ON SECURITY AND PERFORMANCE IN ECC, NONCOMMUTATIVE CRYPTOGRAPHY AND SIGNCRYPTION

A Thesis

Submitted in partial fulfillment for the requirement of the degree of

DOCTOR OF PHILOSOPHY

by

GAUTAM KUMAR

Enrolment No.: 136202

Under the Supervision of

Dr. Hemraj Saini

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION TECHNOLOGY

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT, SOLAN-173234, HIMACHAL PRADESH, INDIA

February 2017

ACKNOWLEDGEMENT

First and foremost I offer my sincerest gratitude to my supervisor Dr. Hemraj Saini who has supported and motivated me throughout my PhD work with his patience and knowledge whilst allowing me the room to work in my own way. I have learnt a lot from him. I consider myself very fortunate for having been associated with the scholar like him. His affection, guidance and scientific approach served as a veritable incentive for completion of this work.

I sincerely thanks to Prof. (Dr.) Satya Prakash Gharera, for his valuable suggestions and comments throughout the whole presentations. I am also thankful to the faculty members on my reading and orals committee's members: Dr. Vivek Sehgal, Dr. Ravindara Bhatt and Dr. Shruti Jain for providing a valuable feedback on the research results. Although it is not possible to name individually, I cannot forget my well wisher of Jaypee University of Information Technology for their persistent support and cooperation.

This acknowledgement will remain incomplete if I fail to express my deep sense of obligation to parents, brothers, mother-in-law for their consistent blessings and encouragements. During the critical conditions they came as a big supporter and motivated me even under odd situations. It was just liked almighty God was always with me and felt I am blessed by God for good deeds.

Finally, I thank my wife "Ashmita Roy" and little lovely daughter "Mansi Gautam" for supporting me throughout my studies at University and as required they always shown full-fledged matured behaviors to complete my work without by requested any of the unnecessary needs.

Gautam Kumar

Enrolment No.: 136202

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled **"ON SECURITY AND PERFORMANCE IN ECC, NONCOMMUTATIVE CRYPTOGRAPHY AND SIGNCRYPTION"** submitted at **Jaypee University of Information Technology, Waknaghat, Solan, H.P, INDIA** is an authentic record of my work carried out under the supervision of **Dr. Hemraj Saini**. I have not submitted this work elsewhere for any other degree. I am fully responsible for the contents of my PhD Thesis.

(Signature of the Scholar)

(Gautam Kumar)

Department of Computer Science & Engineering

Jaypee University of Information Technology, Waknaghat, Solan, H.P, INDIA

February 2017

SUPERVISOR CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled "**ON SECURITY AND PERFORMANCE IN ECC, NONCOMMUTATIVE CRYPTOGRAPHY AND SIGNCRYPTION**", submitted by **Gautam Kumar** at **Jaypee University of Information Technology, Waknaghat, Solan, H.P, INDIA** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

(Signature of Supervisor)

(Dr. Hemraj Saini)

Jaypee University of Information Technology, Waknaghat, Solan, H.P, INDIA

February 2017

LIST OF ACRONYMS & ABBREVIATIONS

(Alphabetically)

ADD	Point Addition Operations
ADDDBL	Composite operation of ADD and DBL as a single operation
ANSI	American National Standards Institute
AVISPA	Automated Validation of Internet Security Protocol Application
CAS	Computer Application Software
CDH	Computational Diffie-Hellman
CDP	Conjugacy Decisional Problem
CL-AtSe	Constraint Logic-based Attack Searcher
CP-ABE	Ciphertext-Policy Attribute-based Encryption
CR	Challenge Response
CSP	Conjugacy Search Problem
DBL	Point Doubling Addition
DIM	Domain Interoperability Manager
DLP	Discrete Logarithm Problem
DLP-ECC	Point Doubling Addition for ECC
DRM	Digital-Right Management
DS	Digital Signature
DSA	Digital Signature Algorithm
EC-operations	Elliptic Curve Group (Arithmetic Points) Operations
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECSM	Elliptic Curve Scalar Multiplication
ED	Encryption-Decryption
ESG	Extra Special Group
FIPS	Federal Information Processing Standards
GSDP	Generalized Symmetrical Decomposition Problem
HIS	Health information systems

HLPSL	High Level Protocol Specification Language
HLPSL2IF	High Level Protocol Specification Language-to-Intermediate Format
HSP	Hidden subgroup or subfield problem
HTA	Health technology assessment
I	Arithmetic Inversion
ICT	Information Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Intermediate Format
IFP	Integer Factorization Problem
ISO	International Organization for Standardization
LSB	Least Significant Bit
M	Arithmetic Multiplication
MAC	Message Authentication Code
mADD	Mixed Addition Operation
MCEPAKE	Multilayer Consensus ECC- Password Authenticated Key Exchange
MSB	Most Significant Bit
MSC	Message Sequence Chart
NAF	Non-Adjacent Form
NB	Normal Basis
NCC	Noncommutative Cryptography
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OFMC	On-the-fly Model Checker
PACS	Picture and Archiving systems
PAKE	Password Authenticated Key Exchange
PCL	Protocol Composition Logic
PDH	Polynomial Diffie-Hellman
PDS	Protocol Derivation System
PKC	Public Key Cryptography
PKI	Public Key Infrastructure

PRS	Proxy Re-Signature
PSD	Polynomial Symmetrical Decomposition
RIS	Radiology information systems
RSA	Rivest-Shamir-Adleman
SATMC	SAT-based Model Checker
SCPRE	Signcryption Proxy Re- Encryption
SCPRS	Signcryption Proxy Re-Signature
SDP	Symmetrical Decomposition Problem
Sq	Arithmetic Squaring
SM	Scalar Multiplication
SSCA	Simple Side-Channel Attack
SUB	Arithmetic Subtraction
TA4SP	Tree-Automata Based Protocol Analyzer
w-NAF	Window Non-Adjacent Form

LIST OF SYMBOLS

$\oplus$	An Addition Group Low Binary Operation on a Curve
|G|	The Order of G
O	The Point at Infinity
α	Root of an Irreducible Polynomial
ω	Non-Zero Terms in an Irreducible Polynomial
−P	A Unary Operation on a Curve E, Namely, Point Inverse
A	Finite Field Arithmetic Addition
D	Finite Field Arithmetic Multiplication by Curve Constant
E	An elliptic curve
E(F)	A Group Formed by The Points on E Defined over The Field F
F	An Arbitrary Finite Field
F_2^m	Finite Fields over Characteristic Two (Binary Extension Fields)
g	Generator of Fp
G	A Random Finite Cycle Group of p Elements
$g_a = g^a \bmod p$	A's Public key
$g_b = g^b \bmod p$	B's Public key
GF (2m)	Finite Fields over Characteristic Two (Binary Extension Fields)
GF (p)	Finite Fields over Prime Integer
I	Finite Field Arithmetic Inversion
k	A Scalar Integer
kP	Elliptic Curve Scalar Multiplication of an Elliptic Curve Point P With a Scalar k
m	Positive Integer
p	Prime Number
P	A Point on a Curve
P(x)	An Irreducible Polynomial
P(xP, yP)	A Point With Coordinates (xP, yP) in Affine Coordinates
r-NAF	Radix-r Non-Adjacent Form
S	Finite Field Arithmetic Square
w-NAF	Width-w Non-Adjacent Form
Z	Set of All Integers

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The thesis addresses the security and performance advancement for the Discrete Logarithmic Problem (DLP) in the following primitives of cryptography such as: Elliptic Curve Cryptography (ECC), Edwards and twisted Edwards Curves, Noncommutative Cryptography (NCC), multilayer key generation for ECC using signcryption and proxy re-cryptographic approach. These entire primitive formulates into the following five objectives:

The first objective claims Radix-16 scalar multiplication without pre-computations for ECC. Using the designed hardware support the proposed claim shows the more appropriateness for reduced instruction set computing and is a particular suite for low memory devices with resistance to the simple side channel attack and safe-error fault attack. This is in theoretically computing 6.25 percent faster than the recently proposed Radix-8 scalar conversion technique without pre-computed operations. The performance from the hardware perspective also improves by 8.33 percent.

The second objective works on the architecture of prime Edwards curves and extended Twisted Edwards curves on 4-processors and 8-processors. The proposed scalar multiplication results for both the curves are available on the reduced clock cycles and in a reduced multiplication processing costs.

The third objective pertains on Noncommutative Cryptography (NCC), which is truly a fascinating area with great hope of advancing performance and security for high end applications. It provides a high level of safety measures. The basis of this group is established on the Hidden subgroup or subfield problem (HSP). A proposed scheme is based on the extra special group (ESG), for finding the solution of an open problem, for the most appropriate Noncommutative platform. This ESG supports at Heisenberg, Dihedral order and Quaternion group. The working principle is made possible on the random polynomials chosen by the communicating parties for secure key-exchange, encryption-decryption and authentication schemes on NCC. On the proposed scheme, this is also enhanced from the general group elements to equivalent ring elements, known by the monomials generations for the cryptographic schemes. The group of orders is more challenging for length based attacks and brute-force attacks.

The fourth objective is the key generation for password authenticated key exchange for multilayer consensus using the signcryption approach. Where, signcryption combines signature and encryption cost in the form of reduced computation cost and communication cost in a single operation. The proposed methodology potentially reduces the overall computation time in key generation and signature generation. The results are tested on SPAN and Automated Validation of Internet Security Protocol Architecture (AVISPA) tools.

The fifth objective focuses on situations under a cryptographic key management by a semi-trusted proxy, where data encrypted under one cryptographic key need to be re-encrypted. In modern era of cryptography, this is one of the new diverse trend and motivating issue. It is probably a secure and efficient trust based approach for third party, who is not directly involved 'called proxy'. Also, the same work is simulated on AVISPA/SPAN. An application of Telemedicine is also simulated on above tool using Radix-16 scalar multiplication.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1CRYPTOGRAPHIC FOUNDATION AND ITS RELIABLE PRIMITIVES

The foundation of cryptography is conceptually a centralized approach to generate the randomness and unpredictability behaviors of keys, management and maintenance of associated resources in order to secure the provided environment. Cryptography is closely connected to number theory, so fundamentally it is based on rigorous mathematics on probability theory. The ciphers systems analysis and statistical methods are heavily drawn to make use of arithmetic structures in cryptography. Moreover, on theoretical problem the pre-assumptions represent the toughness or security strength of the constructions. Information security construction of system is used as algebraic codes and combinatorial structures as the most important techniques, where mathematical designed models and its proofs are forming the foundation of security.

A number theoretic problem offers a foundational framework for security schemes, almost for all cryptographic systems, which releases most of the hard computational problems. Algebraic curves on finite fields in field values are serving as the basis for much of public key cryptography [2]. For example, one well-known algorithm of RSA for security is based on the prime factorization difficulty on a large prime. To find a prime factorization is one of the unsolved problems in computer science and is in general combined under the term discrete logarithm problem.

The acceleration of cryptographic functions is in determining the level of required encryption and is in relation to identifying sensitive information, is one of the areas as a research gap. To consider the various threats at different points to ensure operations are avoiding processing bottlenecks and are still having an appropriate acceleration with the life cycle. To establish the key lengths with the right combination of flexibility and protection are the widely acceptable standards. These should be analogous with the strong classification on cipher/algorithms and the changes over specific time duration. To protect and control sensitive data is the suite of encryption schemes that enables it to expand in the volumes, location and type from the data

centre to virtual environments. A dedicated hardware is also used to provide a variety of solutions for offloading cryptographic processes from application servers and it is needed to consider its efficient complexity analysis along with incorporating high-speed cryptographic processors.

Researchers have explored various theoretic structures on global fields, group's elements, and function infrastructures of fields that can serve as the basis for cryptographic schemes [3]. The research not only contributes to a better understanding of the Discrete Logarithmic Problem (DLP) in mathematical settings, but is also of mathematical interest in its own right.

The efficiency of algorithm is measured in terms of the computation costs. It relies on the speed of the arithmetic in various algebraic structures in the forms of as finite field operations or adding an elliptic point on the curve. Thus, to investigate the efficiency towards improving the speed of the underlying arithmetic operations and the same should be used to solve problems in arithmetic of computational number theory, is the most important to accelerate the performance gain [4]. An algorithm for fast arithmetic of divisors on radix-16 algebraic curves is a research gap and to find the global invariants of global fields in various number theoretic settings is a research interest. This research hangs in between theoretical foundations, design algorithm and its analysis. Further, it focuses on highly-optimized software simulations, and to make its applicability in applications.

1.1.1 Role of Cryptographic Primitives

The definition of Cryptographic primitives says that the cryptographic algorithms should be on well-established on low-level protocols, which are frequently used to construct cryptographic functions for computer system securities. Their routine includes public or private key cryptography, encryption, authentication, digital signatures, one-way hash functions, pseudo randomness, private information retrieval, commitment scheme, and pool communication schemes to anonymize from the mix networks [1].

While creating cryptographic systems, designers use cryptographic primitives as their most basic building blocks, the cryptographic primitives are designed to do one very specific task in a highly reliable fashion. Since cryptographic primitive's is used as building blocks and they are very reliable to perform according to their specification [2]. For example, if an encryption routine claims to be only breakable with X number of computer operations, then if it can be broken with

significantly less than X operations, that cryptographic primitive is said to have failed. If a cryptographic primitive is found to fail, almost every protocol that uses it to become vulnerable. Since creating cryptographic routines is very hard to design a new cryptographic primitive and testing them to be a reliable is one of the long time process, so to make it secure and not to be sensible, is the need of a new cryptographic system. The reasons include:

The designer might not be competent in the mathematical and practical considerations involved in cryptographic primitives. Designing a new cryptographic primitive is very time-consuming and very error prone, even for experts in the field. Since algorithms in this field are not only required to be designed well, but also need to be tested well by the cryptologist community, even if a cryptographic routine looks good from a design point of view it might still contain errors. Successfully withstanding such scrutiny gives some confidence that the algorithm is indeed secure enough to use [3]; security proofs for cryptographic primitives are generally not available [4].

Cryptographic primitives are similar in some ways to programming languages. A computer programmer rarely invents a new programming language while writing a new program; instead, he/she uses one of the already established programming languages to program it. Crypto system designers, not being in a position to definitively prove the security of their system: - choose the best primitive available for use in a protocol usually provides the best available security. However, compositional weaknesses are possible in any crypto system and it is the responsibility of the designer(s) to avoid them.

Cryptographic primitives, on their own, are quite limited and they cannot be considered properly. For instance, a bare encryption algorithm will neither provide any authentication mechanism, nor any explicit message integrity checks. For example, to transmit a message it not should be encoded but should also be protected from tinkering (i.e. it is confidentiality and integrity-protected). An encoding routine can be used in combination, such as DES and a hash-routine SHA-1. If the attacker does not know the encryption key, he/she cannot modify the message such that message digest value(s) would be valid [5].

Combining cryptographic primitives is to make a security protocol. Most exploitable errors (i.e., insecurities in crypto systems) are not only due to design errors in the primitives (assuming always that they were chosen with care), but to the way they are used, i.e. bad protocol design

and buggy or not being careful enough during implementation. There are some basic properties that can be verified with automated methods, such as BAN logic. There are even methods for full verification (e.g. the AVISPA [6] or SPAN [7] or SPI calculus) but they are extremely cumbersome and cannot be automated. Protocol design is an art requiring deep knowledge and much practice; even then mistakes are common.

1.1.2 Levels of Security

The cryptographic primitive uses some models to define its security such as heuristic secure, as secure as, proven secure, quantum secure, and unconditionally secure. A heuristic security refers to as long as no attack has been found on applied systems. Most of practical cryptosystems falls within this category. *As secure as* security is another variation of security that says a cryptosystem or protocol can be proven to withstand a new attack against the other and vice versa.

A system or protocol is said to be proven secure relative to an assumption if one can prove that assumption is true, this implies that the formal security definition is satisfying for that system or protocol.

A cryptosystem is unconditionally secure when the computer power of the opponent is unbounded, and it satisfies a formal definition of security. Although these systems are not based on mathematical or computational assumptions, usually these systems can only exist in the real world where true randomness can be extracted from the universe.

The fundamental to cryptography is based on definition, conceptualizations and construction of computing systems that addresses security concerns. The basis includes such as the approaches on computational difficulty, rigorous treatment on the foundational issues, pseudo randomness, solving cryptographic problems and zero-knowledge proof.

1.1.3 Definition and Importance of Discrete Logarithmic Problem

In mathematics, Discrete Logarithm is a problem of finite group theory [8]. Its definition can be correlated by a numerical example: For any prime P, and an integer a to the power of any number x from 1 to $p - 1$ or beyond on integer is known as Discrete value b, which is generating on this principle. Now, to revert back to the power of a from 1 to $p - 1$ or beyond to obtain or that

satisfies the discrete value- b, is known by the Discrete Logarithmic Problem (DLP). The computation of discrete is easy and is a one way function but the DLP is a hard problem.

This can also be understood by the equation- $y = g^x \bmod p$. On a given g, x and p, it is straight forward to calculate y. In the worst case, an algorithm works x repeated multiplication for achieving greater efficiency. But on given y, g, and p, it is, in general, very difficult to find x (discrete logarithm) for the same [9]. Computing discrete logarithms is believed to be difficult. No efficient general method for computing discrete logarithms on conventional computers is known, and several important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem has no efficient solution [10].

1.2 GENERAL INTRODUCTION AND DLP ON ELLIPTIC CURVE CRYPTOGRAPHY

ECC was proposed by Victor Miller and Neal Koblitz [12]. It has attained a number of advantages; firstly, there is a greater flexibility in choosing the group; second, there is an absence of a sub-exponential time algorithm to break the system if the group is suitably chosen. ECC is a strong scheme due to these two reasons. The Discrete Logarithmic is used to identify the basic and individual points on the curve that satisfy for the strong connection and represents the applicability for the individual elements. Similarly the Elliptic Curve Discrete Logarithm Problem has been defined on given points P and Q in an elliptic curve group (ECG) elements over a finite field to find an integer x such that $xP = Q$. Here x is called the discrete log of Q to the base P.

The time to reach the elliptic curve discrete logarithm problem is $time_{elliptic} \sim exp\left(c\sqrt{m}\right)$. Where, c is a constant and m is the number of discrete points on Elliptic Curve. Comparing this to RSA we see that $time_{RSA} \sim exp\left((logN)^{\frac{1}{3}}\right)$. So, one can say that RSA is broken in sub-exponential time. The discrete log for RSA relies upon the idea of difficulty to factor into the two prime factors. The key lengths of ECC also grow more slowly than those of RSA.

This doesn't seem like a difficult problem, but if you don't know what x is calculating $xP = Q$ takes roughly $2^{x/2}$operations. So if secret says x is 160 bits long, then it would take about 2^{80} operations. To bring this into consideration, if you could do a billion operations per second, this

will take about 38 million years. The smaller size of the keys for Elliptic Curve Encryption makes it ideal for applications like encrypting credit card transactions, cell-phone calls and other applications where speed and memory are main issues. There are merits and demerits in both cases with ECC and RSA encryption. ECC is faster than RSA for signing and decryption, but slower than RSA for signature verification and encryption.

Further, the reason to cover the Elliptic Curve Cryptography (ECC) is to accelerate the standardized performance of RSA algorithm that is being used in public key cryptography and available products for digital signature and encryption used in the field of security. The RSA algorithm uses a heavier and slower processing load specially for conducting a large number of secure transactions in electronic commerce. The major attraction of ECC is showing up in standardized efforts in equal security strength for a far smaller key size. Therefore, it is directly reducing the processing overhead. Further, scalar multiplication is an operation used in ECC as the name represents multiplication but algorithm does the multiplication using repeated addition. So, from the security points of view it is most suitable.

The hierarchy of ECC is a behavioral representation of complete operation that has organized into levels, as shown in Figure 1.1.

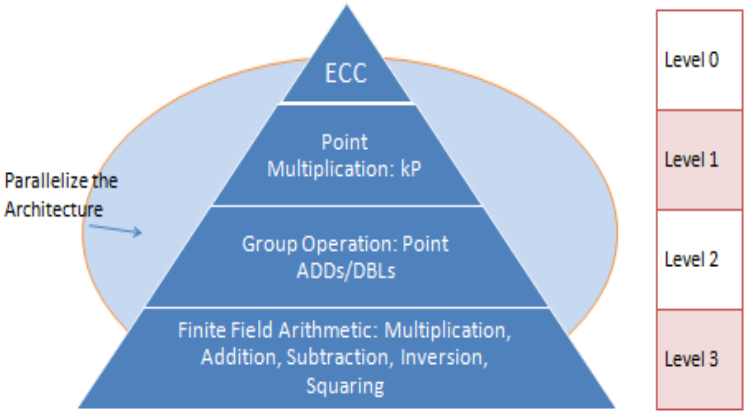


Figure 1.1: Hierarchy of ECC

The level 0 is the highest level, where ECC algorithm is used for its operation of scalar multiplication. This ensures the group operations, which depend on point additions (ADDs) and point doubling (DBLs) and these two operations are dependent on the finite field arithmetic multiplication, additions, subtraction, inversions and squaring operations. The architecture of

ECC has been parallelized to improve the system performance to reduce the pre-computed operations. This may be a motivational issue for further research issues.

The key strength is also representing an advantage for using elliptic curve approaches over RSA. The table 1.1, roughly summarizes the key strength of ECC compared with RSA for the same level of security [141].

Table 1.1: Equivalent Security for RSA and ECC

RSA Key length	ECC Key Length
1024	160
2048	224
3072	256
7680	384
15360	512

ECC algorithm defines the elliptic curve equation on two variables with some of its coefficients. These are restricted in finite field arithmetic. The general equation of elliptic curve is defined as:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (1)$$

Where x and y are variables and a, b, c, d and e are real numbers. This has also a simplified equation of the form as:

$$y^2 = x^3 + ax + b \quad (2)$$

The above such equation is said to cubic and with a degree of 3. To plot a curve, need to compute:

$$y = \sqrt{x^3 + ax + b} \quad (3)$$

For each value of a and b, the plot consists of positive and negative values of y for each value of x. Thus each curve is symmetric about $y = 0$.

Now, to consider the Elliptic curve $E(a, b)$on elliptic curve E for all points (x, y) that should satisfy equation (3). For two different points on (a, b) results are in a different set of values. The geometrical set $E(a, b)$ for $x^3 + ax + b$ doesn't provide repeated factors, with the condition on $4a^3 + 27b^2 \neq 0$.

The algebraic description of scalar multiplication computation is based on either prime fields or binary fields for point addition and point doubling operations. Prime field uses are best for software application and binary fields are best for hardware applications, where it takes

remarkably few logic gates to create a powerful and fast cryptosystem. In figure 1.2, for point addition & doubling cost have been presented for prime field. The scalar multiplication formulas for two such points $P(x_1, y_1)$ and $Q(x_2, y_2)$ for point addition and doubling such as $P + Q = (x_3, y_3)$ and $2P = (x_3, y_3)$ procedure have been given, respectively. These operations depend on the arithmetic operations such as squaring, multiplication and inversion. The addition and doubling depends on the idea of same points and different points. For one point addition 13,617 clock cycles are needed and for one point doubling 14,000 clock cycles are needed, as per reference [15].

Prime Field	**Binary Field**
Doubling: The general condition both points, $P = (x_1, y_1)$ and $Q = (x_1, y_1)$ $\lambda = \frac{(3{x_1}^2 + a)}{2y_1}$ if $P = Q$ $x_3 = \lambda^2 - x_1 - x_2$ $y_3 = \lambda(x_1 - x_3) - y_1$ • Two squaring, Two multiplication, and One inversion	**Doubling:** The general condition $P \neq -P$, where $P = (x_1, y_1)$ and $2P = (x_3, y_3)$ $x_3 = {x_1}^2 + \left(\frac{b}{x_1}\right)$ $y_3 = {x_1}^2 + \left(x_1 + \frac{y_1}{x_1}\right)(x_1) + x_3$ • Two squaring, Two multiplication, and Two inversion
Addition: $\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)$ if $P \neq Q$ $x_3 = \lambda^2 - x_1 - x_2$ $y_3 = \lambda(x_1 - x_3) - y_1$ • One squaring, Two multiplication, and One inversion	**Addition:** $\lambda = \left(\frac{y_1 + y_1}{x_1 + x_2}\right)$ if $P \neq Q$ $x_3 = \lambda^2 + \lambda + (x_1 + x_2) + a$ $y_3 = \lambda(x_1 - x_3) - y_1$ • One squaring, Two multiplication, and One inversion

Figure 1.2: General Cost for ECC Operations

The prime and binary based operations can be easily calculated by computer system, which is also the heart of every cryptosystem for ECC. For binary field, the scalar multiplication on $E(a, b)$on elliptic curve E for all points- (x, y), the point addition $P + Q = (x_3, y_3)$ for $P(x_1, y_1)$ and $Q(x_2, y_2)$ defined on $P \neq \pm Q$, where negative of $P(x_1, y_1)$ is equal to $-P = (x_1, x_1 + y_1)$:

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

$$x_3 = \lambda^2 + \lambda + (x_1, x_2) + a$$

$$y_3 = \lambda(x_1, x_3) + y_1 + x_3$$

The point doubling for- $P(x_1, y_1)$, when $P \neq -P$, is defined as:

$$x_3 = {x_1}^2 + \left(\frac{b}{{x_1}^2}\right)$$

$$y_3 = {x_1}^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3$$

Here one can realize the requirement cost of two squaring, one inversion, and two multiplications.

