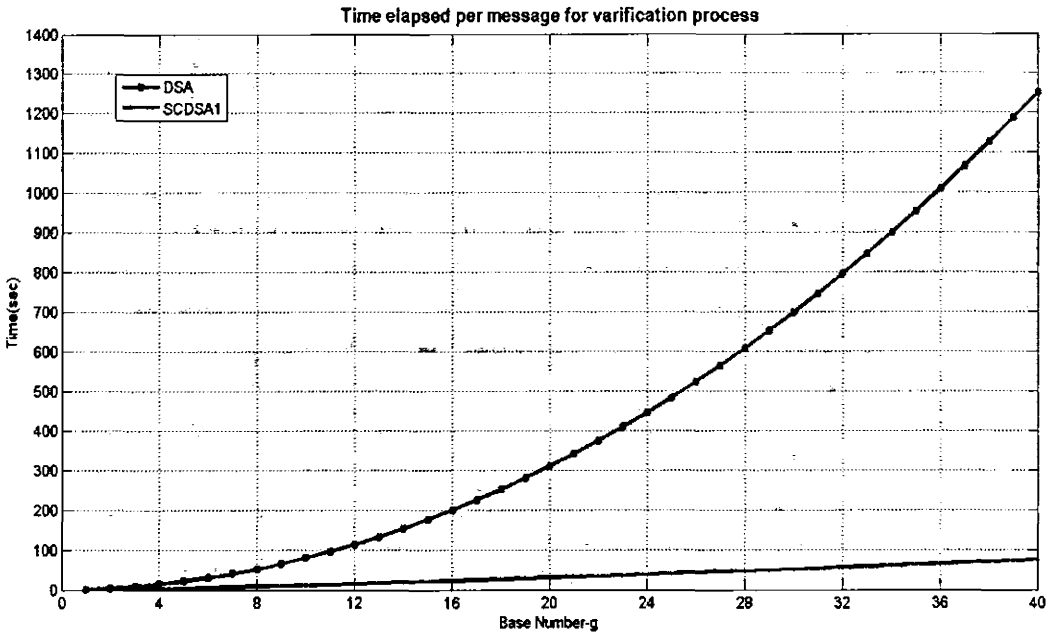


Figure: 5.2: Comparison of time elapsed during verification process

The signing and verification time of our proposed scheme will also be minimized, if we apply the same parameters and only change the number of characters of a message.

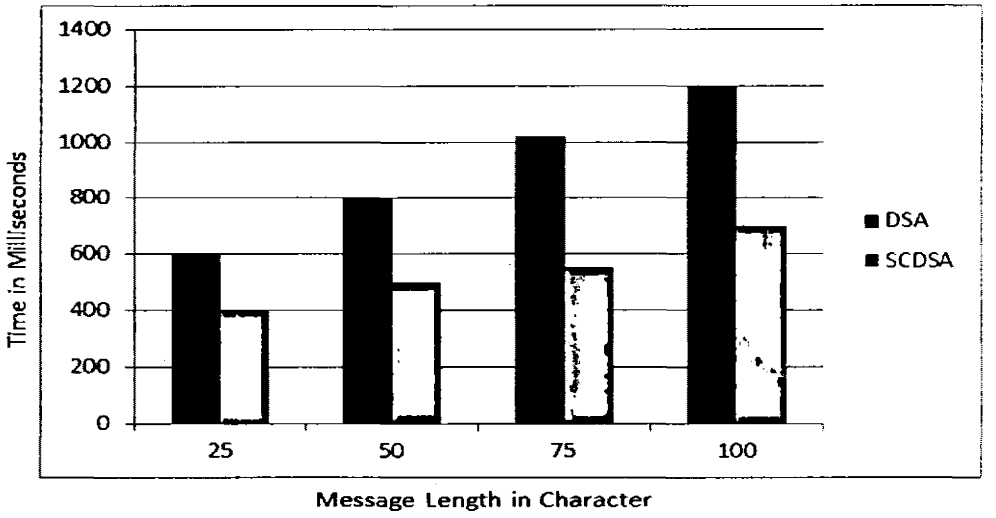


Figure 5.3: Time comparison for Message Variation

Above figure 5.3, show the comparison of DSA and SCDSA signatures.