1.2.1 Working Principle of ECC

The working of elliptic curve contains an interesting property that takes two points on the curve and adds them, further again gets another point on the curve. From the general cryptographic point of view, the extremely useful work is to determine the resultant on two point coordinates (x, y) that add together to form new points on the curve with point addition and point doubling operations. This is defining an over a field operation. Here, a brief idea is presented. Suppose the curves are- $y^2 = x^3 + 8x^2 + 16$, its (x, y) coordinates are represented on the plane in Figure 1.3:

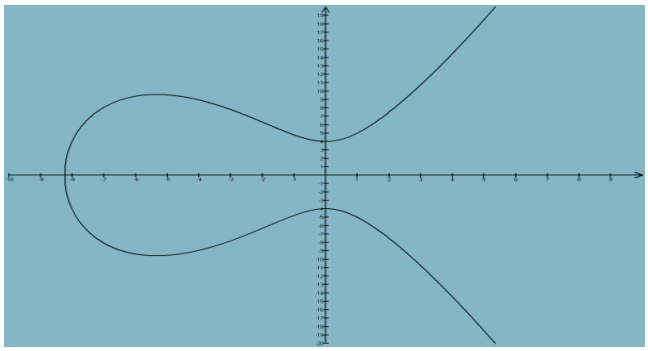


Figure 1.3: Elliptic Curve Graph

One of the simplest ways to analyze the operation on elliptic curve is an imagination on coordinates. To choose a point P on the curve, that helps to guide to find new points on the curve. For finding its negative, add P to the point at infinity is one of process. This is done in our example to find P's mirror image from the x-axis as represented in Figure 1.4:

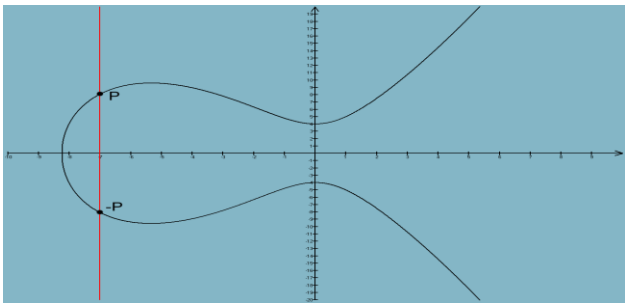


Figure 1.4: Elliptic Curve Graph Points

Adding of two points is done as follows: first a line is drawn containing points P and Q. The scalar multiplication point is named PQ or $P.Q$. The PQ is not a multiplication, it is obtaining on behalf of some arithmetic finite fields operations; it is one of the important to realize. The meaning is that PQ is added to the point at infinity which yields point $P + Q$, as shown in Figure 1.5.

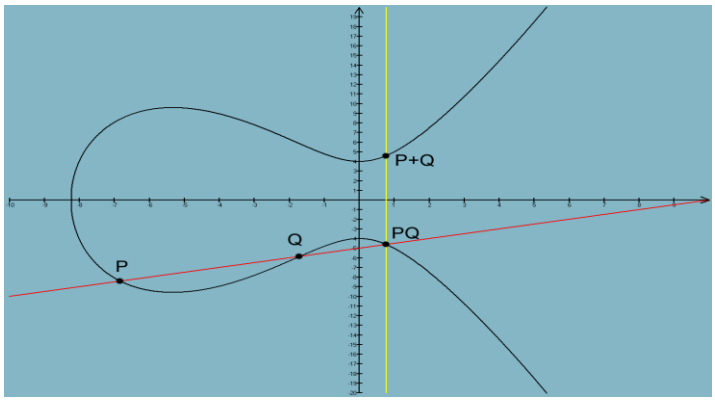


Figure 1.5: Addition and Multiplication Points on Elliptic Curve

In a sense of different possible way for doing addition is when P as is added to any point that intersects the curve using a tangent line drawn and it also represents a special case. The additions for rest are following as previous concepts, as in Figure 1.6.

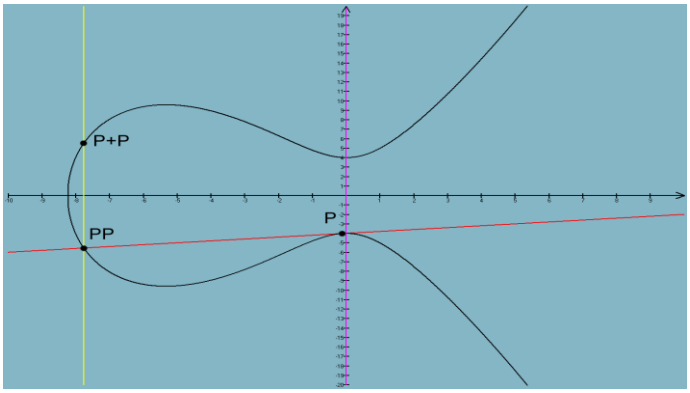


Figure 1.6: Elliptic Curve Point Addition and Multiplication

A subtraction operation is treated as similar as addition work in the standard way. The point to subtract is simply negated before being added in the 2's complement form. Further, multiplication is a possible replacement with the repeated additions. In ECC we never multiply two points together. Instead for same it multiplies its factor in some of the way. The result is

actually the same and it does apparent in readable form. Also, a prime polynomial evaluations on modulus for point addition reaches as a multiplication factor and is shown as follows like to be Figure 1.7:

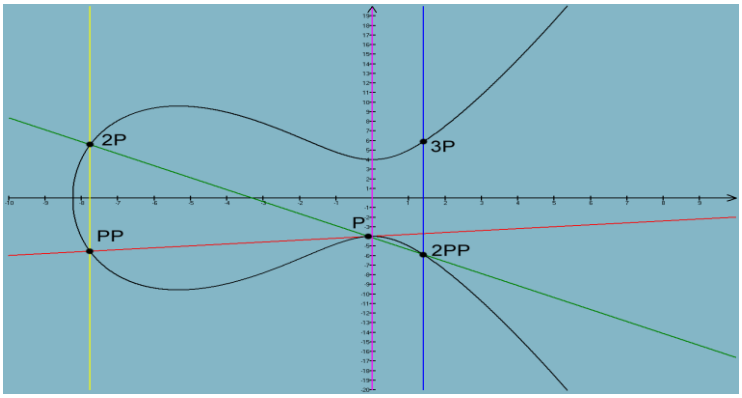


Figure 1.7: Elliptic Curve Graph Point Addition and Point Multiplication

The tripling of point P is like- $P + P + P$;, this is followed by first doubling and then applying point addition. As can be noted, this is how Elliptic Curve can be used to find discrete logarithms so quickly. This type of method is the leading method to generate the cryptography & cryptology on discrete log.

1.3 EXISTING ALGORITHMS WITH ITS RELATIVE COSTS

Motivation: For ECC algorithm, the key exchange and encryption-decryption procedure have been taken from [25]. From the research point of view, a number of procedures/algorithms have been applied, where the major consideration is in reducing the precomputed operation. The procedure for scalar multiplication $(Q = kP)$ is based on secret key k on prime field of $E_p(a, b)$ with the key that should take less than its chosen prime i.e. $k < p$. It is easy to calculate Q from k and P, but it is relatively hard to determine k on the given P and Q. For elliptic curve, this is known by discrete logarithm problem (DLP). Here, existing algorithms have been presented with its relative costs.

1.3.1 Scalar Multiplication using Most Significant Bit First Algorithm

The input to algorithm is a secret key k, converted into m bit binary for the purpose of scalar multiplication $Q = kP$. The initial computation starts from most significant bit (MSB) first, so it

needs to run a loop from second MSB i.e. m-2 to 0. In this algorithm, doubling always calls but addition only calls when the bit is 1. The MSB algorithm is:

1. Initial Assumption: Set $k = (k_{m-1} = 1, (k_{m-2}, k_{m-3}, \dots\dots\dots, k_0))$
2. Objective: Calculate $Q = kP$
3. Initially set up: $Q = P$
4. For $i = m - 2$ to 0
5. $Q = 2Q$
6. If $k_i = 1$ then
7. $Q = Q + P$
8. If end
9. For end
10. Return Q

For the complexity analysis, firstly m bit will always run for every bit, so there will be m point doubling. In second consideration, if m-bit is equal to 1 it runs its from 6 to 8, so on an average it counts half time 1 and half time 0, so average no. of point addition is $\left(\frac{(m-1)}{2}\right)$. The numerical explanation for scalar 7 and 31 is presented below:

7P	**31P**
$\mathbf{7P} = (\mathbf{2}(\mathbf{2}(\mathbf{P}) + \mathbf{P}) + \mathbf{P})$	$\mathbf{31P} = (\mathbf{2}(\mathbf{2}(\mathbf{2}(\mathbf{2P} + \mathbf{P}) + \mathbf{P}) + \mathbf{P}) + \mathbf{P})$

1.3.2 Scalar Multiplication using Least Significant Bit (LSB) first Algorithm

In algorithm a secret key k, converted into m bit binary for the purpose of scalar multiplication $Q = kP$. This algorithm works on two registers. The initial computation starts from least significant bit (LSB) first, so it needs to run a loop from 0 up to last bit i.e. 0 to m-1.

1. Set $k = (k_{m-1}, k_{m-2}, \dots, k_0), k_m = 1$
2. Calculate $Q = kP$
3. Initial Assumption $Q = 0, R = P$

4. For $i = 0\ to\ m - 1$
5. if $k_i = 1$ then
6. $Q = Q + R$
7. if end
8. $R = 2R$
9. For end
10. Return Q

For the complexity analysis, firstly for point addition only runs if m bit is equal to 1, so there is $\left(\frac{(m-1)}{2}\right)$ point addition. In second consideration, if m-bit is equal to 0 it counts in addition to doubling, so on an average of $\left(\frac{(m-1)}{2}\right)$ point doubling. In other words, one can say, an average of $m/2$ point addition and $m/2$ point doubling. Again, the numerical example for $7P$ and $31P$ are presented. For $7P, 7 = (111)_2$, computation steps are as follows: $Q = 0, R = P$

$$Q = Q + R = 0 + R = P, R = 2P$$
$$Q = P + R, R = 4P$$
$$Q = P + 2P + 4P, R = 8P$$

Computation of $31P$, $31 = (11111)_2$, $Q = 0, R = P$

$$Q = Q + R = 0 + R = P, R = 2P$$
$$Q = P + R = P + 2P = 3P, R = 4P$$
$$Q = 3P + 4P = 7P, R = 8P$$
$$Q = 7P + 8P = 15P, R = 16P$$
$$Q = 15P + 16P = 31P, R = 32P$$

MSB and LSB Comparisons

MSB	2P	3P	6P	7P	14P	15P	30P	31P
LSB	P	3P	7P	15P	31P			

There is substantial reduction in computation for LSB in terms of precomputation but there is extra cost in terms of one more register. But there is more scope of parallelism using LSB.

1.3.3 Montgomery Algorithm

Due to the side channel attack problem [as an extra source of information gain from physical implementations in the form of electromagnetic leakages, power consumptions, or sound] as suffered for LSM and MSB, an interesting variation has been created for scalar multiplication in point additions and point doublings, known by Montgomery Ladder algorithm. This algorithm contains the doubles and adds operations for each iteration of loop. It seems to be wasteful in energy saving (in computation costs) but the big advantage in regards the same to be most useful for resisting a side channel attacks.

Algorithm: Montgomery Ladder

1. $\boldsymbol{R_0 = P, R_1 = 2P}$
2. For $\boldsymbol{i = n - 2\ to\ 0}$

   2.1 $\boldsymbol{b \leftarrow 1 - k_i}$

   2.2 $\boldsymbol{R_b \leftarrow R_b + R_{kj}}$

   2.3 $\boldsymbol{R_{kj} \leftarrow 2R_{kj}}$
3. Return $\boldsymbol{R_0}$

The numerical example at $\mathbf{31P}$ below is satisfying the proposed algorithm:

$k = (11111)_2, n = 4$	$R_0 = P, R_1 = 2P$
$i = 3, k_i = 1, b \leftarrow 0$	$R_0 \leftarrow P + 2P, R_1 \leftarrow 2(2P)$
$i = 2, k_i = 1, b \leftarrow 0$	$R_0 \leftarrow 3P + 4P, R_1 \leftarrow 2(4P)$
$i = 1, k_i = 1, b \leftarrow 0$	$R_0 \leftarrow 7P + 8P, R_1 \leftarrow 2(8P)$
$i = 0, k_i = 1, b \leftarrow 0$	$R_0 \leftarrow 15P + 16P, R_1 \leftarrow 2(16P)$

1.3.4 Non-Adjacent Form (NAF)

The Non-Adjacent Form (NAF) is one of the other ways possibly to represent scalar $\boldsymbol{k}$ and computing- $\boldsymbol{kP}$, using the basis set $\{\mathbf{0}, \pm\mathbf{1}\}$. The negative coefficient also works well. The algorithm that is representing for k bits is as follows:

1. Initialize any value k for NAF
2. Initial NAF to be stored as an empty $S = ()$
3. While $(k > 0)$
4. If $(k\%2! = 0)$
5. then set $u = 2 - (k \pmod 4)$
6. else set $u = 0$
7. $k = k - u$
8. Assign u to S, as $S = u$
9. $k = k/2$
10. End of While Statement
11. Print S as an output

K	U	S
31		( )
32	-1	
16		(-1)
16	0	(0,-1)
8		
8	0	(0,0,-1)
4		
4	0	
2		(0,0,0,-1)
2	0	
1		(0,0,0,0,-1)
0	1	
		(1,0,0,0,0,-1)

This begins with the arithmetic value k which is an expansion of NAF. Its binary expansion says, due its algorithm, it expands k in the two nonzero consecutive coefficients, except of zero. The NAF has been explained at $(31) = (1, 0, 0, 0, 0, -1)$.

The algorithm of NAF works as follows:

1. Initial Assumption: Set $k = (k_{m-1}, k_{m-2}, \dots\dots\dots, k_0), k_m = 1$
2. Objective: Calculate $Q = kP$
3. Initially set up: $Q = P$
4. For $i = m - 2$ to 0
5. $Q = 2Q$
6. If $k_i = 1$ then
7. $Q = Q + P$
8. If $k_i = -1$ then
9. $Q = Q - P$
10. For end
11. Return Q

The complexity of this algorithm is presented later (at page 19). In a similar fashion a new algorithm is proposed in the below section.

1.3.5 $\tau - adic$ NAF

When an elliptic curve point is considered in NAF, it is known $\tau - adic$NAF. The algorithm for the same computes as follows:

1. Input $\mathbf{x_0}, \mathbf{y_0}$
2. Set $x = x_0, y = y_0$
3. Set $S \leftarrow ()$
4. While $x \neq 0$ or $y \neq 0$,
5. If x odd,
6. Then set $u \leftarrow 2 - (x - 2y(mod4))$
7. Else

8. Set $u \leftarrow 0$
9. Set $x \leftarrow x - u$
10. Prepend u to S
11. Set $(x, y) \leftarrow (y + (-1)^a\, x/2\,, -\frac{x}{2})$
12. End of while
13. Output S

This algorithm is applicable for evaluating the point on the curve (x, y) as $x = 9, y = 0$ (presented in Table 1.2) in the form of nonadjacent manner and it is not more complicated than integer addition.

Table 1.2: Computation on generalized NAF Algorithm

X	Y	U	S
9	0		( )
8	0	1	
4	-4		(1)
4	-4	0	
-2	-2		(0,1)
-2	-2	0	
-3	1		(0,0,1)
-2	1	-1	
0	1		$(-1,0,0,1)$
0	1	0	
1	0		$(0,-1,0,0,1)$
0	0	1	
0	0		$(1,0,-1,0,0,1)$

This method proves the average volumes of nonzero terms for τ-adic NAF's reduces up to 1/3. The argument presented is a speeded up in computation cost for elliptic curve scalar multiplication. But, it contains a drawback of this representation, and however this method still about twice as long as it's ordinary NAF and improvement in the same is a possible. Therefore a window method is one of possible way to reduce the complexity.

1.3.6 Window Method

This method aims to improve the performance of scalar multiplication on the reduction of precomputed operations on window widths w. This width maps the secret key into its width sizes. Since point doubling is comparatively more efficient than point addition, so reducing the point addition is one of the ways to optimize. Here the computation is based on decimal equivalent values on the reduced information; therefore, point's computation with reduced cost is possible by using this approach. For example, suppose scalar $k = (10\ 01\ 10\ 00\ 00\ 11)_2$ and with the window width 2, this scalar records as $(2\ 1\ 2\ 0\ 0\ 3)$ that consists of six windows. The below algorithm is representing the computation progression.

1. Initial Assumption: Set $k = (k_{m-1}, k_{m-2}, \dots\dots\dots, k_0)$
2. Objective: Calculate $Q = kP$
3. Initially set up: $Q = P$
4. For $i = m - 2$ to 0
5. $Q = 2Q$
6. If $k_i \neq 0$
7. If $k_i > 0$ then $Q = Q + P_{k_i}$
8. Else $Q = Q - P_{k_i}$
9. If end
10. For end
11. Return Q

The complexity of the algorithm is described ahead.

1.3.7 Sliding window method

Sliding window method [24] is a variation of above window method for scalar multiplication. Its complexity is slightly reduced by not counting the series of zero-'s' over the window method. For example, suppose scalar $k = (10\ 01\ 10\ 00\ 00\ 11)_2$ and with the window width 2, this scalar records as like $(1\ 00\ 3\ 0\ 0\ 0\ 0\ 0\ 3)_2$ that consists of the fewer required arithmetic point additions. The other well known algorithms are also available for the fractional width [18], [20], [25].

1.3.8 Radix 8 Scalar Multiplication

For Elliptic Curve Scalar Multiplication a new algorithm has been proposed in 2015 by Abdulrahman & Reyhani-Masoleh [30] on the basis of Radix 8 without pre-computed operations, with no addition and no doubling operations. This is reported to be one of the most optimized & reduced complexity on $log_8^{(k+1)}$ for this scheme. This is also enhancing the parallelism in the arithmetic field and point arithmetic. Table 1.3 shows a summary of relative complexities of the proposed algorithms.

Contribution 1: Because of the research gap, as analyzed from above proposed algorithms, we proposed a secure and efficient scheme for Elliptic curve scalar multiplication on Radix-16, in chapter 2. The specific contribution is summarized as follows:

(i) The theoretical computation cost is based on $log_{16}^{(k+1)}$. So, according to software performance enhancement it get improved by 6.25 % faster than previous proposed scheme and 8.33 % faster with respect to hardware perspective. We designed the hardware schematic which holds the security against safe-error fault attack and safe-error attack.

Table 1.3: Algorithms Complexities for Scalar Multiplication

Algorithm	**Complexity**
Most Significant Bit	k DBLs & $k/_2$ ADDs
Least Significant Bit	$k/_2$ DBLs & $k/_2$ ADDs
Montgomery Method	k DBLs & k ADDs + Side Channel Attack
Non-Adjacent Form (NAF)	$k/_2$ DBLs & $k/_2$ ADDs + Side Channel Attack
Window methods	$k/_{(w+1)}$ ADDs
Sliding window method	Escaping series of zero's on $k/_{(w+1)}$ ADDs
Radix-8 without Pre-Computations	$log_8^{(k+1)}$ without (ADDs & DBLs)

Contribution 2: We worked for scalar multiplication on prime based architecture of Edwards curve & extended Twisted Edwards curves on 4-processors and 8-processors, in chapter 3. The specific contribution is summarized as follows:

(i) We solved the Edwards Curves and twisted Edwards Curves problems on four and eight processors based on reduced computation cost from $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ on four processors and $2M + 3A$ to $2M + 2A$ on 8-processors, respectively. This has helped in accumulation on reduced clock cycles and providing resistance to the simple side channel attack.

1.4 NONCOMMUTATIVE CRYPTOGRAPHY

Motivation: The Noncommutative cryptography (NCC) shows the new research trends in the field of cryptography. Most of the cryptographic problems have been formulated on mathematics and physics. The generation of DLP for NCC is negligible to revert what have been considered to be a big advantage in this field. For the future security, commutative cryptography generalizes its advancement on the open opinion by not putting all the security protocols in one group, so NCC has been proposed. The objective is to cover the concepts of future security techniques based on original information should be hidden and its substituted equivalent ideas will be in the computing consideration, known to be Monomials generations. This opens various research problems and a new direction of future security to be uncovered through this field. This has enhanced it from the general group elements to equivalent substituted elements, known by the monomials generations for the cryptographic schemes. The group of orders is more challenging to assail like length based attack, automorphism, and brute-force attacks. Further, to improve the performance by using the following improvements like using memory, avoiding repetitions in process, look-ahead for future security, automorphism attacks and alternative solutions during the computation process that adds to the big advantages in the field of cryptography. The proposed security assumptions are intractable for the adversary and the attacks like length based, brute-force, automorphism, being negligible to revert back to the original information.

The issue related to the ring structure of the group elements, is one of the most motivational concern. A typical semi-ring structure, such as sparse matrices, showed the potential advantages towards a possible way to avoid the various attacks. The initial order for general and monomials [original parameters are hidden, and it provably equivalently participated in computation] structure on polynomial $\mathbb{Z}$-modular Noncommutative is the foundation, which is based on dihedral order 6 in a three dimensional matrix rings.

Contribution 3: We identified the behavior of Extra Special Group and applied it in cryptographic scheme which provides more robustness and unpredictability compared to all known proposed schemes of Noncommutative cryptography. The overall contribution is summarized as follows:

(i) It is based on a multidisciplinary scenario in an extra special group, on the cryptographic protocol regarding the key-exchange, encryption-decryption and authentication in four dimensional perspective. The key idea is based on a special case of prime order that is more resistant to the attacks and works on the bigger range of probabilistic theory and is based on random polynomial generation for the communicating parties.

(ii) Designed the mono-morphism group or ring element for minimum order of this group.

(iii) The basic length based attack on the group elements is stronger and challenging to assail on brute force attack.

1.5 SIGNCRYPTION

Motivation: A new paradigm 'Signcryption' for the public key cryptography is introduced that simultaneously fulfils both the functions of digital signature and public key encryption in a single step, and most important the cost for the both significantly lower than that required by the traditional "signature and encryption" approaches. This scheme is just like be killing two birds with one stone. When this has been simulated in the signcryption costs, it reduces 58% less in average computation costs time and 70.3% less in average communicational costs. The current status says that the existing algorithms need to signcrypt message with each of its intended recipient's public keys and send them separately to each one of them. This approach is redundant in terms of computational resource usage and bandwidth consumption. Aggregated signcryption has been proposed but it suffers with the Key Escrow problem. Finding the generalized formula for signcryption on reduced computational and communicational cost is our motivational issue on the basic considerations.

Contribution 4: The contribution significance works as follows (in chapter 5):

(i) This presents a procedural approach on protocol generation for a better, improved and stronger security on reduced costs. The basic primitives are applied on Diffie-Hellman and Elliptic Curve Cryptography. The purpose is proving the security properties for

protocol compositional logic that focuses on privacy rights in information assessment in multidisciplinary obligations.

(ii) We portrait a signcryption approach for password authenticated key exchange protocol for multilayer consensus, which logically combines individual signature and encryption cost in the form of reduced computational cost and communications cost in single stride of operation. The overall computation time potentially gets reduced for the proposed methodology on key generation and signature.

(iii) The results for ECC based multilayer consensus key generation approach are tested on Automated Validation of Internet Security Protocol Architecture (AVISPA) tool and SPAN tool.

(iv) Further, by preserving the definition of signcryption, we enhanced the same scheme in relation to the other proposed schemes.

1.6 PROXY RE-CRYPTOGRAPHY

Motivation: The proxy Re-cryptography has been proposed due to key escrow problem which has suffered in the public key infrastructure (PKI) for generating and maintaining the public keys for certificates distribution. In the key exchange process the secret key is held or stored by a third party in cryptography and is known by key escrow problem. This generally happens if proper precautions are not taken in to the consideration, during this the same key is compromising or original user(s) information is lost. The encrypted matter may be used to decrypt, and/or is allowing restoration of the primary matter to its unencrypted state. So in some way the third party involment is risky in escrow systems. The key escrow also enables us to provide a backup source for cryptographic keys:- where the modern cryptography is focusing on to solve the trust problem using the proxy re-cryptographic primitive as an interdisciplinary approach of computer science. A combined effort by Blaze, Bleumer, and Strauss in 1998 gained the credit to the idea for proxy re-cryptography. It has been further formalized by Ateniese and Hohenberger in 2005, which consists of two methods such as: proxy re-encryption and proxy re-signature. The goal of proxy re-encryption is to securely enable the re-encryption of cipher texts from one key to another, without relying on honest parties. Similarly, the goal of proxy re-signature is to securely enable the signature signed by one to transform a duly signed message without relying on trustworthy

parties. An enhanced proxy re-signature scheme was proposed in 2006 and also discussed its several potential applications related of the same. It was also predicted that proxy re-encryption and proxy re-signature will play an important role. Since then, researchers have sparked to throw more light in this area. That's how some excellently schemes have been proposed, like the IEEE P1363.3 standardization group is establishing the standard for proxy re-encryption, which will certainly give power for further researching in the field of proxy re-cryptography [3]. A semi-trusted is an entity to convert cipher texts addressed to those that can be decrypted by using some special information.

Contribution 5: The below Para (i) and (ii) significance is reflected in chapter 7, whereas Para (iii) is discussed in detail in chapter 8.

(i) In this a more optimized notion of signcryption with proxy re-cryptographic definition and its formal verification have been presented.

(ii) It is an innovative approach in the modern cryptography which works in two parts such as proxy re-encryption and proxy re-signature, where a semi-trusted proxy can translate one ciphertext to another ciphertext for the same plaintext using encryption and signature algorithms.

(iii) This presents an application oriented work for Telemedicine using ECC without precomputation on Radix-8 scalar multiplication. The reason to cover is to lead and apply on track in a fascinating area of ECC on a smaller key size to be applicable for various applications on a same level of security strengths.

1.7 PERFORMANCE EVALUATION PERSPECTIVE ON DEFINED PROBLEMS

The evaluation strategy varies from problem to problem such as scalar multiplication complexity consideration for Radix-16, Edward's curves and twisted Edward's curves. The main focus is to accelerate the performance of Elliptic Curve Cryptography. Chapters 2 and 3 have been based on these issues for better performance to the existing approaches. Chapter 4 contains the identified behavior of Extra Special Group for the cryptographic schemes with more robustness for the

known schemes of Noncommutative Cryptography. The length based attack to this group of elements is negligible in achieving the corresponding secret key.

1.8 DESIGN POLICY

Motivation of design policy is the efficient implementations of algorithms. In general, it has been considered to be optimal on security strength, performance achieving on low cost and its mathematical model (complex preferred). These should be simple enough for scalar multiplication methodology on how to record the Discrete Logarithmic Problem (DLP) for its novel significance. The DLP for scalar k is computationally infeasible the original scalar key to revert back. The main reason is to enhance the computational efficiency in relation to the proposed algorithms for scalar multiplication techniques. We elaborate the same from radix-8 scalar multiplication and obtain a lot of special benefits.

Public key protocols on elliptic curves over finite fields are becoming increasingly a common problem for discrete-logarithmic implementation that are based on it. Protocols on elliptic public-key are based on scalar multiplication, and the cost of executing such depends mostly on the complexity of the scalar multiplication operation. Elliptic scalar multiplication is analogous to exponentiation in the multiplicative group of integers where various techniques using memory and computations have been proposed to speedup modular exponentiation.

The get a more efficient improvements in the elliptic cases are available with modular exponentiation, these are generally considered in three kinds:

1. Choosing the curve is the base field over which it is generalized, where efficiency of scalar multiplication is considered. Where one might choose the field of modulo integers, the case for modular reduction is more efficient. This is only applicable for ECC but the RSA option is not available.
2. Subtraction is just similar and efficient as addition. The elliptic scalar multiplication analogous procedure uses a sequence of addition and doublings of points. This is one of the procedures that involves a sequence of squaring and multiplication that is based on the binary expansion of values.
3. Complex multiplication is one of the major roles so that cryptanalysis is difficult to decipher. A finite field for every elliptic curve equipped with a set of operations as scalar

multiplication on integers. The carried operations can be efficiently uses a family of elliptic curves, which they can to utilize in various ways to increase the efficiency of elliptic scalar multiplication.

Objective of the design policy is to use elliptic curve using polynomial and normal basis as part of cryptographic technique that can be implemented efficiently and securely on the various applications such as internet banking, smart cards applications, and a lot of real life applications. The cryptographic technique, which can be implemented, should be immune to internal attacks and should be secure in a theoretical sense of computational complexity, and external attacks as side channel attacks. In addition, its operations should be executable within practical time and possible implementation on limited resources. The below requirements for the cryptographic techniques to work are as follows:

(i) It should be secure enough so that it becomes very difficult or is immune to cryptanalysis, which is known as side channel attack.

(ii) It should be as secure as the traditional elliptic curve cryptosystems in exceptional way.

(iii) It should be as fast as the traditional elliptic curve cryptosystems are and must be desirable.

(iv) The requirement of software in the form of code should be less and memory requirement in case of hardware should be smaller during execution.

CHAPTER 2

SECURE AND EFFICIET ECC: RADIX-16 SCALAR MULTIPLICATION WITHOUT PRE-COMPUTATION

The widely used Elliptic curve cryptography (ECC) is playing a crucial role and contributing a bigger significance with its related benefits in security and performance advancements almost it is applicable for all high end applications. The scalar multiplication algorithms used in ECC are having the scope for gaining the computational efficiency. A smaller key length is the most appropriate for receiving the same level of security strength using this technique. Finding more efficient technique for accelerating the scalar multiplication through the research gap is one of the prior objectives. This chapter claims the proposed Radix-16 scalar multiplication without pre-computed operations, -which is theoretically computing 6.25 percent faster than the recently proposed Radix-8 scalar conversion technique on software performance basis and 8.33 percent on hardware basis. This is showing more appropriateness for reduced instruction set computing with resistance to the safe-error fault attacks and simple side channel attacks. The further extension of proposed work is to find the future application scope for low memory devices.

2.1 INTRODUCTION

Cryptography is a discipline of computer science that is based on the mathematical foundation which leads to enforce security for the applications. The used data security techniques/ algorithms are playing an important role for several relevant applications in the field of security. Cryptographers have proved the matured behaviors at the number of stages. But in preference to this still the various necessities are remained for performance enhancement and system security services that are considered to be the motivational issues in this field. The general practical applications are the thought to protect secret information to disclosure through any of the algorithms; authenticity guaranteed of data and secured message transmission at ends [11].

Diffie and Hellman were first abled to give the public key cryptography (PKC) thought in 1976 [12]. After the same, varieties of PKC's algorithms have been developed on the considerable performance and efficiency improvement, but Elliptic Curve Cryptography (ECC) in all of them has attracted the most attentions. Various algorithms have been considered to be more secure other than ECC, but they need a higher length of key. The increased length in computation does not suite low memory devices. ECC on a shorter key lengths offers the same level of security and better performance. But, the current stage for computational performance is still to be large considered in research, and improvements in the same are possible and it is our motivational issue [13]. The cost of computation has been minimized with the new advanced approaches in overall consideration.

Discrete Logarithmic Problem (DLP) is the heart of cryptography that plays a crucial role in information exchange and contains most of the security concerns. Due this reason, information security is a fascinating area of high computational speed at lower cost and keeps greater significance when passes through the medium. For an efficiently make it to be available for security, the security algorithms used in the field are playing a crucial role. The used algorithms with slow processing put have been ranked low on customer satisfaction and convenience. The fast running algorithms are impacting with high performance and high-speed. These are better leading the security concerns in computations and communication costs. ECC-DLP computation is based on two elliptic points P and Q on the curve, to find the value of k (generally secret key), such that $Q = kP$, which is the core building block in PKC [14]. It evaluates the same on scalar using repeated point doubling (DBL) and point addition (ADD) operations. If this proceeds in the forward direction it is known as scalar multiplication that behaves like negligible to revert back to secret key k.

The three main approaches are working a backbone for the scalar multiplication. The first approach is the underlying finite-field operation based on prime or binary field arithmetic. The second approach uses the algorithms that depend on the scalar representation for scalar multiplication, which decides their computation cost (with respect to its complexities). Some of the existing algorithmic representations are in Most Significant Bit (MSB) first, Least Significant Bit (LSB) first, Nonadjacent form (NAF), Window Method, Sliding Window Method, Width Nonadjacent Form [15], Frobenious Map [16], [17], [18] and Radix-rNAF (r-NAF) [19]. Third

approach uses more hardware support in reducing pre-computation and/or utilization of memory uses, and/or paralleling operations [20]-[23], and/or applying pipelining approaches [24].

In the present work, we have combined the above two approaches in parallel in correlation to the third approach to get an efficient scalar multiplication algorithm. Overall it works are as follows:-

- To extend radix-8 scalar multiplication work for the radix-16 scalar multiplication scheme. This shows that the computation cost is shorter and enhances its performance by 6.25 percent, regarding the computational enhancements, using this scheme and on hardware perspective it improves by 8.33 percent. This is also to in generic considered and no memory pre-computed operations are required during this process.
- To analyze the hardware, for each digit sets variables, dependency graph for Radix-16.
- Finally, to analyze safe-error fault and simple side channel attacks (SSCAs) attacks against the security.

For this chapter, the organization is as follows; section 2.1 presents research gap on computational complexities for scalar multiplication on the various cases. Section 2.2, the radix-r method introduces scalar multiplication recordings, and further be generalized on radix-*r* method especially for radix-16. The numerical foundation is given to justify the proposed approach and needed hardware support, section 2.3 as a dependency graph for all digit set elements is discussed, to propose the architecture for Radix-16. It highlights the advantages of radix-16 with resisting against safe-error fault attacks and simple side channel attacks (SSCAs). The section 2.4, performance analyzed and compared the efficiency of scalar multiplication on some parameters. Instead of that, we have analyzed the performance on hardware and software.

2.2 PRELIMINARIES

2.2.1 Complexities Cases for Scalar Multiplication

ECC algorithm is a hierarchy of operations which is structured in different levels and levels are interrelated to each other. As depicted in Figure 1.1 (*previous chapter*), level 0 is the highest level where ECC algorithm facilitates for scalar point multiplication as kP and this kP ensures in group operations as DBLs and ADDs, and finally these two group operations depend on the

finite field arithmetic operations in multiplication M, Addition A, Subtraction S, Inversion I, and Squaring Sq. For one point ADDs and for one point DBLs operation the required pre-computed operations are 13,617 and 14,000 clock cycles [25], as have been observed on star core 41000 series processor.

The architecture of ECC has been parallelized to improve the system performance on reduced pre-computed operations; the used algorithms have also done the same. This is also our motivational issue. Here a simple thought is given about the known algorithms and its considered computational complexities. Let k is scalar, suppose scalar is represented in m bit binary, according to the Most Significant Bit (MSB) first algorithm it requires m bits doubling (DBLs) and on average $m/2$ bits of addition (ADDs) operations. Similarly, for Least Significant Bit (LSB) algorithm it requires on average $m/2$ bits of ADDs and same bits of DBLs. An another variation in algorithm as a non-adjacent form (NAF), its representation in $\{-1, 0, 1\}$, still in this case, on average $m/2$ bits of ADDS and $m/2$ bits of DBLs, and in addition to this it is resistant against the side-channel attacks [26]. The complexity of w-NAF keeps $m/(w+1)$ in point ADDs only [27]. A variation of w-NAF does in sliding w-NAF, also known by Frobenious operations, that escapes the series of zeros during the scalar multiplication, which counts the enhancement in scalar multiplication (SM) [28]. Also, the hamming-weight is another name which counts its run time complexity in a reduced form for scalar representation.

ECC construction is secured considered according the data released from NIST-2012 guidelines on some certain keys length. Its conceptual point of view, shorter keys for ECC most favor to the short-memory devices in its appropriateness. The real life applications devices for secure and efficient implementations are based on internet banking, smart cards, mobile banking, etc. The exceptional functionality has also been considered through the various advanced techniques that may not escort to any leakages on real-time applications [29]. Abdulrahman and Masoleh in [30] have proposed a model against the SSCAs & safe-error fault attack. They have shown through the schematics dependency any new introduced thing is identified and is resulted in an incorrect SM, as is proposed on Radix-8 scalar multiplications.

Finding the more efficient technique for accelerating the scalar multiplication in Elliptic Curve Cryptography (through the series of identified research gap) is one of our major objectives, and establishes the same in more appropriateness with resistance to side channel attacks and safe-error fault attacks. Therefore, the novel contribution (in chapter 2) is based on

the proposed algorithm of Radix-16 scalar multiplication, which is established on computation cost at $\log_{16}^{(k+1)}$. Compare to recently proposed Radix-8 scalar multiplication algorithm [30] from the implementation point of view, the software performance gets an acceleration on proposed methodology with the basic difference's in its base or its computation cost on (1/8 to 1/16) in %=6.25%, and in a similar fashion with respect to hardware implementation on its computation cost (basis (1/3 to 1/4) in %)=8.33% accelerated.

2.3 PROPOSED RADIX-16 RECORDING TECHNIQUE

This section proposes radix-16 scalar multiplication methodology on how to record the Discrete Logarithmic Problem (DLP) for novel significance, that is being in the range of $[-1,14]$. The DLP for scalar k is computationally infeasible to the original scalar to revert back. The main reason of covering is to enhance the computational efficiency in relations to the proposed algorithms for scalar multiplication techniques. We elaborate the same from radix-8 scalar multiplication and a lot of special benefits are observed.

2.3.1 General Expansion Technique For Scalar k

As the scalar generalizes for scalar multiplication on high radix, an implicit condition to base r is a power of 2, i,e., $r = 2^w$, where- $2 \leq w \leq m-1$, as presented in [30]. This emphasizes the scalar multiplication rP needs only repeated DBLs, where an elliptic point on the curve is P. The scalar k of lengths m-bits are partitioned into l digits as $l = \lceil \frac{m}{w} \rceil$ to as a signed-representation, and let each digit for scalar k as k_i' for $0 \leq i \leq l-1$. The radix-r expansion on scalar k, as $(k_{l-1}', \ldots, k_1', k_0')_r$, where $k_i' \in \{0,1, \ldots\ldots, r-1\}$ for every $i \leq l-1$, represented as in (4):

$$k = \sum_{i=0}^{l-1} k_i' r^i, k_i' \in \{0,1, \ldots\ldots, r-1\} \quad (4)$$

The process to compute the scalar multiplication kP computes in (5):

$$kP = \sum_{i=0}^{l-1} k_i' r^i P. \quad (5)$$

An abelion group with $E(F_q)$ is an identity 'O, let $P \in E(F_q)$ be an input point. The computation of scalar point multiplication kP, must also be a point in $E(F_q)$, i,e $kP \in E(F_q)$. Let kP and P_1 be two points on the curve, which are initialized by 'O and P. Then to define a point for scalar k as:

$$P_{kP}^{j} = \sum_{i=0}^{j} k_i' r^i P, \text{ for any } 0 < j < l. \quad (6)$$

On equation (5) and (6) comparision, the scalar $kP = P_{kP}^{l-1}$ one can observe, so to expose the upper j^{th} part from (6), one can get

$$P_{kP}^{j} = k_i' r^i P + P_{kP}^{j-1}. \quad (7)$$

Now to define the auxiliary point in (8) as:

$$P_{ACC}^{(j)} = r^j P, \quad (8)$$

It is another auxiliary point that initializes to P, i,e., $P_{ACC}^{(0)} = r^j$. Substituting this in (7), one acquires P_{kP}^{j} as:

$$P_{kP}^{j} = k_j' P_{kP}^{j} + P_{kP}^{j} \quad (9)$$

Now, essentially to run the algorithm a recursive point is:

$$P_1^j = r^{j-1} P - P_{kP}^{j} \quad (10)$$

The computational procedure for each input scalar k_i', P_{kP}^{j} and P_1^j the two recursive points are obtained properly either from SUB or ADD operations.

Lemma 1. Consider input scalar represented k_j' be in the range of- $[1,\ l-1]$, and $0 \le k_j' \le r-1$, then P_{kP}^{j}, can be defined in one of the following two ways:

$$P_{kP}^{j} = \begin{cases} P_{kP}^{j-1} + k_j' P_{ACC}^{j} \\ r P_{ACC}^{j} - P_1^j \end{cases} \quad (11)$$

and P_1^j is defined as follows:

$$P_1^j = \begin{cases} r P_{ACC}^{j} - P_{kP}^{j} \\ (r - 1 - k_j') P_{ACC}^{j} + P_1^{j-1}, \text{ where } P_{kP}^{j} = r^j P = r P_{ACC}^{j}. \end{cases} \quad (12)$$

The Lemma 1 proof is explained Appendix 1.

2.3.2 Recording the Scalar k into Signed Radix-16

The scalar multiplication for proposed algorithm is first recorded in the form of non-fifteen encoding representation. It is based on input scalar k assumed in decimal, converted in hexadecimal and stored in register- $a[k_j]$, where $a[k_j] \in \{0,1,2,3,4,5,6,7,8,9, A \leftarrow 10, B \leftarrow 11, C \leftarrow 12, D \leftarrow 13, E \leftarrow 14, F \leftarrow 15\}$ and adjoined one extra digit (signed) next to most significant position. A sequence counter (SC) acts as temporary holding for all digits set

elements in register - $\boldsymbol{a[k_j]}$**.** Now for all $\boldsymbol{a[k_j]}$ scan from right-to-left, by setting j=0 represents the LSB first. If bit $\boldsymbol{a[k_j] = F}$ from the set it is replaced the same by -1, and added +1 as a carry to next digit, 'if not it is' digits are only recorded as passed, and it is continued until SC reached zero. In this case, storing register is also $a[k_j]$. Now register $a[k_j]$ for any scalar k is available in recordings from $\{-1, 0, \dots, 14\}$, in Figure 2.1. The basic idea has been described in Parhami [31] and its related radix analysis is representation in [32].

2.3.3 Proposed Radix-16 Algorithm for Scalar Multiplication

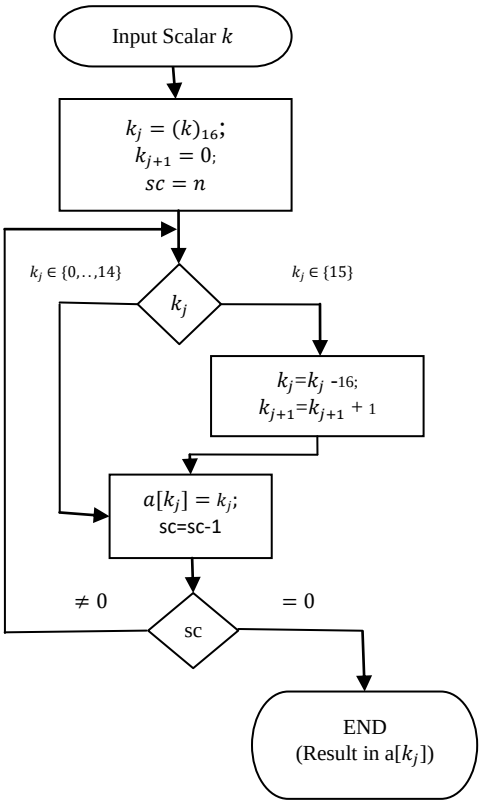


Figure 2.1: Algorithm of Proposed Non-Fifteen Encoding

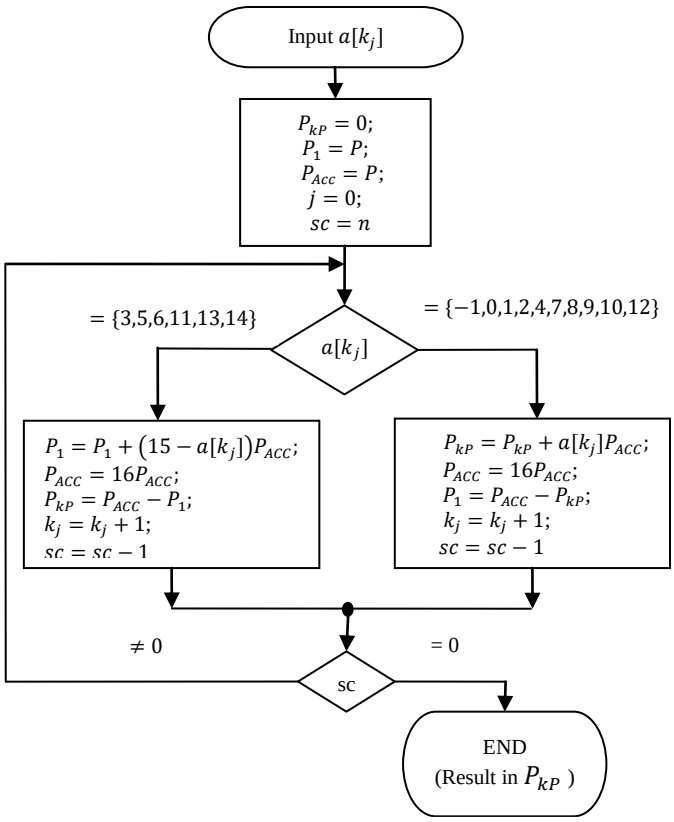


Figure 2.2: Algorithm of Proposed Signed Radix-16 Scalar Multiplication

After a non-fifteen encoding representation stored in register $a[k_j]$ has now been used to do the scalar multiplication, as according to the algorithm described in Figure 2.2. For the same, Lemma 1 is extended by setting all the digit set values either to P_{kP} or P_1, is one of the core part. The maximum Hamming weight for each digit set- k_j for scalar computation P_{kp}, as first group added in (13)

$$P_{kP}^{j} = \begin{cases} P_{kP}^{j-1} + a[k_j]P_{ACC}^{j}, & if\ a[k_j] \in \{-1,0,1,2,4,7,8,9,10,12\} \\ 16P_{ACC}^{j} - P_1^{j}, & if\ a[k_j] \in \{3,5,6,11,13,14\} \end{cases} \quad (13)$$

And for P_1 in a similar way with a maximum of $(15 - a[k_j])$ added in (14)

$$P_1^{j} = \begin{cases} 16P_{ACC}^{j} - P_{kP}^{j}, if\ a[k_j] \in \{-1,0,1,2,4,7,8,9,10,12\} \\ (15 - k_j^{'})P_{ACC}^{j} + P_1^{j-1},\ if\ a[k_j] \in \{3,5,6,11,13,14\} \end{cases} \quad (14)$$

For P_{kP} at this point, P_{ACC} repeated implicitly after every digit set by an update in- $P_{ACC} = 16P_{ACC}$. Now, according to the register digit set, we have done the computation as follows for $a[k_j] \in \{-1,0,1,2,4,7,8,9,10,12\}$:

$$\begin{cases} P_{kP} = P_{kP} + a[k_j]P_{ACC} \\ P_{ACC} = 16P_{ACC} \\ P_1 = P_{ACC} - P_{kP} \end{cases} \quad (15)$$

And for digit set $a[k_j] \in \{3,5,6,11,13,14\}$ it follows the operation as:

$$\begin{cases} P_1 = P_1 + (15 - a[k_j])P_{ACC} \\ P_{ACC} = 16P_{ACC} \\ P_{kP} = P_{ACC} - P_1 \end{cases} \quad (16)$$

The scalar multiplication algorithm given for Radix-16, as shown in Figure 2.2, computes scalar multiplication for any of the elliptic point P. In reference to computation cost t for scalar k, it can define its cost- $t = \lceil log_{16}k \rceil + 1$, whereas for radix-8 its cost is $t = \lceil log_8 k \rceil + 1$.

To start computation based on three registers such as $P_{kP} = 0$, $P_1 = P$, $P_{ACC} = P$ as an initial assumptions and sequence counter to total number of digits in non-fifteen encoding. Register valued now been scanned from right-to-left i.e., the least significant bit first as $k_j = 0$ up to most significant bit. The algorithmic procedure calls until SC reaches zero, the scalar multiplication result of P_{kP} returned as output.

Table 2.1: Numerical example of scalar multiplication using Radix-16

Digit Set	**Initialization**	**(Iteration from Right-to-Left)**					
		SC=6, $a[k_j] = 5$	SC=5, $a[k_j] = 7$	SC=4, $a[k_j] = \bar{1}$	SC=3, $a[k_j] = 6$	SC=2, $a[k_j] = 1$	SC=1, $a[k_j] = 0$
$\mathbf{a[k_j]} \in \{-1,0,1,2,4,7,8,9,10,12\}$	$P_{kP} = 0$; $P_1 = P$; $P_{Acc} = P$		$P_{kP} = 117P$ $P_{Acc} = 256P$ $P_1 = 139P$	$P_{kP} = -139P$ $P_{Acc} = 4096P$ $P_1 = 4235P$		$P_{kP} = 89973P$ $P_{Acc} = 1048576P$ $P_1 = 958603P$	$P_{kP} = 89973P$ $P_{Acc} = 16777216P$ $P_1 = 16687243P$
$\mathbf{a[k_j]} \in \{3,5,6,11,13,14\}$		$P_1 = 11P$ $P_{Acc} = 16P$ $P_{kP} = 5P$			$P_1 = 41099P$ $P_{Acc} = 65536P$ $P_{kP} = 24437P$		

Here proposed algorithm is justifying through the use of numerical example. The assumed scalar $k = 89973$ and its hexadecimal representation is- $(15F75)_{16}$. Again, it is represented in non-fifteen representation as- $(016\bar{1}75)$. Table 2.1 is a representation of proposed signed radix-16 scalar multiplication. On the three registers, the loop started and is executed t in times, i.e., that is $t = \lceil log_{16}89973 \rceil + 1 = 5$. Whereas the same problem is solved using radix-8 scalar multiplication procedure but the complexity is relative higher. Therefore, to derive the theoretical speedup is in 6.25% faster in computation costs on proposed methodology, with relative to radix-8 regular scheme of elliptic curve scalar multiplication methodology for each digit sets.