5.3.1 Comparison of Communication overhead DSA and SCDSA per message

The existing DSA using different parameters like n of bit length *512-1024,q* of bit length *160* and g will be in the range of finite field for example *512*-bits. The signing algorithm is as following.

- $r = (g^k \bmod n) \bmod q$
- $s = (k^{-1}H(M) + va * r) \bmod n$
- Signature (r, s)

Hence the Signature length is calculated as following.

$|r| = |q| = 160$ bits

$|s| = |n| + |H(M)| = 512$ bits $+160$ bits

Signature (r, s) = $|q| + |n| + 160 = 160+512+160 = 832$ bits per message.

In our proposed scheme SCDSA1 the following algorithms are designed to make the r =160 bits and q =160 bits so the signature length will be 320 bits only, which is very small size.

- $r = \text{hash}((g^k \bmod n) \parallel m)$
- $s = k/(r + va) \bmod q$
- Signature = (r, s)

$|r| = 160\ bits$

$|s| = |q| = 160\ bits$

Signature $(r,s) = 160 + |q| = 160 + 160 = 320$ bits

So communication overhead per message has minimized approximately 60% per message.

5.3.3 Security Analysis Using Baby-Step and Giant -Step Algorithm

Security Analysis of DLP based DSA measured using by Baby-Step and Giant-Step method. The running time and memory storage of this algorithm has considered for the measurement of security. The running time of the algorithm is analyzes in term of input size in the form of bits and how much computing time it take. The Baby-Step and Giant-Step method used to solve the DLP Algorithm, $y=g^k$ by using the following steps.

Table 5.7: Security Analysis

DLP Based DSA					
k	g^k	yg^{-nk}	k	g^k	yg^{-nk}
1	5	269	21	1613	517
2	25	1261	22	2014	639
3	125	790	23	2002	821
4	625	914	24	1942	332
5	1108	603	25	1642	859
6	1506	1627	26	142	1050
7	1479	1336	27	710	1368
8	1344	1464	28	1533	1644
9	669	167	29	1614	171
10	1328	183	30	2	1214
11	589	273	31	10	1282
12	928	275	32	50	656
13	606	1799	33	250	1673
14	1013	1295	34	1250	82
15	1031	477	35	199	1974
16	1121	414	36	995	1523
17	1571	816	37	941	751
18	1804	556	38	671	1451
19	952	102	39	1338	346
20	726	1078	40	639	1442

The value of g is belonging to finite field F_q. Suppose $n = 1 + \sqrt{N}$ where $\sqrt{N}$ is in floor form. Now the values of k, g^k and yg^{-nk} are list in the form of a table. We consider discrete logarithm

problem $5^x = 3 \bmod 2017$. In this example g = 5 y =3, $n = 1 + \sqrt{2017} = 45$, $g^{-1} = 807$ in the range of finite field 2017. The above table-5.7 has constructed by using these parameters and compared the values of Baby-Step (g^k) and Giant-Step (yg^{-nk}) and recorded the point where the both values be same. Then find out the private key $x = i + jn$, is the solution of $y = g^k$. In the listed table the 22nd row's $yg^{-nk} = 639$ has compared with the row number 40 of $g^k = 639$. The value $5^{40} = 639 = 3.5^{-22(45)} = 3$. Hence the solution of the DLP is x = 40 + 22 (45) = 1030. Ours scheme, Shortened Complex Digital Signature Algorithm using CDLP having no possible attack during communication in the open network by adversary. The inverse mod, of a Complex numbers, is not lying in the domain of Baby-Step and Giant-Step method. Using the complex number for Shortened Digital signature is n time secure than m, where n >>m even whenever our proposed scheme designed by using very small complex number instead of largest real number.