Table 2.2: Scalar Bits Processing Stages

$a[k_j]$	Processing Stages	$a[k_j]$	Processing Stages
-1	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_{kP} = P_{kP} - P_{ACC}$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$	7	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_{ACC} = P_{Temp} - P_{ACC};$ $P_{kP} = P_{kP} + P_{ACC}; P_{ACC} = 2P_{Temp};$ $P_1 = P_{ACC} - P_{kP}$
0	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_{kP} = P_{ACC} - P_1;$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$	8	$P_{ACC} = 2P_{ACC}; P_{ACC} = 2P_{ACC};$ $P_{ACC} = 2P_{ACC}; P_{kP} = P_{kP} + P_{ACC};$ $P_{ACC} = 2P_{ACC}; P_1 = P_{ACC} - P_{kP}$
1	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_{kP} = P_{kP} + P_{ACC}$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$	9	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_{kP} = P_{kP} + P_{ACC}; P_{ACC} = 2P_{Temp}$ $P_1 = P_{ACC} - P_{kP}$
2	$P_{ACC} = 2P_{ACC}; P_{Temp} = 2P_{ACC};$ $P_{Temp} = 2P_{Temp}; P_{kP} = P_{kP} + P_{ACC}$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$	10	$P_{ACC} = 2P_{ACC}; P_{Temp} = 2P_{ACC};$ $P_{Temp} = 2P_{Temp}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_{kP} = P_{kP} + P_{ACC}; P_{ACC} = 2P_{Temp}$ $P_1 = P_{ACC} - P_{kP}$
3	$P_{ACC} = 2P_{ACC}; P_{ACC} = 2P_{ACC};$ $P_{Temp} = 2P_{ACC}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_1 = P_1 + P_{ACC}; P_{ACC} = 2P_{ACC};$ $P_{kP} = P_{ACC} - P_1$	11	$P_{ACC} = 2P_{ACC}; P_{ACC} = 2P_{ACC};$ $P_{Temp} = 2P_{ACC}; P_1 = P_1 + P_{ACC};$ $P_{ACC} = 2P_{Temp}; P_{kP} = P_{ACC} - P_1$
4	$P_{ACC} = 2P_{ACC}; P_{ACC} = 2P_{ACC}$ $P_{Temp} = 2P_{ACC}; P_{kP} = P_{kP} + P_{ACC}$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$	12	$P_{ACC} = 2P_{ACC}; P_{ACC} = 2P_{ACC};$ $P_{Temp} = 2P_{ACC}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_{kP} = P_{kP} + P_{ACC}$ $P_{ACC} = 2P_{Temp}; P_1 = P_{ACC} - P_{kP}$
5	$P_{ACC} = 2P_{ACC}; P_{Temp} = 2P_{ACC};$ $P_{Temp} = 2P_{Temp}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_1 = P_1 + P_{ACC}; P_{ACC} = 2P_{Temp};$ $P_{kP} = P_{ACC} - P_1$	13	$P_{ACC} = 2P_{ACC}; P_{Temp} = 2P_{ACC};$ $P_{Temp} = 2P_{Temp}; P_1 = P_1 + P_{ACC};$ $P_{ACC} = 2P_{Temp}; P_{kP} = P_{ACC} - P_1$
6	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{ACC};$ $P_{Temp} = 2P_{ACC}; P_{ACC} = P_{ACC} + P_{Temp};$ $P_1 = P_1 + P_{ACC}; P_{ACC} = 2P_{Temp};$ $P_{kP} = P_{ACC} - P_1$	14	$P_{Temp} = 2P_{ACC}; P_{Temp} = 2P_{Temp};$ $P_{Temp} = 2P_{Temp}; P_1 = P_1 + P_{ACC};$ $P_{ACC} = 2P_{Temp}; P_{kP} = P_{ACC} - P_1$

Experimental result verification in C programming in comparison to Radix-8 and Radix-16 scalar multiplication is available in Appendix 2 at page no. 148.

2.4 PROPOSED PROCESSING STAGES AND HARDWARE ARCHITECTURE FOR RADIX-16

The processing states are based on initial assumptions, such as $P_{kP} = 0, P_{ACC} = P, P_1 = P$, where P is an elliptic point on the curve. The states P_{ACC}, P_1 and P_{Temp} work as temporary holding registers. In Table 2.2, a computational procedure aspect is considered for all digit set elements. Further, Table 2.3 is representing processing sequence as like to suggested in Table 2.2. In general, each digit sets belong to a group-1 $\in \{-1,0,1,2,4,7,8,9,10,12\}$ or group-2 $\in \{3,5,6,11,13,14\}$, the only purpose is to evaluate the scalar multiplication P_{kP} and resulting state-1 or resulting state-2 store the final result.

Table 2.3: Digit Sets Processing Sequence

Digit Sets	$P_{kP} = 0;$ $P_{ACC} = P;$ $P_1 = P;$	(i)		(ii)		(iii)		(iv)	Group	**Resulting state-1**			**Resulting state-2**		
		P_{ACC}	P_{Temp}	P_{ACC}	P_{Temp}	P_{ACC}	P_{Temp}	P_{ACC}		P_{kP}	P_{ACC}	P_1	P_1	P_{ACC}	P_{kP}
-1	〃		2P		4P		8P		1	-P	16P	17P			
0	〃		2P		4P		8P		1	0	16P	16P			
1	〃		2P		4P		8P		1	P	16P	15P			
2	〃	2P			4P		8P		1	2P	16P	14P			
3	〃	2P		4P			8P	12P	2				13P	16P	3P
4	〃	2P		4P			8P		1	4P	16P	12P			
5	〃	2P			4P		8P	10P	2				11P	16P	5P
6	〃		2P		4P		8P	9P	2				10P	16P	6P
7	〃		2P		4P		8P	7P	1	7P	16P	9P			
8	〃	2P		4P		8P			1	8P	16P	8P			
9	〃		2P		4P		8P	9P	1	9P	16P	7P			
10	〃	2P			4P		8P	10P	1	10P	16P	6P			
11	〃	2P		4P			8P		2				5P	16P	11P
12	〃	2P		4P			8P	12P	1	12P	16P	4P			
13	〃	2P			4P		8P		2				3P	16P	13P
14	〃		2P		4P		8P		2				2P	16P	14P

2.4.1 Hardware Dependency Graph

Using the hardware support we created hardware schematics for scalar multiplication in support of all digit set elements, as like to be shown in Figure 2.3. The dependency graph is designed on the basic consideration for each digits, it contains terminologies and processing sequences. Each terminologies used in the same represents its meaning, such as Sel represent either to pick P_{kp} or P_1. CTR is control option and it is an indication for SUB or ADD operations. Where, output1 or output2 is a register, guides to store result for digit set either from group-1 or group-2 elements. Table 2.4 is an indication for the evaluation sequence for each case of digit set $a[k_j]$ with an indicated Sel, CTR, Output1 or Output2 associated with the dependency graph from Figure 2.3(a)-to-(j), respectively. The scalar multiplication result for digit set $\in \{-1,0,1,2,4,7,8,9,10,12\}$ hold on output1 and digit sets $\in \{3,5,6,11,13,14\}$ hold on output2.

The computation of SM at register set -1 progresses by Sel selects P_{kP}, and this digit stuffed to Group-1, so to compute (12) as- $P_{kP} = P_{kP} + a[k_j] * P_{ACC} = (-1)P$. The computed result stored at output1. Control of CTR manages the SUB operation. A similar idea is specified for another register set elements in table 2.4 with its dependency depicted in Figure 2.3.

The elliptic operation is in general depends on a sequence of DBLs and ADDs/SUBs. The complete dependency graph for all register set elements has been shown through Figure $2.3(a) – to – (j)$. Here an analysis is presented for digit set elements at -1 and 0. The access of P_{kP} at digit set for -1 requires the processing $P_{kP} - P_{ACC}$, hence, the SUB is equivalent to a ADD operation in computer as a 2's complement addition. The dependency graph is shown at five stages are evaluation is written in below (Note: concrete figure for five stages has been shown in Figure 2.4 for all register set elements):

$$\text{Stage 1: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 2: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 3: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 4: } P_{kP} = P_{kP} - P_{ACC};\ P_{ACC} = 2P_{Temp};$$

$$\text{Stage 5: } P_1 = P_{ACC} - P_{kP}$$

A second example for 0 digit set, in general the evaluation of P_{kP} doesn't require processing. But, to keep the scheme consistent in relation to other cases, it re-evaluate P_{kP} by doing the following operation at $P_{kP} = P_{ACC} - P_1$. The P_{kP} and P_1 are always preserved due this reason.

Table 2.4: Scalar Multiplication at Digit Sets

Figure No	$a[k_j]$	Sel	CTR	Output1	Output2
Figure 2.3(a)	-1	P_{kP}	ADD	$P_{kP} = (-1)P$	
	0	P_{kP}	SUB	$P_{kP} = (0)P$	
	1	P_{kP}	ADD	$P_{kP} = (1)P$	
	14	P_1	ADD	$P_1 = (2)P$	$P_{kP} = (14)P$
Figure 2.3(b)	2	P_{kP}	ADD	$P_{kP} = (2)P$	
	13	P_1	ADD	$P_1 = (3)P$	$P_{kP} = (13)P$
Figure 2.3(c)	3	P_1	ADD	$P_1 = (13)P$	$P_{kP} = (13)P$
Figure 2.3(d)	4	P_{kP}	ADD	$P_{kP} = (4)P$	
	11	P_1	ADD	$P_1 = (5)P$	$P_{kP} = (11)P$
Figure 2.3(e)	5	P_1	ADD	$P_1 = (11)P$	$P_{kP} = (5)P$
	10	P_1	ADD	$P_{kP} = (10)P$	
Figure 2.3(f)	6	P_1	ADD	$P_1 = (10)P$	$P_{kP} = (6)P$
Figure 2.3(g)	7	P_{kP}	ADD	$P_{kP} = (7)P$	
Figure 2.3(h)	8	P_{kP}	ADD	$P_{kP} = (8)P$	
Figure 2.3(i)	9	P_{kP}	ADD	$P_{kP} = (9)P$	
Figure 2.3(j)	12	P_{kP}	ADD	$P_{kP} = (12)P$	

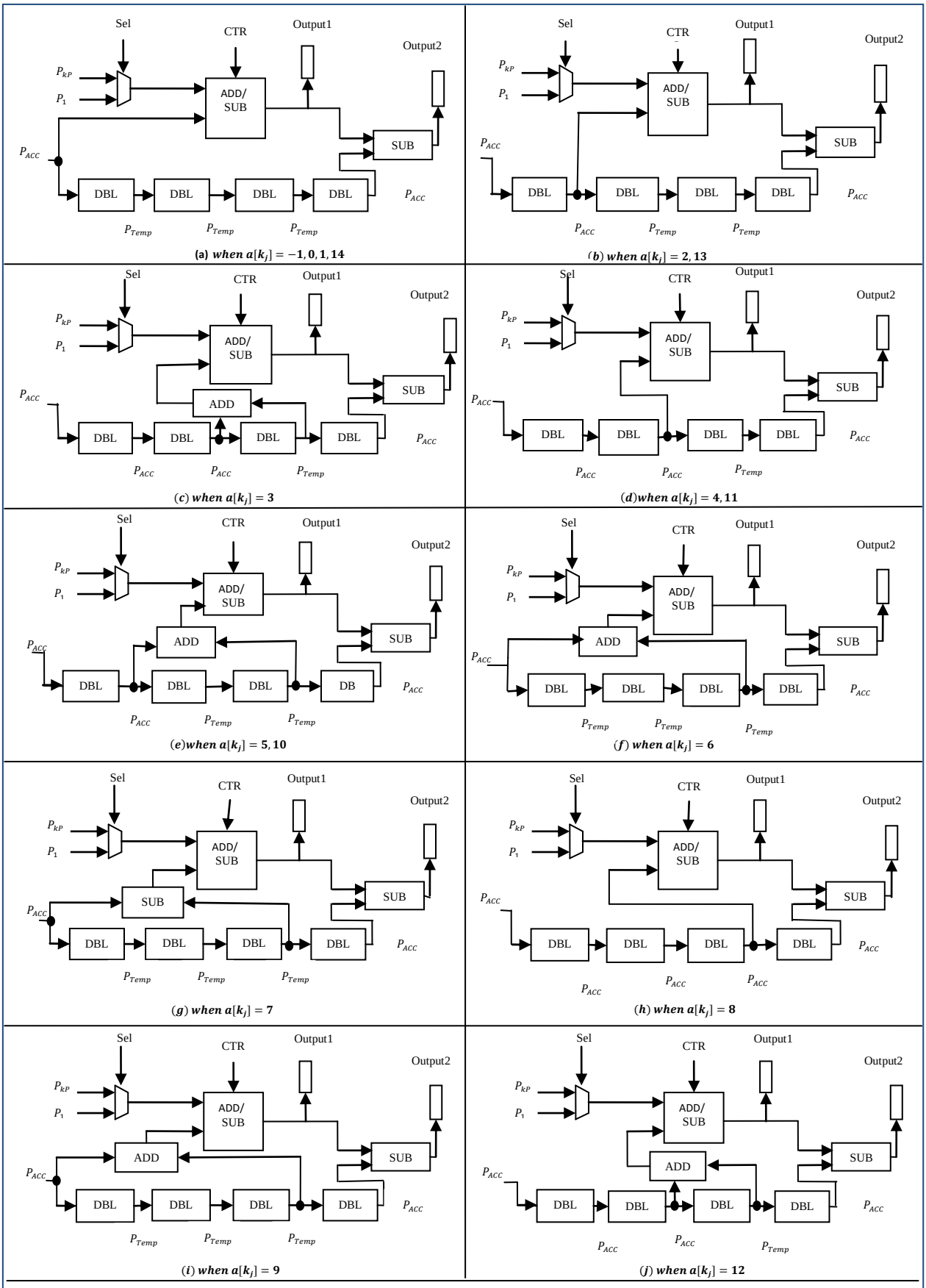


Figure 2.3: Hardware Radix-16 Dependency Graph for Digit Sets

In addition, the remaining parameters are also being considered in consistent. It is observed for all cases it doesn't affect the evaluation sequence of scalar multiplication- kP at any stage, and hence no rash to introduce a dummy operation, so it is considered to be from the safe-error fault attack. The evaluations of operations have been shown in 5 stages- as follows:

$$\text{Stage 1: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 2: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 3: } P_{Temp} = 2P_{ACC};$$

$$\text{Stage 4: } P_{kP} = P_{ACC} - P_1;\ P_{ACC} = 2P_{Temp};$$

$$\text{Stage 5: } P_1 = P_{ACC} - P_{kP}$$

It is point to note the hardware requires the necessary operations in 2 ADDs and 4 DBLs.

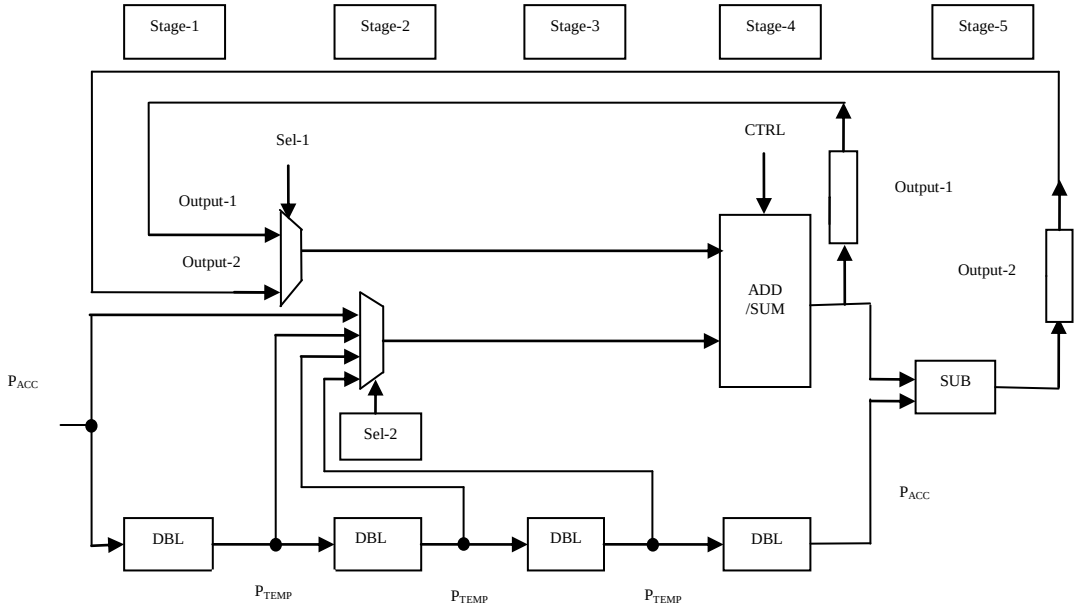


Figure 2.4: EC-Overall Dependency Graph at Five

2.4.2 Overall Dependency Graph at Five Stages

The dependency graph at radix-16 is presented in Figure 2.4 as an overall consideration for EC-operation. The feature of this scheme is stimulating in a similar way that are already crop updated above for -1 or 0. The foremost difference in remaining digit set is in the operand's transposition only. The cost per 4 bits is fixed for this procedure at $4DBLS + 2ADDs$.

Here in a similar way considered in evaluation for the whole digit set elements and terminologies are described such as Sel-1 decides the selection of either the output-1 or output-2

register, for computation of scalar multiplication Sel-2 chooses P_{ACC} directly related to be part or may be part of any temporary holding register P_{Temp}. CTR is a control option and is in a parameters indication, in addition one more operation is certain for either do ADDs or SUBs operations. In complete sense one can derive the composition of dummy variable inclusion is almost may not make any impact on the result and new inclusion is determined. So, it may be safe for the safe-error fault attack. The 5 states evaluation sequence is as:

$$\text{Stage 1: DBL}$$
$$\text{Stage 2: DBL}$$
$$\text{Stage 3: DBL}$$
$$\text{Stage 4: DBL, ADD/SUB}$$
$$\text{Stage 5: SUB}$$

2.4.3 Overall Dependency Graph at four Stages

The above dependency graph described is a possible generalization at four stages on Radix-16, we designed and managed the same as predicted in Figure 2.5. This is an overall dependency graph for all digit sets elements. SUB operation is accustomed by ADD operation in parallel at stage-1 using DBL operation. Initial $P_{kP} = 0, P_{ACC} = P, P_{kP} = P$. For scalar multiplication- P_{kP}, either the result at output1 or output2 register. In a similar fashion, it starts processing from right-to-left, i.e., LSB first, by setting $P_{ACC}^{0} = P$, and input1 either to be $P_{kP} = 0$ or $P_1 = P$. The next operation performs until sequence counter doesn't reach MSB. P_{Temp} works as temporary register and it goes in astray after final scalar multiplication computation.

During the processing, the two scenarios are in major concerns:

(i) The SUB operation treated in computer science as equal to addition in 2's complement, so subtraction is considered as similar to addition operation. Accordingly, one DBL and one ADD operation implemented in parallel. The architecture consideration is based on 4-clock cycles to complete one's iteration at 4-bits at a time in relation. During the stage-2 and stage-3, P_{Temp} is used to hold the immediate result.

(ii) The dependency graph works at an architecture organization in parallel at total of 4 DBLs and 2 ADDs. Four bits are processed for scalar at every clock cycle and contents of P_{Temp} doesn't need to be store in longer.

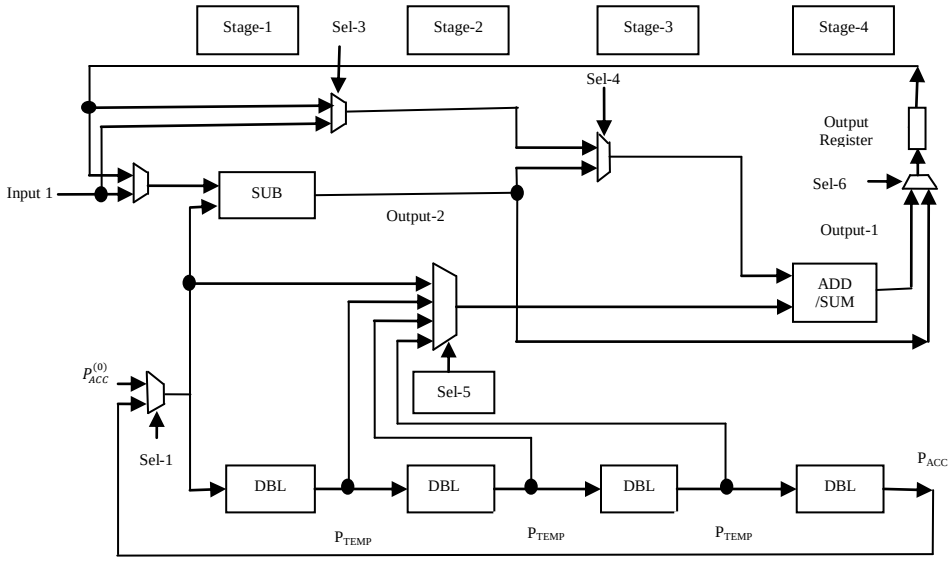


Figure 2.5: EC-Overall Dependency Graph at Four

The above shown schematic is consisting a unique identified behavior's in its sense. No dummy operations are used during the processing, so fault analysis and risk in these regards are negligible. Now, the dependency graph can be considered to be safe-error fault attack and against the simple side channel attacks, respectively.

Initial assumptions could not change; it is fixed for the proposed algorithm. If assumptions change so, it will occur in incorrect results and it will violate the principle of safe-error fault attacks. The reason we can clarify by assuming at digit set=0 (as in general it doesn't require processing) for keeping the proposed scheme consistent in relation to other digit set elements, it explicitly does scalar multiplication P_{kP} by doing the operation at $P_{kP} = P_{ACC} - P_1$. The scalar multiplication P_{kP}, and two auxiliaries P_1 and P_{ACC} are always preserved due that reason. In addition to it, the remaining digit set elements (-1, and 1 to 14) are also being considered in consistent in advanced, and it has been observed for all cases it doesn't affect the evaluation sequence of scalar multiplication kP at any stage. The inclusion of any dummy operations doesn't show its consistency.

2.5 PERFORMANCE ANALYSIS OF THE PROPOSED ECSM SCHEME

The scalar multiplication at Radix-16 power consumption is fixed for the proposed scheme that was shown in Figure 2.5. It is shown that the scheme is inherently restricted against safe-error fault attack and simple side channel attack, so any liability introduced into any operation will

bring about an incorrect scalar multiplication result. The following analysis represents its special benefits:

2.5.1 Related computation cost with ADDs and SUBs

In the following, it has been understood that a temporary register was provided as an ingredient to the processor. It is also difficult or impractical to differentiate between SSCA attacks for ADD and SUB operations [33]-[34]. The concluding remarks are justified as follows. The cost of the contradiction operation in- $GF(p)$, i.e., mapping- $x \to -x$, is about to half the cost of addition/subtraction on modular reduction. So, to the proportion ratio is in cost computation that are nearly to the same for one point ADD and one SUB an operation, as- $ADD/SUB \cong 0.99$.

2.5.2 Dependency Graph for SSCA-Protected Scheme for Scalar Multiplication

The DLP generated for scalar multiplication using the hardware support is unable to revert back the original scalar and it is unaware from SSCA operations on ADDs and DBLs in a uniform way. Coron has been masked the dependency by introducing dummy operations, it is noted that the adversaries may determine which arithmetic ADDs are the dummy operations [35], [36]. A fixed pattern for DBLs and ADDs is proposed Moller in [37], Okeya in [38] used the same for windows-based method for dummy operations. The Montgomery Ladder method [39], [40]-[42] is the best suited in favor of SSCA scheme on only change in hardware implementation. Supplementary to the above protection, this scheme has enhanced with resistance to safe-error fault attack, SSCA, and is in the consideration in reduced computational cost given by AbdulRahman and Masoleh in [30]. Our proposed scheme contains the same protection schemes on more reduced costs and chances to generate the more unpredictability & randomness behaviors.

2.5.3 Software and Hardware Perspective

In regards the software performance perspective, the proposed methodology is compared on computational costs, therefore for each digit sets Radix-16 is an acceleration by 6.25 percent in compared to the radix-8 scalar multiplication. Also, one of the major considerations is in memory saving on shorter representation at the base 16. Now, from the hardware performance

perspective for each digit sets in scalar multiplication computational cost is reduced compared to radix-8 to radix-16, i,e., $1 / 3$ to $1/ 4$, that is representing 8.33 percent in acceleration.

2.6 SUMMARY

The work presented in this chapter is an Elliptic Curve Scalar Multiplication at radix-16 on without pre-computed operations. The formulated methodology is based on mathematical explanation and best suits to all digit set elements contained in computation. The approach is uniquely identified by a single digit set assessment is a prime consideration, as a result it can be treated as one of the recent advanced development. It is also predicted on the methodological approach, in a sense of computation costs, for scalar multiplication at 6.25 percent in acceleration in comparison to recently proposed radix-8 scheme. On the hardware performance perspective it is observable in 8.33 percent acceleration. The securities and performance are the most challenging issues, so the proposed scheme is applied both to software implementation and hardware algorithms, and it is best suits to the proposed approach. Therefore, for reduced instruction set computing, it is one of the most appropriate techniques - where short-memory procedure is most attractive in favor to protect from simple-side channel attacks and safe-error fault attacks.

CHAPTER 3

ON REDUCED COMPUTATION COST FOR EDWARDS AND EXTENDED TWISTED EDWARDS CURVES

Scalar multiplication techniques are having the scope for gaining the computational efficiency for Elliptic Curve Cryptography (ECC). The security strength and effectiveness schemes have shown better results as reported in literature for very shorter key lengths. The Edwards curves are one of the forms used in cryptography that is showing one of the advanced studies for generating the more randomness and unpredictability behaviors. The numbers of researchers have shown significant improvement in solving the same problem on two, four and eight processors and that are contributing immensely contribution in the field of security. In this chapter, we have solved the Edwards Curves and twisted Edwards Curves problems on four and eight processors based on reduced computation cost from $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ on four processors and $2M + 3A$ to $2M + 2A$ on 8-processors, respectively. The operation is performing on input scalar (usually secret key) which multiplies with point-coordinates on curve. This is accumulated on reduced clock cycles with resistance to the simple side channel attack.

3.1 INTRODUCTION

Cryptography is a discipline of computer science and it has been generalized for security aspects from definition and concepts of computing systems. It is fulfilling the security requirements on systematic foundational issues. It has been treated as a branch of mathematics. Modern cryptography is mostly focusing on security problems, perfect definition and light-weight evolution methodology that suits short-memory devices with low computation and communication cost. The security mechanisms work as a backbone for information systems. These are preventing adversaries from business secrets. Recent research trends are observed for security techniques, types of processor used to influence the performance, using resources and given architecture are acting as a central role in information systems. The public-key cryptography is a major technique to protect the security. Today's it is using special functionalities, advanced algorithms and focused curves that are in very particular to accelerate software performance and reduce hardware specification storage dependence on some base point.

In public key cryptography, ECC [12]-[13] has attracted the most attention from the research community in the last three decades. ECC has gained much popularity and is also dominating RSA/DSA systems today due to its higher computational speed on shorter key sizes. Scalar multiplication is a central operation of ECC that eventually depends on point addition and point doubling operations and these two operations depends on the finite field's arithmetic [14].

Discrete Logarithmic Problem (DLP) is acting as a most sensitive part of cryptography which is in general generated on applied algorithms. The faster algorithms are running and compete with prompted in the computation and communication scenario [118]. DLP-ECC is working on a given two elliptic points P and Q on the curve, to find the value of k (generally secret key), such that- $Q = kP$, which acts like a foundational building block in PKC [15]. It computes cryptographic function in the forward direction using repeated point additions (ADDs) and point doublings (DBLs) operations. It is known as scalar multiplication. But, the adversaries try to find the secret key on the generated scalar multiplication values, which has been considered negligible to revert back to ECC. ECC is a center of attraction due to better security and performance on shorter key sizes with a low costs and attracting the most attention in suitability almost for all applications concerning which takes less memory to implement devices..

The rapid growth on memory and low cost arithmetic in cryptographic applications are attracting the most attention in the recent scenario. Edwards curves are used in the field of Elliptic Curve Cryptography (ECC), where Harold Edwards in 2007 [44] first studied about a family of curves for (ECC). Thus, Edward's curves are considered as a family of elliptic curves that are often used for cryptographic functions. These are existing over finite fields arithmetic and practically applied for security measures. The foundation of these curves is based on the mathematical formulation. Twisted Edward's curves are a generalization of the Edwards curves. The generalized curves are used in important security schemes as well and are well worth studying.

Bernstein and Lange developed various applications for Edward's curves in cryptography [46]. They also pointed out several advantages of Edwards form in comparison to the more well known Weierstrass form. Here we have summarized works related to Edward's and twisted Edward's curves:-

- Edward's followed addition law on the results produced from the Gauss/Euler example and generalized it in the form of elliptic curve to do the arithmetic on this curve in [44]. The general equation of Edwards curves is:

$$x^2 + y^2 = 1 + dx^2y^2, \text{ for some scalar, where } d \in \{0,1\}. \quad (17)$$

One another form for Edward's curves is also available with c and d parameters such as:

$$x^2 + y^2 = c^2(1 + dx^2y^2), \text{ where } c,\ d \text{ with } cd(1 - c^4.d) \neq 0. \quad (18)$$

The reviews on addition, doubling and a dual addition-doubling law for Edwards and Twisted Edwards curves fulfill the criteria into the complete curves. The following terms such as unified refers to addition formula is remain valid throughout when two input points are identical and it can also be used for point doubling, and the term complete refers to the addition formula for all inputs.

The Edwards addition law: The Edwards curves (18) say have two elliptic points, with such coordinates (x_1, y_1) and (x_2, y_2), addition point (x_3, y_3) is based on affine coordinates as:

$$(x_3, y_3) \rightarrow \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_1y_2 - cx_1x_2}{1 - dx_1y_1x_2y_2}\right) \quad (19)$$

On appropriate denominators insertion one obtains a Edwards addition law in the following coordinates, such as projective coordinates, inverted coordinates, extended coordinates, and completed coordinates.

The Edwards addition law is in generic doublings operations and named as strongly unified. The point $(0,1)$ in addition law is the neutral element. The negative coordinates of a point (x_1, y_1) is $(-x_1, y_1)$.

Affine Doubling Formulae (independent of d):

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{y_1^2 + ax_1^2}, \frac{y_1^2 - ax_1^2}{2 - y_1^2 + ax_1^2}\right) = (x_3, y_3) \quad (20)$$

The dual addition law: Hisil et al. in [21] introduced the addition law

$$(x_3, y_3) \rightarrow \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + cx_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}\right) \quad (21)$$

The dual addition law is the same likely treated as Edward's addition law; nevertheless there are some of the exceptional cases.

- A general version defined by Bernstein and Lange $x^2 + y^2 = a^2(1 + dx^2y^2)$ or simply $x^2 + y^2 = (1 + dx^2y^2)$ together for computing the group operations on projective coordinates in [46]. The outcome of addition cost is $10M + 1S + 1D$ with a=1. The rest of this paper includes multiplication by constant curve factor D.
- Bernstein and Lange in 2007 invented Edward's coordinates in [47], which reduced the cost for the group operations on point addition costs $9M + 1S + 1D$ on Edward's curves.
- Bernstein et al. introduced the new form of twisted Edward's curves on $ax^2 + y^2 = 1 + dx^2y^2$ and considered to be a generalization of the same [43]. Due to this reason the arithmetic speed was enhanced on a suitable point representation. This new representation is known as extended twisted Edward's curves which add an auxiliary coordinate to twisted Edward's coordinates. Despite the same, they developed the faster ways for doing the point addition and composed coordinates on the lower degree of arithmetic computation.
- Jacobian Projective coordinates have generalized on 4-processors by Longa and Miri on the Fast and Flexible Prime Fields [20]. They accelerated the techniques on cheaper operations on the substitution of multiplication with square on the fact that a square cost is less than multiplication. The conventional approach also works for the same and its significance is in protecting Simple Side-Channel Attacks (SSCA).
- Hisil et al. [21] introduced a fast algorithm for twisted Edward's curves and pushing the recent speed limits on performing group operations on a wide range of applications. The faster algorithm for point addition is presented in paper is 9M+1S. It is also described the new addition algorithm is implemented on four processors gaining the reduced cost to 2M. In addition to it, the presented algorithm is natural protection on simple power analysis from side channel attacks.
- Bernstein at al. in [48] suggested to use Elliptic curve method for Edwards curves that pointed out the improvement above the arithmetic level as follows: (1) on behalf of Montgomery curves they used Edwards curves; (2) using extended twisted Edward's curves; (3) addition-subtraction chains on used sliding window method; (4) on increased window size to extend on chosen base points and small parameters curves.

- Abdulrahman and Masoleh in 2015 [30] solved the problem of Edwards and Twisted Edwards curves on 4-processors and 8-processors respectively on the cost of 2M+1S+1D+2A and 2M+3A.

This chapter is organized as follows: section 3.2 is parallelized for Edward's curves on 4-processor architecture. This contains the Edwards curve problem on two coordinates that solves for 4-processors architecture. The advantages we get in the form of computation cost. Similarly we solve the problem of extended twisted Edward's curves which is based on 8-processors with its computational cost in section 3.3. Finally, we summarize our work.

3.2 PARALLEL ARCHITECTURE ON EDWARDS

In this section, we parallel the architecture of Edward's curves on 4-processors that are showing a significant addition operation of the proposed work. This follows on two points coordinates of Edwards curve such as $P_1(X_m, Z_m)$ and $P_2(X_n, Z_n)$ present a protected scalar multiplication scheme for the prime field on all the parallel and simple side channel attacks that have reported with the various proposed approaches on the fast Montgomery curve for Montgomery Ladder method [21] and radix-8 scalar multiplication [30].

The coordinates of point additions are as follows:

$$\begin{cases} X_{m+n} = \big((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\big) \\ Z_{m+n} = X_{m-n}\big((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\big)^2 \end{cases} \tag{22}$$

Whereas the coordinates of point doublings are as follows:

$$\begin{cases} 4X_m Z_m = (X_m + Z_m)^2 - (X_m - Z_m)^2 \\ X_{2m} = (X_m + Z_m)^2 . (X_m - Z_m)^2 \\ Z_{2m} = 4X_m Z_m \left((X_m + Z_m)^2 + \big(\big((A+2)/4\big)(4X_m Z_m)\big)\right) \end{cases} \tag{23}$$

The proposed method is solving this problem for ADD-DBL operations on the reduced computational complexity from 2M+1S+1D+3A [30] to 2M+1S+1D+2A based on the 4-processors, as shown in Figure 3.1. The comparative study in relation to the proposed scheme is showing a significant improvement in addition.

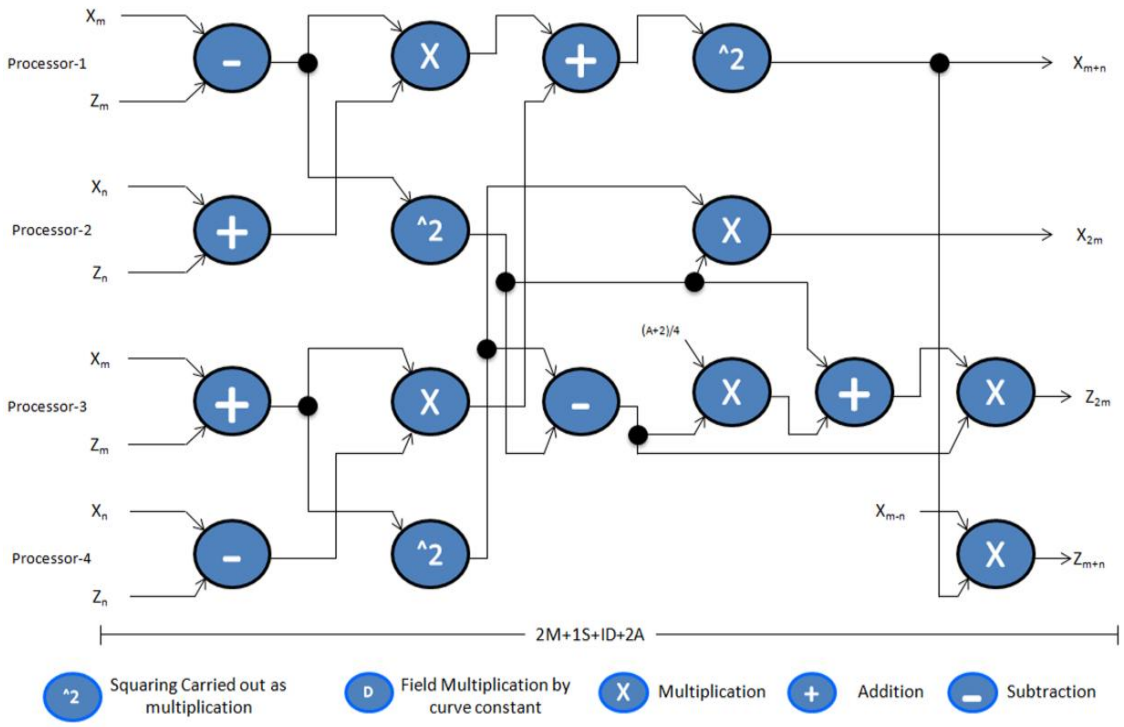


Figure 3.1: Parallel architecture for ADD-DBL on 4-processors

3.3 PARALLEL ARCHITECTURE ON EXTENDED TWISTED EDWARDS CURVES

The extended twisted Edward's curve on eight processors is parallelized for its coordinates. One of the combined operations of point ADD and point DBL is incorporated in a single operation as ADDDBL. The arithmetic cost on 8-processors is implementation for ADDDBL extended twisted Edward's curve on prime field is generalized on curves [46] with its equation:

$$\varepsilon_T: ax^2 + y^2 = 1 + dx^2y^2 \tag{24}$$

Where, $a, d \in GF(p)$, with $ad(a-d) \neq 0$. A faster way to develop DBL and ADD operations is in [21], an additional auxiliary coordinate is added to the extended twisted Edwards coordinates. It is observed and represented in [21] for extended twisted Edward's curves in quadruple coordinates.

According to definition of twisted Edward's curves which says it is based on four coordinates with two point's scalar multiplication. Suppose- $P_1(X_1, Y_1, T_1, Z_1)$, and $P_2(X_2, Y_2, T_2, Z_2)$, be two different points on curve ε^e, with $Z_1 \neq 0$ and $Z_2 \neq 0$, then point addition coordinates $P_3(X_3, Y_3, T_3, Z_3)$, are given as follows [11]:

$$\begin{cases} X_3 = (X_1Y_2 - Y_1X_2)(T_1Z_2 + Z_1T_2) \\ Y_3 = (Y_1Y_2 - X_1X_2)(T_1Z_2 - Z_1T_2) \\ T_3 = (T_1Z_2 - Z_1T_2)(T_1Z_2 + Z_1T_2) \\ Z_3 = (Y_1Y_2 - X_1X_2)(X_1Y_2 - Y_1X_2) \end{cases} \quad (25)$$

And for doubling coordinates formula, i.e., $P_4(X_4, Y_4, T_4, Z_4) = 2P$, is given in [11] by:

$$\begin{cases} X_4 = (2X_1Y_1)(2Z_1^2 - Y_1^2 + X_1^2) \\ Y_4 = (Y_1^2 - X_1^2)(Y_1^2 + X_1^2) \\ T_4 = (2X_1Y_1)(Y_1^2 + X_1^2) \\ Z_4 = (Y_1^2 - X_1^2)(2Z_1^2 - Y_1^2 + X_1^2) \end{cases} \quad (26)$$

In a special case $a = -1$, needed DBLs and ADDs operations are $4M + 4S + 6A$ and $8M + 10A$ respectively, considering that arithmetic subtraction and addition are equal. The proposed composite (ADD+DBL=ADDDBL) operation for this curve is solved for both ADD and DBL operations in 5 steps on splitting the computational task on 8-processors in [30]. This is reported to be the fastest way to do the scalar multiplication. According to this, the effective time has been reduced to $2M + 3A$ operations on 8 processors.

Our proposed scheme is achieving faster scalar multiplication result, as shown in Figure 3.2. As a simplicity purpose, the required registers (or auxiliaries) in the Elliptic Curve Scalar Multiplication schemes are not analyzed or discussed. Also in the paralleling process, we imposed the architecture limitation on SIMD (Single Instruction Multiple Data) operations that have already been done in [22], [20].

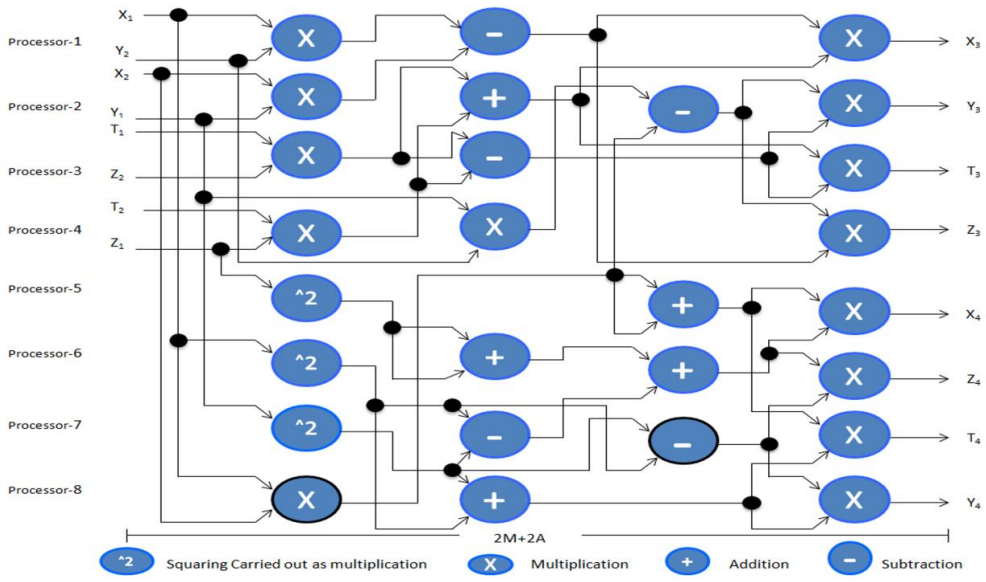


Figure 3.2: Paralleling ADDDBL Operation on Prime Extended Twisted Edwards Curve

According to our proposed work, we solved the same problem for the scalar multiplication at 4-states, which takes a shorter clock cycle to initiate the process in one's multiplication reduction (in relation to the previously proposed work) and it is considered as an immense contribution to the overall performance improvement. The dependency graph using equation (9) and (10) shows two equations require a computational cost of one's multiplication operation in saving. The ADDDBL operation scheme is on eight independent processes, i.e., process 1 to process 8-where finite arithmetic operations are represented by a circle and it is labeled according to the type of operations. In the proposed scheme, it is explicitly the squaring (S) operation is performed and multiplication (M) operation is carried out. On the prime extended twisted Edwards curves the effective time cost of DBL operation is obtained by one round saving and it is completed in an effective time of $2M + 2A$.

The general operations for 8-processors on s-bit scalar multiplication requires $6\frac{(s-1)}{3}M + 3\frac{(s-1)}{3}A$ for Montgomery Ladder method in [40] and the extended twisted Edwards curves on radix-8 ECSM method requires $5\frac{(s)}{3}M + \frac{(s)}{3}A$ in [30]. Our proposed ECSM required operations of $4\frac{(s)}{3}M + \frac{(s)}{3}A$.

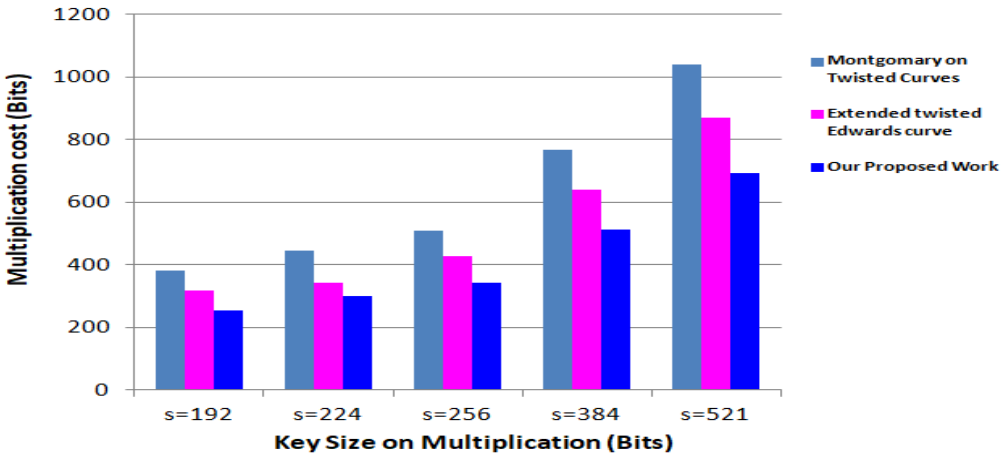


Figure 3.3: Comparative cost reduction of our proposed approach

In figure 3.3, we have made a comparative study that our proposed solution for extended twisted Edwards curve is providing better than the existing methodologies, which has been generalized from the formerly reported literature. [If SIMD limitation is not proposed on results of Figure 3.3 the following consequences may occurs, that are available in Appendix 3 at page 148].

The comparative time complexity to complete the point ADDs and point DBLs takes the shorter clock cycle to initiate the same. Finally, in Table 3.1, we linked the related parallel schemes and its required complexities on key sizes s={192,224,256,384,521}.

Table 3.1: Comparison of Related Parallel Scheme on Edwards Curve

Prime Fields Size GF(p)	**Schemes on Processor**	**Computational Time Complexity**
s=192	4 Processors for Jacobian Projective Coordinates [45]	191M+637S
	4 Processors for Extended Twisted Edwards [21]	319M+191S
	Montgomery Ladder method on the Montgomery curve [40]	382M+382S
	Montgomery Ladder at Montgomery curve [21]	382M+191S
	New Regular Radix-8 Processor Scheme [30]	320M+64S
	Our Proposed 8 Processors Scheme	256M+64S
s=224	4 Processors for Jacobian Projective Coordinates [45]	223M+744S
	4 Processors for Extended Twisted Edwards [21]	372M+223S
	Montgomery Ladder method on the Montgomery curve [40]	446M+446S
	Montgomery Ladder at Montgomery curve [21]	446M+223S
	New Regular Radix-8 Processor Scheme [30]	446M+75S
	Our Proposed 8 Processors Scheme	299M+75S
s=256	4 Processors for Jacobian Projective Coordinates [45]	225M+850S
	4 Processors for Extended Twisted Edwards [21]	425M+245S
	Montgomery Ladder method on the Montgomery curve [40]	510M+510S
	Montgomery Ladder at Montgomery curve [21]	510M+255S
	New Regular Radix-8 Processor Scheme [30]	427M+86S
	Our Proposed 8 Processors Scheme	342M+86S
s=384	4 Processors for Jacobian Projective Coordinates [45]	383M+1177S
	4 Processors for Extended Twisted Edwards [21]	639M+383S
	Montgomery Ladder method on the Montgomery curve [40]	766M+766S
	Montgomery Ladder at Montgomery curve [21]	766M+383S
	New Regular Radix-8 Processor Scheme [30]	640M+128S
	Our Proposed 8 Processors Scheme	512M+128S
s=521	4 Processors for Jacobian Projective Coordinates [45]	520M+1734S
	4 Processors for Extended Twisted Edwards [21]	867M+520S
	Montgomery Ladder method on the Montgomery curve [40]	1040M+1040S
	Montgomery Ladder at Montgomery curve [21]	1040M+520S
	New Regular Radix-8 Processor Scheme [30]	869M+174S
	Our Proposed 8 Processors Scheme	695M+174S

The evaluation schemes is relatively in computation enhancement, and is presented in the respective orders, (i) Jacobian projective coordinates in [45], (ii) extended twisted Edwards curves on the 4-processor scheme in [21], (iii) on the Montgomery curve on the 4-processor Montgomery Ladder method in [40], (iv) Montgomery Ladder method on the Montgomery curve shown in [40], (v) the extended twisted Edwards curves on 8-processor scheme in [30]. But our proposed extended twisted Edwards curves on 8-processor in terms of computational time complexity on prime field is better than all.

In this section, we proposed a protected scalar multiplication for the prime extended twisted Edwards curve that can perform faster than all the parallel and SSCA-protected schemes, on behalf of literature including the fast Montgomery Ladder method on the Montgomery curve [40] and scalar multiplication at Radix-8 [30].