CHAPTER 6

CONCLUSION AND FUTUR WORKS

6.1 Conclusion

This thesis has practically and theoretically concluded that the proposed Shortened Complex Digital Signature Algorithm having less computational time and less communication overhead during signing and verifying of a message. This means that we are minimized the communication overhead and time complexity during signing and verifying of digital signature for a message. The reason is of using small numbers as compare to DLP for signing and verification and the method of squaring and multiplication method during calculation of the power to minimize the number of operation. On the other hand side it is very hard to break SCDSA Based on CDLPas compare to DSA based on DLP, because the intruders used to recovers the private key required more calculations and computation as compared to DLP based on real numbers. Secondly SCDSA based on complex numbers using small numbers and provides equal security as compare to DSA based on DLP using large real numbers.

6.2 Future Work

The future work may includefinding out SCDSA by using IFPto minimize the computational cost and communication overhead,to make it more suitable for memory constraint devices such as PDA and devices implementing smart cards and make it practically applicable for these devices.

References

[1] W. Diffie, M.E. Hellman,"New Directions in cryptography", IEEE Transactions on Information Theory, Vol. 22, Issue 6, pp. 644-654, Nov, 1976.

[2] R.L.Rivest, A.Shamir, L.Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",Communication of the ACM, Vol. 21, pp. 120-126, 2003.

[3] T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" IEEE Transaction on Information theory, Vol. 31, Issue 4, JULY 1985.

[4] A. N. Moldovyan"An Approach to Shorten Digital Signature Length" Computer Science Journal of Moldova, Vol. 14, no.3, pp. 390-396, 2006.

[5] Z. Shao, "A Provably secure short signature scheme based on discrete logarithms" Journal of Information science Vol. 177, pp. 5432-5440, May 2007.

[6] E.S Ismail, N. Tahat and R.R Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms" Journal of Mathematics and statics Vol. 4, Issue 4, pp. 222-225, 2008.

[7] A. Nikolay,"Short Signatures from Difficulty of FactorizationProblem" International Journal of Network Security, Vol.8, Issue1, pp.90-95, Jan 2009.

[8] N. Tahat, E. Ismail, R. Ahmad, "A New Blind Signature Scheme Based On Factoring and Discrete Logarithms" International Journal of Cryptology Research, Vol. 1, Issue 1, pp. 1-9, 2009.

[9] A.Sagheer, N. Mottar "Complex Public Key Cryptosystem" AL-Mansour Journal Vol.14, Issue 14, pp.105-119, 2010.

[10] H.Chen, X.Shen"A new Digital Signature Algorithm Similar to ElGamal Type" Journal of Software, Vol.5,Issue3, pp. 320-327, March 2010.

[11] E.Noorouzi, A. Reza, E. Haghighi, F.Peyravi, A.Zadeh "A New Digital Signature Algorithm" International Conference on Machine Learning and Computing IPCSIT Singapore, Vol.3, 2011

[12] S. Verma and B. Sharma "A New Digital Signature Scheme Based on Two Hard Problems" International journal of pure and applied science and technology, Issue10, pp. 55-59, June 2011.

[13] H.Zhang, "El-Gamal Digital Signature Scheme with a private key pairs" IEEE transaction in computer science and information engineering, pp. 1-5, 2010.

[14] M.Parida, " A Secure Short Signature Scheme Based upon Biometric Security" Vol. 2, Issue5, First student Research Symposium in conjunction with Seventh ICDCIT, Feb 2011.

[15] H. Lin, T. Zong,and Y. Yeh, "A DL Based Short strong Designated Verifier Signature Scheme with Low Computation" Journal of Information science and Engineering, Vol. 27, pp. 451-463, 2011.