There are two parameters (Multiplication and Subtraction), our contribution is reflecting at the level of multiplication costs (bits) only with respect to the used key (bits), whereas our subtraction cost is remain the same to the previously proposed solution, therefore here in our contribution this parameter we didn't considered and we have not shown in our thesis.

3.4 SUMMARY

This chapter makes contribution of significant improvement in performance for the scalar multiplication techniques proposed for the Edwards and extended twisted Edwards curves. The problem statements have been defined on 4-processors and 8-processors having to gain the computational efficiency for Elliptic Curve Cryptography (ECC). The ECC is justifying the security strength and effectiveness on the shorter key lengths. The comparative reduction cost on the 4-processors is $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ and on the 8-processors is $2M + 3A$ to $2M + 2A$.

CHAPTER 4

NOVEL NONCOMMUTATIVE CRYPTOGRAPHY SCHEME USING EXTRA SPECIAL GROUP

On Elliptic Curve Cryptography (ECC) and twists in ECC for scalar multiplication is a possible generalization on non-commutative properties. Using these properties is certainly generating a new perspective in cryptography. Therefore, Noncommutative Cryptography (NCC) is one of most fascinating area in security up gradation. It provides high level of safety measures and performance enhancement almost for all end applications. The basis of this NCC group is established on the Hidden subgroup or subfield problem (HSP). The major focus of this chapter is to establish the cryptographic schemes on the extra special group (ESG). ESG is showing one of the most appropriate Noncommutative platforms for the solution of an open problem. The working principle is based on the random polynomials chosen by the communicating parties to secure key-exchange, encryption-decryption and authentication schemes. This group supports at Heisenberg, Dihedral order and Quaternion group. Further, this also enhances it from the general group elements to equivalent ring elements, known by the monomials generations for the cryptographic schemes. In this regards, special or peculiar matrices show the potential advantages. The projected approach is exclusively based on the typical sparse matrices, and an analysis report is presented that are fulfilling the central cryptographic requirements. The order of this group is more challenging as it assails like length based, automorphism, and brute-force attacks.

4.1 INTRODUCTION

Cryptography is a discipline of computer science, where algorithms and security practices are acting as a central tool. This is traditionally based on the mathematical foundation. The practical applications contain the assurance of legitimacy, protection of information from confessing, and protected message communication systems for essential requirements. To enforce security, the cryptographic schemes are concerned with playing vital role responsiveness in the field of

security for numerous relevant applications all over the world. The absolute measure of cryptographic approaches shows the full-fledged appropriateness. But, the serenities fondness with an assortment of more arbitrariness and impulsiveness with statistical responses are the motivational issues.

Public key cryptography (PKC) thought was first proposed by Diffie and Hellman [12]. Since then varieties of PKC algorithms have been proposed, where Elliptic Curve Cryptography (ECC) [14], [49] in all of them has attracted the most attention in the cryptographic area. ECC has played a crucial role that made a big impact on the lower computational and communicational cost. Today ECC is considered to be tenable, but researchers are looking for alternative approaches for future security by not putting all the security protocols in one group only, i.e., commutative group. On behalf of the open opinion, a brief analysis is presented below. Shor's in 1994 [50], proposed a competent quantum algorithm for solving the discrete logarithm problem (DLP) and integer factorization problem (IFP). A Kitaev's framework in 1996 [51] considered as a special case on DLP, called as hidden subgroup or subfield problem (HSP). Stinson sensibly observed in 2002 that the most eternal PKCs belong to a commutative or abelion group only, whose intention is susceptible in the forthcoming future. Accordingly, cryptographers Goldreich and Lee advised, don't put all cryptographic protocols in one group. The reason was clear to introduce a new field of cryptography; this was only the opening of Noncommutative cryptography [52]. Then afterwards for key-exchange, encryption-decryption (ED) and authentication schemes for cryptographic protocols on Noncommutative cryptography were developed for various problems. Those were analogous protocols like the commutative cases. The elliptic curve over the HSP [53] comprehensively resolved DLP, as recognized by ECC-DLP. The random HSP over Noncommutative groups are well-organized on quantum algorithms, which are also well responsive. Further, the evidences are recommending HSP over Noncommutative groups that are much harder [54].

The earlier structure of Noncommutative cryptography was based on the braid based cryptography for the generalizations of the protocols. Afterward several other structures like Thompsons, Polycyclic, Grigorchuks or matrix groups/ring elements were proposed. The cryptographic primitives, methods and systems of the Noncommutative cryptography are based on algebraic structures of group, ring and semi-ring elements. But, in all of them matrix group of elements has shown the prospective advantages. In contrast, implementations in recent

applications (protocols) using public key cryptographic approaches on Diffie-Hellman, RSA and ECC are based on number theory. They are solving the various problems like session key establishments, encryption-decryption and authentication schemes.

The basis of Noncommutative cryptography is based on $*$ (contains reflection and/or rotation) operation on the Noncommutative group G of $(G,*)$ that consists of Group, Ring, Semi-ring, or some algebraic structural elements- in which, two group elements a and b of G are such that $a * b \neq b * a$, known by Noncommutative or Non-abelion group. The group of these problems are broadly encompassing in between the relations of mathematics and physics.

4.1.1 Background

The generation of Noncommutative cryptographic approach has a solid backbone for security enhancements and performances; of course numerous attempts have been made available for the same. A brief analysis is described below:

- Wagner and Magyarik in 1985 [55] proposed undecidable word problems on semi-group elements for public key cryptography (PKC). But, Birget et al. [56] pointed out; it is not based on word problem, and proposed a new system on finitely generated groups with a hard problem.
- On braid based cryptography, a compact key established protocol proposed by Anshel et al. [57] in 1999. The basis was difficulty in solving equations over algebraic structures. In research paper, they recommended braid type of groups may subsist to be a good alternate platform for PKC in advance.
- Afterward, Ko et al. in 2000 [58] anticipated a new PKC by using braid groups. The Conjugacy Search Problem (CSP) is the intractability security foundation, such as effective canonical lengths and braid index when they are chosen suitably. Further, the area under consideration met with immediate successes by Dehornoy in 2004 [59]; Iris Anshel et al. in 2003 [60]; Iris Anshel et al. in 2006 [61]; Cha et al. in 2001 [62]. Despite the fact, 2001 to 2003, recurring cryptanalytic sensation Ko et al. in 2002 [63]; Cheon and Jun 2003 [64] diminished the initial buoyancy on the noteworthy theme, on Hughes and Tannenbaum in 2000 [65]. Many number of authors proclaimed the impetuous death on braid-based PKC, Bohli et al. in 2006 [66]; Dehornoy in 2004 [67]. After, Dehornoy's gave a survey on the state of the subject stating that a significant research is still desirable to accomplish a definite

and final conclusion on the cryptographic prospective of braid groups.

- In Paeng et al. in 2001 [68] proposed a new scheme of PKC built on finite non-abelion groups. The DLP generation is based on automorphism through inner group passing as conjugation accomplishment. These were further improved, named as MOR systems.
- In the meantime, one way function and trapdoors generated on the finite fields were remarkable in group theory by Magliveras et al. 2000 [69]. Later on, in 2002 Vasco et al. [70] confirmed an appropriate generality on factorization and several cryptographic primitives as a uniform description on convincing homomorphic cryptosystem which were constructed for the first time for non-abelion groups. Meanwhile, Magliveras et al. in [71] proposed a new approach for public key cryptosystems designing as trapdoors and working as one-way functions in finite groups. Grigoriev [72] and Ponomarenko [73], consequently, extended the difficulty of membership problems on integer matrices for a finitely generated random group of elements.
- The arithmetic key exchange was enlightened by Eick and Kahrobaei 2004 [74], and an innovative cryptosystem on polycyclic groups was proposed by them. The structures of polycyclic groups are complex issues of their own cyclic group. The algorithmic theory and investigation properties are more difficult that seems to have a more open proposal. The progression tenure is a succession of subgroups of a group $G = \mathrm{G}_1 \rhd \mathrm{G}_2 \rhd \cdots \rhd \mathrm{G}_{n+1} = \{1\}$. Each series term in succession is not only belong from the entire group and is not contained in the former term. A group G is called polycyclic series with cyclic aspects, i.e., $\mathrm{G}_i/\mathrm{G}_{i+1}$ is recurring for $i = 1, \ldots, n$.
- Shpilrain and Ushakov in 2005 [75], recommended that Thompson's group is a good proposal for building PKC's. The assumptions under the decomposing problem are intractable, ancillary to the Conjugacy search problem, described over- R.
- In 2005, Mahalanobis [76] is in discriminated the D-H key exchange on a cyclic group with finite non-abelian as a nilpotent group. The nilpotent group is a normal series to each quotient $\mathrm{H}_i/\mathrm{H}_{i+1}$ lies in the centre of $\mathrm{G}/\mathrm{H}_{i+1}$and is supposed to be a central succession. A class of nilpotent group is the shortest series length with its shortest nilpotency degree. Polycyclic groups are engendered nilpotent in finite fields and instead of it have a central series in cyclic factors. Also Dehornoy in 2006 gave an authentication scheme on the left self-distributive (LD) systems. Further, this idea is developed on the concept of the one-way

LD system inclusion, structured by Wang et al. in 2010 [77]. For all elements, the algebraic association on $(A,*)$ is left self-distributive $a, b, c \in A$, $a * (b * c) = (a * b)(a * c)$.

- To extract from a given $a * b$ and b is said one-way function and is intractable. An LD system, in general, is much different from groups or semi-groups or semi-rings. Even the regarding facts are not associative. So, to describe solitarily a non-trivial LD system over any Noncommutative group G via the mapping $a * b \triangleq ab\bar{a}$.
- Moreover, the Conjugacy search problem (CSP) in group G is mostly be intractable, so the derivative of an LD system is treated as one-way.
- In 2007, Cao et al. [78] are given a methodology for cryptographic schemes establishments on polynomials structures elements. These are derived on non-commutative properties for group, rings or semi-rings elements to build cryptographic scenario and these are referred as $\mathbb{Z}$-modular methods. Further, the protocol application was based on non-abelion on Dihedral order 6 by Kubo in 2008 [79] is the initial order for this group and construction is based on three dimensional revolutions.
- In 2008, Reddy et al. 2008 [80], $\mathbb{Z}$-modular method was build on signature schemes incorporation on Noncommutative groups, rings or semi-ring elements.
- The cryptographic protocol implementations were constructed on four-dimensional by Moldovyan and Moldovyan in 2010 [81]. The perspectives were the generalizations for security enhancement on the basis of Noncommutative groups.
- In 2014, Myasnikov and Ushakov [82] cryptanalyzed the authentication scheme proposed by Shpilrain and public-key encryption to use the hardness of the Conjugacy search problem in Noncommutative monoids. A heuristic algorithm was devised by them to solve these problems, and declared these protocols are anxious.
- Svozil in 2014 [83] proposed the metaphorical recognized hidden variable on non-contextual indecisiveness that can’t be comprehended by quantum systems. The cryptanalytic attacks are not accompanied or aligned by quasi configurations, and the theorems don’t subsist assembled proofs reclined over the same.

4.1.2 Motivation and our contribution

The issue related to the ring structure of the group elements is one of the most motivational concerns. A typical semi-ring structure, such as sparse matrices, shows the potential advantages

and shows a possible way to avoid the various attacks. The initial order for general and monomials [original parameters are hidden, and it's probably equivalent consideration takes part in computation process] structure on polynomial $\mathbb{Z}$-modular Noncommutative is the foundation.

Our contribution is in multidisciplinary scenario on extra special group on the cryptographic protocol regarding the key-exchange, encryption-decryption and authentication in four dimensional perspective. The key idea is based on a special case of prime order which is more resistant to attacks and proposed approach works on the bigger range of probabilistic theory.

4.1.3 Work Organization

The contents of chapter are organized into its subsequent sections. The next section presents cryptographic preliminaries for modular polynomial assumptions on general scalar multiplication and monomials like scalar multiplication on group, ring and semi-ring elements. Section 4.3 presents the fundamental of the proposed work on the extra special group and its elementary analysis is elaborated. Sections 4.4 and 4.5 are our core part, where our considerations are perfectly set aside by the general protocol schemes for the session key establishment; encryption-decryption; authentication schemes, and further for similar works on monomials generations on group and ring or semi-rings elements are created . In section 4.6, a brief idea is presented to achieve the bigger search space for the length based attack, which gives its security guarantees. Finally, the work concludes, along with references.

4.2 PRELIMINARIES

4.2.1 $\mathbb{Z}$ Modular Assumptions on Noncommutative Cryptography

The scalar multiplication is the basis for all cryptographic computations. The major goal of scalar multiplication is to generate the discrete logarithmic value. A new public key cryptography on polynomials scalar multiplication over the Noncommutative ring R is proposed by Cao et al. in 2007 [78]. The developed scheme is based on modulo prime integers, named as $\mathbb{Z}$-modular method. The derived $\mathbb{Z}$-modular structure on ring is $\mathbb{Z}$ (r), and this structure applies for positive $\mathbb{Z}^{+}[r]$ and/or negative $\mathbb{Z}^{-}[r]$ on Noncommutative ring R elements, where $r \in R$ is undetermined. Also, group and semi-ring are comprehensively applicable on $\mathbb{Z}$-modular assumptions.

4.2.1.1 Noncommutative Rings on $\mathbb{Z}$ modular method

The integral coefficient polynomial on additive Noncommutative is defined on ring $(R, +, 0)$ and for multiplicative Noncommutative $(R, ., 1)$, for ring R elements is well-defined for scalar multiplication on $k \in \mathbb{Z}^+$ and $r \in R$,

$$(k)r \cong \underbrace{r + \cdots + r}_{k \text{ times}}$$

Further, for $k \in \mathbb{Z}^-$,

$$(k)r \cong \underbrace{(-r) + \cdots + (-r)}_{-k \text{ times}}$$

Finally, if it is to define on scalar $k = 0$, it is likely to be $(k)r = 0$.

Proposition 1: In general, scalar multiplication on Noncommutative is $(a)r.(b)s \neq (b)s.(a)r$, when- $r \neq s$. Recall a polynomial with positive integral coefficient- $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}^+$, for all- x. To assign the component x as an element- $r \in R$, then to attain a precise element in ring R is given as:

$$f(r) = \sum_{i=0}^{n} (a_i)^{r^i} = a_0.1 + a_1.x + \cdots + a_n.x^n$$

In addition, suppose r be undetermined, then polynomial over f (r) is univariable polynomial lying on R. The polynomial on univariable over R as a whole set is denoted as- $\mathbb{Z}^+[r]$, and it is defined as follows for the respective functions on two different ring elements:

$$f(r) = \sum_{i=0}^{n} (a)_i{}^{r^i} \in \mathbb{Z}^+[r], \text{and } h(r) = \sum_{j=0}^{m} (b)_j{}^{r^j} \in \mathbb{Z}^+[r]$$

Again, if $n \geq m$, then

$$\left(\sum_{i=0}^{n} (a_i)^{r^i}\right) + \left(\sum_{j=0}^{m} (b_j)^{r^j}\right) = \sum_{i=0}^{m} (a_i + b_i)r^i + \sum_{i=m+1}^{n} (a_i)^{r^i}$$

And according to the property of distributive law it generalizes the above equation as:

$$\left(\sum_{i=0}^{n} (a_i)^{r^i}\right) + \left(\sum_{j=0}^{m} (b_j)^{r^j}\right) = \left(\sum_{i=0}^{n+m} (p_i)^{r^j}\right)$$

Where,

$$p_i = \left(\sum_{j=0}^{i} (a_j b_{i-j})^{r^i} \right) = \sum_{j+k=i} (a_j)(b_k)$$

Theorem 1:- $f(r).h(r) = h(r).f(r), \forall f(r) \in \mathbb{Z}^+[r]$ and $\forall h(r) \in \mathbb{Z}^+[r]$, where $\forall$ signifies for all elements.

Proof: Here ring r be a subset of ring R that is applied on polynomial functions of $f(r)$and $h(r)$, for all positive integers of- $\mathbb{Z}^+[r]$. A ring is a set of elements with two binary operations of addition and multiplication which satisfy the following case properties on commutative, associative, identity, inverse and closure. In addition to the same some more properties are also satisfying for all ring elements as:

(i) Closure multiplication: if a and b belong to ring elements, then $a.b$ is also exists in ring.

(ii) Associative of multiplication: $a(bc) = (ab)c$ for all a, b, c.

(iii) Distributive laws: $a(b + c) = ab + ac$ or $(a + b)c = ac + bc$ for all a, b, c.

(iv) Commutative of multiplication: $ab = ba$ for a, b.

(v) Multiplicative Identity: $a.1 = 1.a = a$ for all a.

(vi) No zero divisors: for all a and b in R and $ab = 0$, then either $a = 0$ or $b = 0$ and doesn't follow it on divide by zero.

Therefore, this theorem proves itself on the above properties of (i), (iii), and (iv).

4.2.2 Two Well-Known Cryptographic Assumptions

The assumptions of security strength are due to the difficulty of the following two problems:

(i) **Conjugacy Decisional Problem (CDP):** On given two group elements a and b, to determine for a random x to produce the value of other group elements, such that $b = a^x$ or to produce the same using the Conjugacy multiplicative inverse as: $b = x^{-1}ax$..

(ii) **Conjugacy Search Problem (CSP):** The two group elements of a and b in a group G, to find whether there exists x in G, such that $b = a^x$ or Conjugacy multiplicative inverse $b = x^{-1}ax$.

If no algorithm exists to solve the CSP, by applying x on one group of elements to determine the

other group of elements i.e., $a \rightarrow b^x$, then this is considered to be a one way function. In the contemporary computation, both the problems on general Noncommutative group G are too complicated enough to determine the assumptions on cryptographic primitives. The CSP assumptions are difficult-enough to solve this problem on probabilistic polynomial time. Whereas, CDP assumptions are a unique representation for any group, ring or semi-ring elements for cryptographic use, and one of the most important major advantage is the transition of all these finishes efficiently over each other.

4.2.3 Using Monomials in $\mathbb{Z}$ modular metod

The $\mathbb{Z}$-Modular method on polynomials are constrained in monomials i.e., if original information of group elements are hidden with its equivalents ring or semi-ring elements or some algebraic structured elements, such implementations in computation is viewed as a special case. Under these considerations new creations of public-key encryption schemes from Conjugacy Search Problems are proposed.

4.2.3.1 Conjugacy Search Problem

Let $(G, ., 1)$ be a Noncommutative monomials for an element- $a \in G$, other group element- $b \in G$, such that $a.b = b.a$, then it is assumed to be group a as reversible, and say b is an inverse of a, but the important none of all elements in G are reversible. It is unique in nature if the inverse of a exists and is denoted by a^{-1}. In monomials, the positive power of a group element for n integer describes it as: $a^n = \underbrace{a + \cdots + a}_{n \text{ times}}$ for $n > 1$. If b is the inverse of a, one can also define the negative power of a by setting: $a^{-1} = \underbrace{b + \cdots + b}_{n \text{ times}}$ for $n > 1$. The Conjugacy Search Problem can be extended to monomials G, for $\forall a \in G$ and $\forall x \in G^{-1}$, xax^{-1} is a conjugate to a, and call x as conjugator of the pair (a, xax^{-1}).

Definition 1: Conjugacy Search Problem (CSP): On Noncommutative monomial for any group G on the two group elements $a, b \in G$, it is defined on $b = xax^{-1}$ for some unknown element- $x \in G^{-1}$, the objective of the CSP in G is to find $x \in G^{-1}$ such that $b = x'ax'^{-1}$.

Definition 2: (Left self-distributive system): Let S be a non-empty set well defined on function F

as $F : S \times S \to S$, it is further be defined on $F(a, b)$ by $F_a(b)$, then it holds the following formula on $F_r(F_s(p)) = F_{F_r(s)}(F_r(p)), (\forall p, r, s \in S)$ and call $F_{\cdot}(.)$ is a left self-distributive system (LD).

Theorem 2: Suppose G be Noncommutative monomials, function F on conjugate follows as $F: G^{-1} \times G \to G$, $(a, b) \mapsto aba^{-1}$, and is known by LD system and abbreviated as Conj-LD.

Proof: According to definition 2, the term LD is an analogical observation from $F_r(s)$ as a binary operation in $r * s$, then this is observed as $r * (s * p) = (r * s) * (r * p)$, where "$*$" is left distributive with respect to itself. On these consideration of LHS is following to RHS as: $F_r(F_s(p)) = F_r(s * p) = r * (s * p) = (r * s) * (r * p) = F_r(s) * F_r(p) = F_{F_r(s)}(F_r(p))$. Here, it is satisfying the function F on $F_r(F_s(p)) = F_{F_r(s)}(F_r(p))$ as in an LD system. Thus, theorem 2 proves these observations.

Proposition 2: Let F be a Conj-LD system over a Noncommutative monomials defined on G for given $a \in G^{-1}$ and $b, c \in G$, the followings proposals are well-defined, according to [91]:

(i) $F_a(a) = a$.

Proof: Since- $aaa^{-1} = a$, so $F_a(a) = a$.

(ii) $F_a(b) = c \Leftrightarrow F_{a^{-1}}(c) = b$.

Proof: $F_a(b) = c \xrightarrow{\text{yields}} aba^{-1} = c \xrightarrow{\text{yields}} a^{-1}ca = b \xrightarrow{\text{yields}} F_{a^{-1}}(c) = b$.

(iii) $F_a(bc) = F_a(b)F_a(c)$.

Proof: $F_a(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = F_a(b)F_a(c)$.

4.2.4 Symmetry and Generalization Assumptions over Noncommutative Groups

To explain the symmetries and its generalizations on the Noncommutative cryptography are the following problems are on group G:

(i) **Symmetrical Decomposition Problem (SDP):** Given $(a, b) \in G$ and $m, n \in Z$, find $x \in G$ such that $b = x^m.a.x^n$.

(ii) **Generalized Symmetrical Decomposition Problem (GSDP):** Given $(a, b) \in G$,$S \subseteq G$ and $m, n \in Z$, find $x \in G$ such that $b = x^m.a.x^n$.

The GSDP is evidently a sort of constrained SDP, and if subset S is enough large, then in general does not leakage information one to extract x from $x^m.a.x^n$. Now, it is understood that GSDP is

at least as rigid as SDP. The following GSDP hypothesis says that it is not flexible to solve the same in a probabilistic polynomial time with non-negligible precision with respect to problem scale. In this regard these works are like discrete logarithm problem (DLP) over group G.

4.2.5 Computational Diffie-Hellman (CDH) Problem over Noncommutative Group G

The CDH problem to its subset S on Noncommutative to determine $a^{x_1x_2}$ or $a^{x_2x_1}$ for known a, a^{x_1} and a^{x_2}, where $x \in G$, $x_1, x_2 \in S$. The commutative means to extract $x_1 \in C(x_2)$, then the relation holds for $a^{x_1x_2} = a^{x_2x_1}$. It is noticeable that DLP in GSDP over G is tractable. But, the converse of the same is not true. At the present time, no evidence is available to resolve the this problem without on extraction on x_1 (or x_2) from a and a^{x_1}(or a^{x_2}). CDH hypothesis over G is then defined the problem over G is intractable. In this regards, no such probabilistic polynomial time algorithm exists to solve the dilemma with significant accuracy the existing problem. The same definition is also very well-distinct for a Noncommutative semi-ring. Hence, DLP of GSDP and CDH assumptions over Noncommutative semi-group are well-appropriates.

4.3 EXTRA SPECIAL GROUP

The definition says any prime p to the power $1 + 2n$ i.e., p^{1+2n}, sustains the twofold properties: (i) Heisenberg group and semidirect product of cyclic group order and/or (ii) Dihedral order 8 and Quaternion group. The two belonging group elements revolve around a fixed center, known by extra special group [84]. These are based on finite size fields on modulo primes and analogues to group elements follow sparse matrices properties. Due to this reason, group contains the dual identity, which meets the requirement for perfect cryptography. The quotients or remainders belong to *nontrivial (*Nontrivial refers to terms or variables are not equal to zero or identity after resultant) element, whose center is cyclic. Since, its size is prime so its classification based on either prime $p = 2$ or p =odd. The reason is clear any prime starts from2, and for rest belongs to odd primes only.

At $p =$ odd, the extra special group for p odd is given below:

(i) The group of triangular 3×3 matrices over the field with p elements, with 1's on the diagonal. The group is exponent p for p odd. These are known by Heisenberg group elements.

(ii) The semidirect product of a cyclic group of order p^2 by a cyclic group of order p acting nontrivial on it.

Again, if n is a positive integer, then for p odd is given as below:

(i) The central product of n extra special group of order p^3, all of exponent p. This extra special group also has exponent p.

(ii) The central product of order p^3, at least one of exponent should be p^2.

Now, consider **prime- $\mathbf{p = 2}$**, the minimum order starts from $n = 1$, so extra special group order $8 = 2^3$, described as:

(i) The Dihedral group D_8 in order 8, this group has 4 elements of order 4.

(ii) The Quaternion group of order 8, which is six elements of order 4. Example like:

$$\begin{bmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Again, if we consider n being a positive integer for Quaternion groups then:

(i) For an odd integer, the central product is in the Quaternion group.

(ii) For an even integer, the central product is in the Quaternion group.

4.3.1 Heisenberg Group

A group of 3×3 upper triangular matrices contains the several representations in terms of functional spaces whose center acts nontrivially on it. A matrix multiplication is in the form:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Where elements of a, b, c belong to commutative ring elements. Further, the real/integer numbers belong to ring structured elements, known by respective continuous/discrete Heisenberg group [85]. The continuous group comes from the description of quantum systems in one-dimension. The association with n-dimensional systems is more general in this regards. The products of two Heisenberg matrices in the three-dimensional case are given by:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

The Heisenberg neutral element of group is the identity matrix. The discrete Heisenberg group

x, y, z generators are the non-abelian of ring elements on the integers a, b, c:

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

and relations $z = xx^{-1}yy^{-1}, xz = zx, yz = zy$, where $z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is the generator with the center. A polynomial growth rate of order 3 using the Bass's theorem is used to generate any element through

$$x = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = y^b z^c x^a$$

The behavior of the Heisenberg group to modulo odd prime p over a finite field is called extra special group of exponent p.

4.3.1.1 Security Strength of Heisenberg Group

The Heisenberg group on public key cryptography follows polycyclic behaviors if and only if a sub series $G_1 \rhd G_2 \rhd \cdots \rhd G_{n+1} = \{1\}$ for a group G (where $\rhd$ denotes variations of G in cyclic form). For each positive integer of the n^{th} elements of Heisenberg generates an infinite non-abelian forms (using the binary addition and multiplication operations on matrix or sparse matrix elements), which makes the scheme of Heisenberg to be practical choice for an efficient implementation of hardware and software. This gives a unique normal form just after group operations, so the group may be considered to be an effective solution provider for cryptographic use.

4.3.2 Dihedral Order 8

The dihedral is a group of operations on a finite set of elements that includes the problems of mathematics and physics. A cycle of rotations and reflections on group elements is the basis that forms the properties of this group. One of the simplest examples of non-abelian group is dihedral order 6 [92].

In the proposed work the minimum order is Dihedral order 8, denoted by D_8, or (also called D_4) [86]. The subgroups of this (Dihedral order group G) are generating by rotations and/or reflections, those are forming a cyclic subgroup that is one of the key advantage. For

representing the Dihedral order 8, a glass square of certain thickness with letter "F" is considered. The identity element is denoted by e. In order to form more movement of square that makes letter "F" with visible difference on $0^0, 90^0, 180^0, 270^0$ [clock-wise rotations], are taken into consideration, as shown in Figure 4.1.

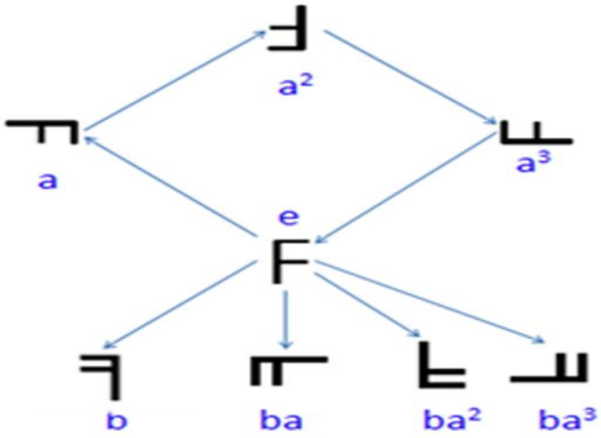


Figure 4.1: Symmetries of Dihedral Order-8

One more 'b' (reflection) operation is used relative to its corresponding above four rotations. Further, to define the composition movement such as 'ba', first do the operation for 'a' and there after application of 'b' is shown. For remaining two of- (ba^2 *and* ba^3) are working like the previous one. Now, after the corresponding operation, the same can be represented in four dimensions, as depicted in Figure 4.2. The group element is a property that it's center and derived subgroup are fixed on explicit limitations under it.

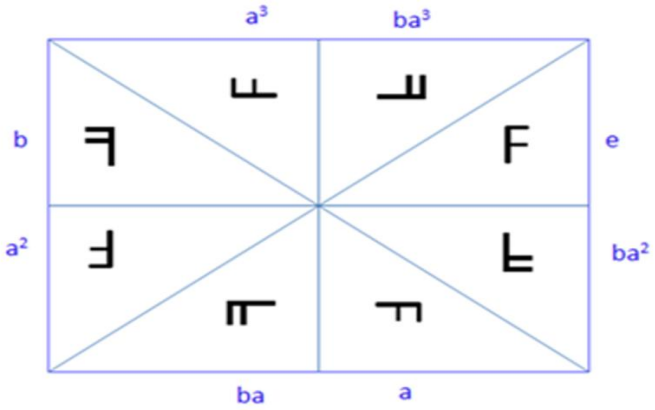


Figure 4.2: Four Dimensional Representations

The abstract movements of all operations are fixed on certain boundaries, and these are generally represented by Cayley graph. The graph is mixed with eight vertices, four edges and

eight arrows. This is one of the fundamental tools in combinatorial theory to make group

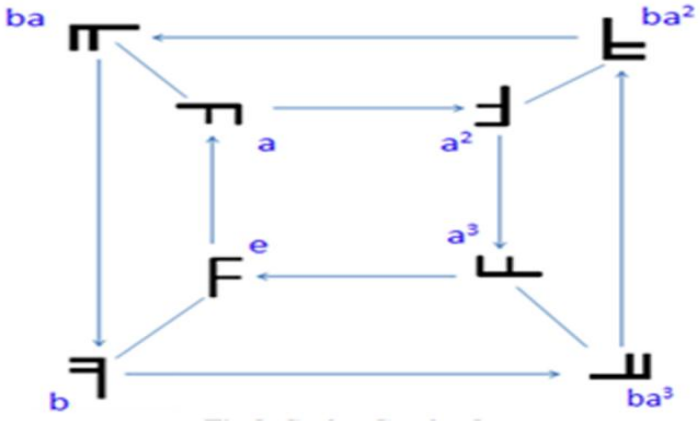


Figure 4.3: Cayley Graph of D_4

elements to revolve around the fixed axis, as elaborated in Figure 4.3.

Again, a table known by Cayley table is presented for a finite set of elements in all possible permutations by arranging its products in a square table reminiscent to multiplication. For the same, dihedral order 8 based Cayley table is shown in Table 4.1.

Table 4.1: Cayley Table

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	e	a^3	a^2	a
ba	ba	ba^2	ba^3	b	a	e	a^3	a^2
ba^2	ba^2	ba^3	b	ba	a^2	a	e	a^3
ba^3	ba^3	b	ba	ba^2	a^3	a^2	a	e

Finally, we are co-relating the same concept from mathematics. Here, the composition of eight different but interrelated operations for D_8 is specifically specified for the mathematical suites that will be used in cryptographic applications, where mathematics is the foundation for

almost all applications. Here is a similar consideration of the above concept on square glass; a different perspective to distinguish the same for the cryptography purposes is presented as a schematic representation in Figure 4.4. These are in the ordered group elements from G_1 to G_8 for rotations/movements and reflections in- $e, a, a^2, a^3, b, ba, ba^2, ba^3$, as a result. A detailed cryptographic applications scheme is considered in section 4.5.3 and 4.5.4.

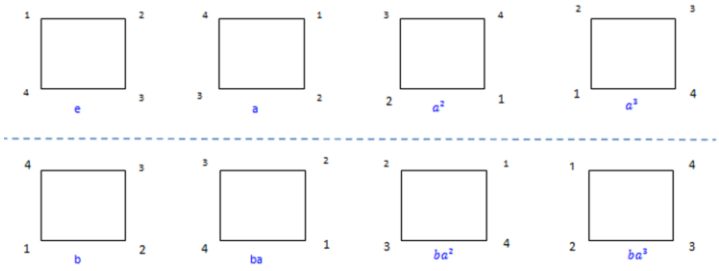


Figure 4.4: Schematic Representation on Dihedral 8

4.3.3 Quaternion Group

The Quaternion group [87] is a non-abelion, order of eight elements that forms of four-dimensional vector space over the real numbers. These are isomorphic to a subset of certain eight elements under multiplication. The group is generally indicated by Q or Q_8, and is given by the group representation $Q = (-1, i, j, k)|(-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1$ where 1 is the identity element and -1 commutes with the same. This is of the same order as Dihedral D_8, but the only difference is in its structure. So, it may be considered an immoderation of a Dihedral of order 8. The depicted Table 4.2 is a Cayley table for- Q_8:

Table 4.2: Cayley Table (Quaternion Group)

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	I	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	J	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	K	-j	j	I	-i	1	-1

4.3.3.1 Security Strength of Quaternion Group

Quaternion group using number theory gives multifold security properties in cryptography. The real beauty of quaternion is Noncommutative nature and multiplication on these group lie on a sphere in four-dimensional space. Due to this nature, the highest level of probable confusion can be achieved in applied applications and it can be derived for enormous applications. The used matrices and algebra (where multiplication order is important for end user applications) make its bigger significance for the future security proposals. The resultant of quaternion easily converts to other representations just like the two original unit quaternion, whereas from the adversary side also it is almost impossible to break such kind of scheme. Further, still to analyze and implement in cryptography is the need, which may give a high security specification on the quaternion group.

4.4 NONCOMMUTATIVE CRYPTOGRAPHY ON GROUPS AND RINGS

The mathematical rationalization over matrix group or ring is exemplified on $\mathrm{M}(\mathbb{Z}_{\mathrm{N}})$, based $\mathrm{N} = \mathrm{p}.\mathrm{q}$, where p and q are two secure primes. This is intractable, in view of the fact that $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M(\mathbb{Z}_{\mathrm{N}}), a \in (\mathbb{Z}_{\mathrm{N}})$ from $A^2 = \begin{pmatrix} a^2 & 0 \\ 0 & 0 \end{pmatrix} \in M(\mathbb{Z}_{\mathrm{N}})$ with no significant factors of N [78].

The above said ring can be enhanced with respect to security by using special or peculiar sparse matrices of rings elements.. As our contribution, shows the stronger security specifications on the above described sections 4.3.1.1 and 4.3.3.1 which are based on Heisenberg and Quaternion groups respectively. Further, due to Noncommutative nature of generated semi-ring elements for Dihedral order of 8 (presented in next section) also satisfies the properties of N very well. The key parameters over matrix ring elements are dedicated with the following accomplishments: (i) the center of a matrix ring over the matrix operations for scalar multiplication belong to the center of Ring elements, which is perfect suit for algorithmic properties. (ii) Polynomial function as a secret key doesn't reveal any secrets over the ring or is hard to find on modulo prime factors. Exponential growths on each word for length based attacks are further added as ingredients to give strength in the proposed scheme. (iii) The proposed assumptions are unique and irreversible on noncommutative properties. Therefore, it is more

suitable to cryptography.

4.4.1 Key Exchange Algorithm on Noncommutative

The Noncommutative key exchange cryptography works are reminiscent of Diffie-Hellman key exchange [88] similar to a commutative case, but the major distinction is the itinerary actions on selection of global parameters, generation of private keys, production rule for shared secret session keys, and encryption-decryption. The effectiveness of the algorithm depends on the impenetrability of computing the DLP. The security of the algorithm lies on the prime

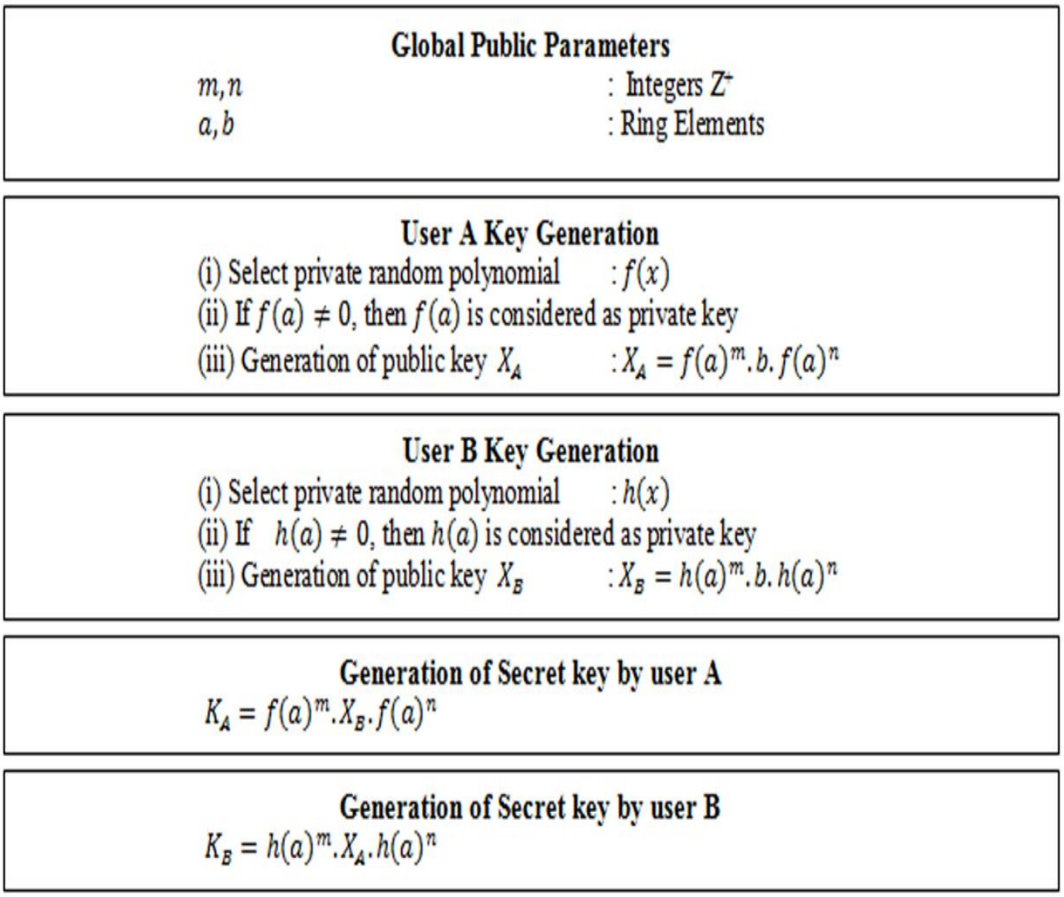


Figure 4.5: Key-exchange on Noncommutative Ring

factorization on two secure primes, random private polynomial chosen by user A and user B, respectively. A detailed elaboration through the numerical example on ring and Quaternion group for key exchange and encryption-decryption are presented in this section, which belong to the extra special group.

The key-exchange agreement over matrix ring elements is depicted in Figure 4.5, the global parameters are:

$$m = 3, n = 5, a = \begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix}, b = \begin{pmatrix} 1 & 9 \\ 3 & 2 \end{pmatrix}, N = 7 * 11$$

User A is chosen as their random polynomial- $f(x) = 3x^3 + 4x^2 + 5x + 1$. Evaluate the polynomial- f(a), if $f(a) \neq 0$ then, the polynomial will be considered as a private key for user A. The A's private key:

$$f(a) = 3\begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix}^3 + 4\begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix}^2 + 5\begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix} + 1.I = \begin{pmatrix} 19 & 20 \\ 28 & 44 \end{pmatrix} mod\ 77$$

Now, the generation of public key X_A by user A:

$$X_A = f(a)^m . b . f(a)^n = \begin{pmatrix} 19 & 20 \\ 28 & 44 \end{pmatrix}^3 . \begin{pmatrix} 1 & 9 \\ 3 & 2 \end{pmatrix} . \begin{pmatrix} 19 & 20 \\ 28 & 44 \end{pmatrix}^5 = \begin{pmatrix} 3 & 56 \\ 9 & 2 \end{pmatrix} mod\ 77$$

At the other end user B has chosen their random polynomial- $h(x) = x^5 + 5x + 1$. Further, to evaluate the polynomial h(a), if $h(a) \neq 0$ then, this polynomial value will be considered as private key:

$$h(a) = \begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix}^5 + 5\begin{pmatrix} 17 & 5 \\ 7 & 4 \end{pmatrix} + 1.I = \begin{pmatrix} 70 & 52 \\ 42 & 58 \end{pmatrix} mod\ 77$$

and the generation of public key for user B:

$$X_B = h(a)^m . b . h(a)^n = \begin{pmatrix} 70 & 52 \\ 42 & 58 \end{pmatrix}^3 . \begin{pmatrix} 1 & 9 \\ 3 & 2 \end{pmatrix} . \begin{pmatrix} 70 & 52 \\ 42 & 58 \end{pmatrix}^5 = \begin{pmatrix} 0 & 39 \\ 35 & 68 \end{pmatrix} mod\ 77$$

Finally, the session key extracted by the user A is K_A:

$$K_A = f(a)^m . X_B . f(a)^n = \begin{pmatrix} 19 & 20 \\ 28 & 44 \end{pmatrix}^3 . \begin{pmatrix} 0 & 39 \\ 35 & 68 \end{pmatrix} . \begin{pmatrix} 19 & 20 \\ 28 & 44 \end{pmatrix}^5 = \begin{pmatrix} 21 & 37 \\ 49 & 69 \end{pmatrix} mod\ 77$$

and the session key extracted from user B as K_B:

$$K_B = h(a)^m . X_A . h(a)^n = \begin{pmatrix} 70 & 52 \\ 42 & 48 \end{pmatrix}^3 . \begin{pmatrix} 3 & 56 \\ 9 & 2 \end{pmatrix} . \begin{pmatrix} 70 & 52 \\ 42 & 48 \end{pmatrix}^5 = \begin{pmatrix} 21 & 37 \\ 49 & 69 \end{pmatrix} mod\ 77$$

4.4.2 Key-Exchange Using Heisenberg Group (Upper Triangular Matrices)

Further, we applied the same algorithm for session key-establishment over a Heisenberg group. It is demonstrated on the global parameters, where assumptions are:

$$m = 3, n = 5, a = \begin{pmatrix} 1 & 5 & 7 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 6 & 9 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}, N = 7 * 11$$

For user A, a random polynomial is chosen as- $f(x) = 3x^3 + 4x^2 + 5x + 6$. Evaluate the

polynomial on f(a), if f(a) ≠ 0 then, polynomial value considered as a private key for user A:

$$f(a) = 3\begin{pmatrix}1 & 5 & 7\\ 0 & 1 & 4\\ 0 & 0 & 1\end{pmatrix}^3 + 4\begin{pmatrix}1 & 5 & 7\\ 0 & 1 & 4\\ 0 & 0 & 1\end{pmatrix}^2 + 5\begin{pmatrix}1 & 5 & 7\\ 0 & 1 & 4\\ 0 & 0 & 1\end{pmatrix} + 6I = \begin{pmatrix}18 & 33 & 29\\ 0 & 18 & 11\\ 0 & 0 & 18\end{pmatrix} mod\ 77$$

The generation of public key X_A by user A is:

$$X_A = f(a)^m.b.f(a)^n = \begin{pmatrix}18 & 33 & 29\\ 0 & 18 & 11\\ 0 & 0 & 18\end{pmatrix}^3 .\begin{pmatrix}1 & 6 & 9\\ 0 & 1 & 3\\ 0 & 0 & 1\end{pmatrix}.\begin{pmatrix}18 & 33 & 29\\ 0 & 18 & 11\\ 0 & 0 & 18\end{pmatrix}^5$$

$$= \begin{pmatrix}9 & 32 & 10\\ 0 & 9 & 71\\ 0 & 0 & 9\end{pmatrix} mod\ 77$$

At the other end user B has chosen his random polynomial- $h(x) = x^5 + 5x + 1$. Evaluated the polynomial h(a), the private key:

$$h(a) = \begin{pmatrix}1 & 5 & 7\\ 0 & 1 & 4\\ 0 & 0 & 1\end{pmatrix}^5 + 5\begin{pmatrix}1 & 5 & 7\\ 0 & 1 & 4\\ 0 & 0 & 1\end{pmatrix} + 1I = \begin{pmatrix}7 & 50 & 39\\ 0 & 7 & 40\\ 0 & 0 & 7\end{pmatrix} mod\ 77$$

and the generation of public key for user B:

$$X_B = h(a)^m.b.h(a)^n = \begin{pmatrix}7 & 50 & 39\\ 0 & 7 & 40\\ 0 & 0 & 7\end{pmatrix}^3 .\begin{pmatrix}1 & 6 & 9\\ 0 & 1 & 3\\ 0 & 0 & 1\end{pmatrix}.\begin{pmatrix}7 & 50 & 39\\ 0 & 7 & 40\\ 0 & 0 & 7\end{pmatrix}^5$$

$$= \begin{pmatrix}42 & 56 & 35\\ 0 & 42 & 0\\ 0 & 0 & 42\end{pmatrix} mod\ 77$$

Finally, the session key is extracted by the user A as K_A:

$$K_A = f(a)^m.X_B.f(a)^n$$

$$= \begin{pmatrix}18 & 33 & 29\\ 0 & 18 & 11\\ 0 & 0 & 18\end{pmatrix}^3 .\begin{pmatrix}42 & 56 & 35\\ 0 & 42 & 0\\ 0 & 0 & 42\end{pmatrix}.\begin{pmatrix}18 & 33 & 29\\ 0 & 18 & 11\\ 0 & 0 & 18\end{pmatrix}^5$$

$$= \begin{pmatrix}70 & 42 & 28\\ 0 & 70 & 0\\ 0 & 0 & 70\end{pmatrix} mod\ 77$$

and the session key is extracted by user B as K_B:

$$K_B = h(a)^m.X_A.h(a)^n$$

$$= \begin{pmatrix}7 & 50 & 39\\ 0 & 7 & 40\\ 0 & 0 & 7\end{pmatrix}^3 .\begin{pmatrix}9 & 32 & 10\\ 0 & 9 & 71\\ 0 & 0 & 9\end{pmatrix}.\begin{pmatrix}7 & 50 & 39\\ 0 & 7 & 40\\ 0 & 0 & 7\end{pmatrix}^5$$

$$= \begin{pmatrix} 70 & 42 & 28 \\ 0 & 70 & 0 \\ 0 & 0 & 70 \end{pmatrix} mod\ 77$$

4.4.3 Encryption-Decryption Algorithm on Heisenberg Group

The encryption-decryption procedure on Heisenberg group is offered in Figure 4.6.