[16] Cisco Syste, Inc, All Rights Reserved, "A Beginner's Guide to Network Security" 2001.

[17] J.E. Canavan,"Fundamentals of Network Security" ARTECH HOUSE, INC, 2001.

[18] M. Kumar, "Cryptographic study of some Digital signature scheme"Ph.D thesis,Dr. B.R. Ambedker University, Agra, 2003.

[19] H. Jono and Z. Heng"A practical digital multi-signature scheme based on discrete logarithm", Advance in Cryptology in Springer and Verlag, pp.16-21, 1992.

[20] L.Harn and T.Kiesler, "New Scheme for Digital Multi-signature" Electronic Letters, Vol. 25 Issue 15, pp. 1002-1003, 1989.

[21] J. Nechvatal"Public key cryptography", NIST – USA, 1992.

[22] D. Chaum,"Group signatures", Advance in Cryptology-Eurocrypt, Springer Verlag,pp. 257-265, 1991.

[23] L. Chen and T.PPederson,"New group signature signatures", Advance in Cryptology Eurocrypt - 94, Springer Verlag, pp.171-181, 1994.

[24] Y. Desmedt and Y. Frankel,"Threshold cryptosystems", Advances in Cryptology – Crypto- 89, Springer Verlag, pp. 307-315, 1990.

[25] Y. Desmedt"Threshold cryptography", European Transactions on Telecommunicationsand Related Technologies,Vol. 5 Issue 4, pp.35 – 43, 1994.

[26] D. Chaumand V. Autwerpan"Undeniable signatures", Advance in Cryptology-Eurocrypt-89, Springer Verlag, pp. 212-216, 1989.

[27] D. Chaum"Zero knowledge undeniable signatures", Advance in Cryptology-Eurocrypt - 90, Springer Verlag, pp. 458-464, 1990.

[28] J.L. Camenish,J.M. Piveteare and M.A. Stadler"Blind signature based on discrete logarithm problem", Advance in Cryptology-Eurocrypt - 94, Springer Verlag, pp. 428-432, 1994.

[29] D. Chaum,"Blind signature for untraceable payments", Advances in Cryptology – Crypto- 82, Springer Verlag, pp. 199-203, 1982.

[30] K. Zhang, "Nourepudiable Proxy signature scheme", http://www.citeseer.nj.nec.com, 1997.

[31] K. Zhang,"Threshold proxy signature schemes", Advances in Cryptology - Crypto–98, Springer, Verlag, LNCS # 1396, pp. 282 – 289, 1998.

[32] M.S. Hwang, C.C. Yang, S.Tzeng, "Improved digital signature scheme based onFactoring and discrete logarithms", Journal of Discrete Mathematical Sciences andCryptography, Vol. 5 Issue 2, pp. 151-155, 2002.

[33] R. L. Rivest, A. Shamir, L.Adleman, "A method for obtaining digital Signatures andPublic Key Cryptosystems", Common ACM Vol. 21, 1978.

[34] T. Gamal, "A public-key cryptosystem and a signature scheme based on discrete Logarithms", IEEE Transactions on Information Theory, pp. 469-472, 1985.

[35] S. Zeng, C. Yang and M. Hwang, "A new digital signature scheme based on Factoring and Discrete Logarithm", International Journal of Computer Mathematics, pp. 9-14, 2004.

[36] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms", IEEProceedings, Computers and Digital Techniques, pp. 193-195, 1994.

[37] Z. Shao, "Digital signature schemes based on factoring and discrete logarithms", Electronic Lett, pp.1518-1519, 2002.

[38] B. Schneier, "Applied Cryptography"Second Edition, John Wiley & Sons, Inc, 1996.

[39] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.

[40] National Institute of Standards and Technology, NIST FIPS PUB 180-1, "Secure ,Hash Standard," U.S. Department of Commerce, April 1995

[41] D.R. Stinson, Cryptology: Theory and Practice, CRC Press, Inc., 1995