Global Public Parameters

m, n	: Integers Z^+
a, b	: Ring Elements
M	: Message
$H(M)$	: Hashed Message

User A Key Generation

(i) Select private random polynomial: $f(x)$
(ii) If $f(a) \neq 0$, then $f(a)$ is considered as private key
(iii) Generation of public key X_A : $X_A = f(a)^m . b . f(a)^n$

User B Key Generation

(i) Select private random polynomial: $h(x)$
(ii) If $h(a) \neq 0$, then $h(a)$ is considered as private key
(iii) Generation of public key X_B : $X_B = h(a)^m . b . h(a)^n$

Encryption (by sender B)

C	: Ciphertext
D	: Decryption Key
$C = h(a)^m . b . h(a)^n$,	$D = H(h(a)^m . X_A . h(a)^n) \oplus M$

Decryption

$M = H(f(a)^m . C . f(a)^n) \oplus D$

Figure 4.6. Encryption-Decryption Algorithm on Noncommutative Group

The approach of Noncommutative cryptography, works same as in the general case, where our assumptions are:

$$m = 3, n = 5, a = \begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & 9 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 9 & 5 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}, N = 7 * 11, M = \begin{pmatrix} 27 & 19 & 25 \\ 34 & 8 & 7 \\ 45 & 5 & 9 \end{pmatrix}$$

User A randomly chosen a random polynomial $f(x) = 3x^3 + 4x^2 + 5x + 6$, then f(a) considered to be private key:

$$f(a) = 3\begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & 9 \\ 0 & 0 & 1 \end{pmatrix}^3 + 4\begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & 9 \\ 0 & 0 & 1 \end{pmatrix}^2 + 5\begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & 9 \\ 0 & 0 & 1 \end{pmatrix} + 6I = \begin{pmatrix} 18 & 33 & 13 \\ 0 & 18 & 44 \\ 0 & 0 & 18 \end{pmatrix} mod\ 77$$

The generation of public key:

$$X_A = f(a)^m.b.f(a)^n = \begin{pmatrix}18 & 33 & 13\\ 0 & 18 & 44\\ 0 & 0 & 18\end{pmatrix}^3 . \begin{pmatrix}1 & 9 & 5\\ 0 & 1 & 3\\ 0 & 0 & 1\end{pmatrix} . \begin{pmatrix}18 & 33 & 13\\ 0 & 18 & 44\\ 0 & 0 & 18\end{pmatrix}^5$$
$$= \begin{pmatrix}9 & 59 & 42\\ 0 & 9 & 49\\ 0 & 0 & 9\end{pmatrix} mod\ 77$$

Onward moving, user B randomly chose their own random polynomial $h(x) = x^5 + 5x + 1$ and computes private key if $h(a) \neq 0$:

$$h(a) = \begin{pmatrix}1 & 5 & 9\\ 0 & 1 & 9\\ 0 & 0 & 1\end{pmatrix}^5 + 5\begin{pmatrix}1 & 5 & 9\\ 0 & 1 & 9\\ 0 & 0 & 1\end{pmatrix} + 1.I = \begin{pmatrix}7 & 50 & 1\\ 0 & 7 & 13\\ 0 & 0 & 7\end{pmatrix} mod\ 77$$

and the public key generated for user B:

$$X_B = h(a)^m.b.h(a)^n = \begin{pmatrix}7 & 50 & 1\\ 0 & 7 & 13\\ 0 & 0 & 7\end{pmatrix}^3 . \begin{pmatrix}1 & 9 & 5\\ 0 & 1 & 3\\ 0 & 0 & 1\end{pmatrix} . \begin{pmatrix}7 & 50 & 1\\ 0 & 7 & 13\\ 0 & 0 & 7\end{pmatrix}^5$$
$$= \begin{pmatrix}42 & 28 & 35\\ 0 & 42 & 35\\ 0 & 0 & 42\end{pmatrix} mod\ 77$$

The sender of the public key treats as cipher text C, (in our case user B is sender):

$$C = h(a)^m.b.h(a)^n = \begin{pmatrix}42 & 28 & 35\\ 0 & 42 & 35\\ 0 & 0 & 42\end{pmatrix}$$
$$D = H(h(a)^m.X_A.h(a)^n) \oplus M$$

$$= H\left(\begin{pmatrix}7 & 50 & 1\\ 0 & 7 & 13\\ 0 & 0 & 7\end{pmatrix}^3 . \begin{pmatrix}9 & 59 & 42\\ 0 & 9 & 49\\ 0 & 0 & 9\end{pmatrix} . \begin{pmatrix}9 & 59 & 42\\ 0 & 9 & 49\\ 0 & 0 & 9\end{pmatrix}^5\right) \oplus \begin{pmatrix}27 & 19 & 25\\ 34 & 8 & 7\\ 45 & 5 & 9\end{pmatrix}$$
$$= H\left(\begin{pmatrix}70 & 21 & 35\\ 0 & 70 & 7\\ 0 & 0 & 70\end{pmatrix}\right) \oplus \begin{pmatrix}27 & 19 & 25\\ 34 & 8 & 7\\ 45 & 5 & 9\end{pmatrix} = \begin{pmatrix}12 & 42 & 57\\ 35 & 31 & 52\\ 44 & 4 & 30\end{pmatrix}$$

The original message

$$M' = H(f(a)^m.C.f(a)^n) \oplus D$$
$$= H\left(\begin{pmatrix}18 & 33 & 13\\ 0 & 18 & 44\\ 0 & 0 & 18\end{pmatrix}^3 . \begin{pmatrix}42 & 28 & 35\\ 0 & 42 & 35\\ 0 & 0 & 42\end{pmatrix} . \begin{pmatrix}18 & 33 & 13\\ 0 & 18 & 44\\ 0 & 0 & 18\end{pmatrix}^5\right) \oplus \begin{pmatrix}12 & 42 & 57\\ 35 & 31 & 52\\ 44 & 4 & 30\end{pmatrix}$$
$$= \begin{pmatrix}27 & 19 & 25\\ 34 & 8 & 7\\ 45 & 5 & 9\end{pmatrix}$$

4.4.4 Analysis and Strength of Proposed Scheme

We are now analyzing the computational hardness or complexity analysis with its related strength as a security and performance considerations (mostly on each parameter of algorithms):

Prime Factors of N - The proposed procedure stands on hidden prime factorization of N (N is absence in the proposed algorithm, but due to explicit clarification it is shown wherever needed) which are the below mentioned points in support of strong security analysis:

(i) Since $N = 7 * 11$ is based on two prime factors, and factorization of N is extremely difficult to find its exact factors due its computer intensive nature for large primes. To find an algorithm which does it fast is one of unsolved problem of computer science.

(ii) The time requires into prime factor grows exponentially, so if the algorithm uses large prime based integers, it is unrealistic to crack it down.

(iii) Prime factorization is mostly a unique problem, and all integers (except 1 and 0) are made up of primes, due this ingeniousness it becomes hard to encode any information of any length as a single integer is inflexible.

Private keys - A secret key generation is based on random chosen polynomial $f(x)$ or $h(x)$, since polynomial is irreducible in its nature if and only if it doesn't result as artifact in two polynomials. An integer analogy of prime polynomial is described as an irreducible polynomial. A polynomial contains the three classes of polynomials such as:

(i) Ordinary polynomial

(ii) Modulo prime based polynomial, and

(iii) Modulo prime based polynomial defines on another polynomial whose powers are in some integer n.

In class (i) arithmetic operation (addition, subtraction, and multiplication) is performed on polynomials using the rules of algebra, and division is only possible if field elements are coefficients of the same. Class (ii) contains the arithmetic operations as of (i), but the division result is used (in general) in quotient and remainder forms. This represents a special significance in cryptography because it gives a unique solution for the above prime factorization on specified problem. Here class (iii) is not elaborated; due to proposed approach is working on (i) and/or (ii).

Public keys - The polynomial functions of $f(x)$ or $h(x)$ to the power of m and n, with two multiplications on modulo prime is the basis for public key generation for respective senders and receivers. The generated public key (which passed into the medium) represents as a Discrete Log Problem (DLP) for the algorithm and since it is established on modulo prime based polynomials that are irreducible in these contexts. Adversaries try to conceptualize the secret key on the

global parameters and public key, those are freely available. According to proposed scheme, a large prime factor of N (standard length 160 bits) may be sufficient to make adversaries against it to get fruitful ideas or valid secret keys.

Timing Attacks - Timing attacks is a stunning way that abstract the pattern generated from the cryptographic algorithm and try to access the security appearance from electromagnetic signals released from the computer systems. The release of signals and transmissions are the part of computer operations. The signals are alarming in the two senses: (i) a random interference comes first, which can be only be burglars, and (ii) these signals can be amplified through some auxiliary equipments for some useful purposes. A report is available that are suggesting on electromagnetic radiation interference with radio navigation devices, as (i) it is a general procedure and it is not an issue to be considerable, but if (ii) is applied then who are interested in such pattern of abstract generation, the decoding and restoration can lead to vulnerable information about safety, feedbacks and/or secret information leakage, where an adversary tries to determine the secret key on amount of time taken by the computer to decipher the private message.

In real time practice, polynomial exponentiation on modular accomplishment does lead to extreme timing variations. So in this regards, Noncommutative be a practical choice for future work on such type of typical variations generations. Instead of the same, there are some countermeasures, which may lead to strengthen the measures in timing variation affects:-

Polynomial exponentiation time: As all exponentials take different time in polynomial generation before returning to give final result, so this one is simply a point to ponder, so performance analysis doesn't degrade its efficiency with its variances.

***Random Delay*:** One can get a better performance by adding a random delay to the exponentials in applied algorithms and may confuse the timing attacks.

***Blinding*:** It can confuse the adversary by multiplying a random number into the ciphertext before performing exponentiation. This can be one of the ways to out-reach adversaries from original ciphers.

Brute-Force Attacks - The brute-force attacks refer to finding all the possible secret keys. The defense against attacks shows a larger randomness and unpredictability behavior on a shorter key length on our proposed approach, since it is a special case of Elliptic Curve Cryptography

(ECC), therefore the algorithms is sufficiently working on a smaller length keys. The execution time of smaller length key takes a shorter time, so it is reflected a big impact on efficiency. A lot of reports are available regarding the computational performance for ECC and RSA algorithms, whereas our approach (Noncommutative) with regards to the efficiency, speed, and cryptanalysis is better than them.

Chosen-Ciphertext Attacks - This attack is a form of active attack, where adversaries try to find plaintext corresponding to its ciphertexts by its choice. The first choice may experience on decryption module on a random chosen ciphertexts, before the actual ciphertext is sent for an interested use. The second choice involves the same module on input of one's choice at any time, where these all are recorded and try to gain the actual plaintexts. As the presented algorithm experience a blind feedbacks, where the Noncommutative cryptography is not a vulnerable one to chosen ciphertext attacks (CCA) especially for ring or semi-ring, group and Heisenberg elements; because in CCA an adversary chooses a number of ciphertext and tries to decrypt with targeted private keys, where the chosen cipher text is hashed with the corresponding polynomial exponentials.

Simulation and Importance of Hash Uses - The simulation of hash H is based on power of 2 functions on Mat Lab tool. Where the importance of hash function dictates the following properties: (i) Output of hash generates pseudo-randomness for the standard cryptographic tests, (ii) Hash is in easy to compute for any given key that makes a practical use for hardware and software implementations, (iii) On a given hash H, computationally it is infeasible to find y, such that $H(y) = x$, (iv) For any pair (x, y) it is computationally infeasible to find $H(x) = H(y)$, is a strong collision resistant property, and (v) For any x block, it is infeasible (computationally) to find $y \neq x$, is a weak collision resistant property.

4.5 MONOMIALS BASED CRYPTOGRAPHY USING NONCOMMUTATIVE GROUPS AND SEMI-RINGS

The polynomials used in $\mathbb{Z}$ -Modular method for Noncommutative cryptography are based on the group elements that runs at the back end and its equivalent semi-rings elements works from the

front, known by the monomials generated schemes. In this regards the original information is hidden, whereas for an adversary it will be practically impossible to decipher the original information. Such kind of participation in computation is viewed as a special case. We have formulated the semi-ring elements that are working perfectly under the assumptions of our Dihedral order 8, which is a part of Extra Special Group. The section is first exploring the basic assumptions on monomials and then there are detailed proposed works.

4.5.1 Extension of Noncommutative Groups

A Noncommutative group $(G, ., 1_G)$ and ring elements- $(R, +, ., 1_R)$, its monomials can be defined as $\tau: (G, ., 1_G) \to (R, ., 1_R)$. The inverse map works monomials as $\tau^{-1}: \tau(G) \to G$ and it is also a well defined on its definition. For any two group elements $a, b \in G$, $\tau(a) + \tau(b) \in \tau(G)$ is also true. For a new element $c \in G$ assigned as $c \triangleq \tau^{-1}(\tau(a) + \tau(b))$, then c called as quasi-sum of a and b, and is denoted by $c = a \boxplus b$ [31]. Similarly for $k \in R$ and $a \in G$, then $k.\tau(a) \in \tau(G)$, afterword for any new element one can assign $d \in G$ as $d \cong \tau^{-1}(k.\tau(a)$, here called d as a quasi-multiple of a, and is denoted by $d = k \boxtimes a$. In final sense, the monomial τ is treated in a linear sense with the following equalities:

$$\begin{aligned}
\tau(k \boxtimes a \boxplus b) &= \tau\big((k \boxtimes a) \boxplus b\big) \\
&= \tau(d \boxplus b) \\
&= \tau\left(\tau^{-1}\big(\tau(d)\big)\right) \boxplus \tau(b) \\
&= \tau\left(\tau^{-1}\left(\tau\left(\tau^{-1}\big(k.\tau(a)\big)\right)\right)\right) \boxplus \tau(b) \\
&= \tau\left(\tau^{-1}\big(k.\tau(a)\big)\right) \boxplus \tau(b) \\
&= k.\tau(a) \boxplus +\tau(b)
\end{aligned}$$

For $a, b \in G$ and $k.\tau(a) + \tau(b) \in \tau(G)$, for function $f(x) = z_0 + z_1 x + \cdots + z_n x^n \in Z[x]$ can be defined as:

$$f\big(\tau(a)\big) = z_0.1_R + z_1.\tau(a) + \cdots z_n.\tau(a)^n \epsilon\, \tau(G)$$

Now, a new element assigned $e \in G$ as: $e = \tau^{-1}\big(f(a)\big)$

$$= \tau^{-1}(z_0.1_R + z_1.\tau(a) + \cdots z_n.\tau(a)^n)$$

If it is held to find the inverse of polynomials, called e as quasi-polynomial function f, denoted as

$e = f(a)$. For sake of clarity on any arbitrary $a, b \in G$, $k \in R$, $f(x) \in Z[x]$, $a \boxplus b, k \boxtimes a$ and $f(a)$ are not always well defined. The below theorem 3, is a natural and general scheme, which works for Noncommutative monomials.

Theorem 3: For any $a \in G$, and $f(x)$, $h(x) \in Z[x]$, if $f(a)$ and $h(a)$ are precisely defined, then it meets two conditions (i) $\tau(f(a)) = f(\tau(a))$, and (ii) $f(a).h(a) = h(a).f(a)$

Proof: (i) Due to property of monomials on quasi-polynomial, the group element for any function f applies with its equivalent ring elements, so in the intermediary function f results on ring or semi-ring R and is observed on numerical analysis it results in the same elements of ring R. It can also be validated on LHS and RHS consideration:

LHS: $\tau(f(a)) = \tau(G)$ $(\because f(a) = G, \text{is group elements})$

$= R$ $(\because \tau \; is \; a \; monomial, so \; \tau(G) \to R, since \; R \; is \; inverse \; of \; Group)$

RHS: $f(\tau(a)) = f(R)$ $(\because \tau(a) = R, is \; ring \; elements)$

$= R$ $(\because f(R) generates \; ring \; elements)$

Proof: (ii) $f(a).h(a) = \tau\left(\tau^{-1}(f(a))\right).\tau\left(\tau^{-1}(h(a))\right)$ $\left(\because \tau\left(\tau^{-1}(g)\right) = g, g \in G\right)$

$= \tau\left(\tau^{-1}(f(a)).\tau^{-1}(h(a))\right)$ $(\because \tau \text{ is a monomial})$

$= \tau\left(\tau^{-1}(f(a).h(a))\right)$ $(\because \tau^{-1} \text{ is monomial})$

$= \tau\left(\tau^{-1}(h(a).f(a))\right)$ $(\because \text{Theorem 1})$

$= \tau\left(\tau^{-1}(h(a)).\tau^{-1}(f(a))\right)$

$= \tau\left(\tau^{-1}(h(a))\right).\tau\left(\tau^{-1}(f(a))\right) = h(a).f(a)$

4.5.2 Further assumptions on Noncommutative Groups

Consider the assumption on Noncommutative polynomial version for group elements for any random pick up element- $a \in G$, and it is defined on a polynomial as $P_a \in G$ by- $P_a \cong \{f(a) \in \tau(G): f(x) \in Z[x]\}$. Then, the definition on group G over $(G, .)$ says for:

(i) **Polynomial Symmetrical Decomposition (PSD) Problems over Noncommutative Group G:** Given $(a, x, y) \in G^3$ and $m, n \in Z$, find $z \in P_a$ such that $y = z^m.x.z^n$.

(ii) **Polynomial Diffie-Hellman (PDH) Problems over Noncommutative Group G:**

Compute $x^{z_1 z_2}$ or $x^{z_2 z_1}$ for given a, x, x^{z_1} and x^{z_2}, where $a, x \in G$ and $z_1, z_2 \in P_a$.

The assumptions are on PSD or PDH for cryptographic definition on $(G, .)$ is mostly being intractable and polynomial probabilistic time algorithm doesn't subsist any clue to solve this problem in accurateness and admiration [77].

Theorem 4: The generalized extra-special p-group over the monomials are free from attacks.

Proof: Suppose the group on G with $(G, ., 1_G)$ is a Noncommutative group, and semi-ring R on $(R, ., 1_R)$ is semi-ring and it's monomials defined as $\tau : (G, ., 1_G) \to (R, ., 1_R)$, such that the group elements always work at the back end, and computation is only defined on the monomials semi-ring elements. In these regards, the original extent of the algorithm is always hidden. The working of this prime p-group is an example of hidden subgroup or subfield problem. Hence, the theorem proves that the generalized extra-special p-group over the monomials are free from attacks.

4.5.3 Monomials like Key Exchange Algorithm

The global parameters of the proposed algorithm, at dihedral order 8, for key exchange using monomials is presented in Figure 4.7, where our assumptions are as follows:

$$m = 16, n = 55, a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

and the relative monomials of group elements $\tau : (G, ., 1_G) \to (R, ., 1_R)$ represented below, respectively. At Dihedral group of order 8 is of 8 groups, we assumed the same from G_1 to G_8 and its corresponding ring monomials from R_1 to R_8. Such group and ring elements are assigned in sequence as $G_1 \to R_1, G_2 \to R_2, G_3 \to R_3, G_4 \to R_4, G_5 \to R_5, G_6 \to R_6, G_7 \to R_7, G_8 \to R_8$. These all will be used in cryptographic primitives.

$$G_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, G_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, G_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, G_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$G_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, G_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, G_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, G_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, R_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, R_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, R_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$R_5 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, R_6 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, R_7 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, R_8 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

In the computation process, ring elements are generated on negative modulo prime, where Lemma 1 is clearly-distinct.

Lemma 1: The variability generation for equivalent monomials ring structured elements in the range of $\{-1, 0, 1\}$ is negative modulo prime of (-2).

Proof: By inspection, it is observed the negative modulo prime on (-2) results in the variations of $\{-1,0,1\}$, which well-suits to an equivalence in the monomials like generation elements to our proposed scheme of Dihedral order of 8 (where Dihedral 8 is specially a part of extra special group).

Global Public Parameters

m, n : Integers Z^-

a, b : Group Elements from Ring

Suppose $(G, ., 1_G)$ is a non-commutative group, $(R, ., 1_R)$ is ring and $\tau: (G, ., 1_G) \to (R, ., 1_R)$ is a mono-morphism.

User A Key Generation

(i) $f(x)$: Random Polynomial Chosen by A

(ii) Select $f(x) \epsilon Z(x)$ at random so that $f(a)$ is well defined i,e $f(\tau(a)) \epsilon \tau(G)$ then user A takes $f(a)$ as private key X_A : $X_A = f(a)^m.b.f(a)^n$

User B Key Generation

(i) $h(a)$: Random Polynomial Chosen by B

(ii) Select $h(x) \epsilon Z(x)$ at random so that $h(a)$ is well defined i,e $h(\tau(a)) \epsilon \tau(G)$ then user B takes $h(a)$ as private key X_B : $X_B = h(a)^m.b.h(a)^n$

Generation of Secret Shared Session key by user A

$K_A = f(a)^m.X_B.f(a)^n$

Generation of Secret Shared Session key by user B

$K_B = h(a)^m.X_A.h(a)^n$

Figure 4.7: Monomials Key-exchange on Noncommutative Ring

The user A chooses a random polynomial $f(x) = 4x^2 + x + 2$, and on $f(a) \neq 0$, the secret/private key elected for user A as $f(a) = \tau^{-1}\left(f(\tau(a))\right)$

$$= \tau^{-1}\left(4\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + 2\right)$$

$$= \tau^{-1}\left(\begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix} mod\ (-2)\right) \qquad [\because \text{Lemma 1}]$$

$$= \tau^{-1}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \xrightarrow{R_5 \to G_5} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

The generation of public key X_A:

$$X_A = f(a)^m . b . f(a)^n$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{16} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{55}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Further, a random polynomial chosen by user B as $h(x) = 3x^4 + x^3 + 4x^2 + 3x + 4$ and computes private key: $h(a) = \tau^{-1}\left(h(\tau(A))\right)$

$$= \tau^{-1}\left(3\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^4 + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^3 + 4\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 + 3\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + 4\right)$$

$$= \tau^{-1}\left(\begin{pmatrix} 3 & 6 \\ 2 & 3 \end{pmatrix} mod\ (-2)\right) \qquad [\because \text{Lemma 1}]$$

$$= \tau^{-1}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

And generation of public key for user B, afterwards sends them to user A:

$$X_B = h(a)^m . b . h(a)^n$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{16} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{55} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Now, user A extracts the session key as:

$$K_A = f(a)^m . X_B . f(a)^n$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{16} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{55} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

And user B extracts the session key as:

$$K_B = h(a)^m . X_A . h(a)^n$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{16} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{55} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

4.5.4 Monomials like Encryption-Decryption Algorithm on Noncommutative Cryptography

The way for encryption and decryption module for monomials algorithm is presented at dihedral order 8, as is shown in Figure 4.8 on step-by-step procedure (as carry-out below). The algorithm

is presented on two random primes p and q, such that $q|p-1 \neq 0$, generator function g is an order of q and message M. The numerical dictation is elaborated here, where global assumptions are:

$m = 12, n = 19, a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, p = 23, q = 11, g = 6,$ and $M = 17.$

The random polynomial $f(x) = 2x^5 - 5x^2 + 3$ is chosen by user A, the private key:

Global Public Parameters	
m, n	: Integers Z^+
a, b	: Group Elements from Ring
p, q	: Secure Primes
g	: Generator Function
M	: Message
Suppose $(G, ., 1_G)$ is a non-commutative group, $(R, ., 1_R)$ is ring and $\tau: (G, ., 1_G) \to (R, ., 1_R)$ is a mono-morphism.	
User A Key Generation	
(i) $f(x)$	: Random Polynomial Chosen by A
(ii) Select $f(x) \in Z(x)$ at random so that $f(a)$ is well defined i,e $f(\tau(a)) \in \tau(G)$ then user A takes $f(a)$ as private key X_A	: $X_A = f(a)^m . b . f(a)^n$
User B Key Generation	
(i) $h(a)$	: Random Polynomial Chosen by B
(ii) Select $h(x) \in Z(x)$ at random so that $h(a)$ is well defined i,e $h(\tau(a)) \in \tau(G)$ then user B takes $h(a)$ as private key X_B	: $X_B = h(a)^m . b . h(a)^n$
Encryption (User B)	
Cipher Text	: C
Decryption Key	: D
C	: Sender Public Key
D	: $H(h(a)^m . X_A . h(a)^n) \oplus M$
Decryption (User A)	
Original Message M'	: $H(h(a)^m . C . h(a)^n) \oplus M$

Figure 4.8: Monomials Encryption-Decryption Algorithm on Noncommutative

$$f(a) = \tau^{-1}\left(f(\tau(a))\right)$$

$$= \tau^{-1}\left(2.\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^5 - 5.\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 + 3\right)$$

$$= \tau^{-1}\left(\begin{pmatrix} 8 & 1 \\ 5 & 8 \end{pmatrix} mod\ (-2)\right) \qquad [\because \text{ Lemma 1}]$$

$$= \tau^{-1}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \overset{R_5 \to G_5}{\Longrightarrow} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

The public key is generated as X_A:

$$X_A = f(a)^m . b . f(a)^n$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{12} . \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}^{19}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Moving ahead, user B choose its own random polynomial $h(x) = 9x^4 + x^3 + 4x^2 + 9x + 4$ and computes private key as $h(a) = \tau^{-1}\left(h(\tau(A))\right)$

$$= \tau^{-1}\left(9\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^4 + \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^3 + 4\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^2 + 9\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} + 4\right)$$

$$= \tau^{-1}\left(\begin{pmatrix}9 & -4\\ 12 & 9\end{pmatrix} \bmod (-2)\right) \qquad [\because \text{ Lemma 1}]$$

$$= \tau^{-1}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$$

The public key is generated for user B as X_B

$$X_B = h(a)^m . b . h(a)^n$$

$$= \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}^{12} \cdot \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix} \cdot \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}^{19} = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}$$

In the next step, we need to use a hash function, where we are exploring the same through Lemma 2, then.

Lemma 2: The hash function is defined on H, which works as follows $H: \begin{pmatrix}1 & 2 & 3 & 4\\ \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4\end{pmatrix} \to \left(g^{2^0.\sigma_1 + 2^1.\sigma_2 + 2^2.\sigma_3 + 2^3.\sigma_4}\right) mod\ p$

Proof: By hypothesis for hash H as assumed by Cao et al. 2007 [78], which is based on Dihedral order of 6 for hash- $H: \begin{pmatrix}1 & 2 & 3\\ \sigma_1 & \sigma_2 & \sigma_3\end{pmatrix}$. In the present work, as a contribution, the authenticity of hash is preserved by applying to Dihedral order of 8 (a part of extra special Group) without hampering the original concepts.

Suppose user B is sender, then, according to our proposed algorithm its public key treats it as our cipher text. The decryption key D is assigned as:

$$D = H(h(x)^m . X_A . h(x)^n) \oplus M$$

$$= H\left(\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^{12} \cdot \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^{19}\right) \oplus 17$$

$$= H\left(\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right) \oplus 17$$

$$\xrightarrow{R_2 \to G_2} \left(\left(g^{2^0.4 + 2^1.1 + 2^2.2 + 2^3.3}\right) \bmod p\right) \oplus 17 \qquad [\because \text{ Lemma 2}]$$

$$= \left(\left(6^{2^0.4+2^1.1+2^2.2+2^3.3} \right) \bmod 23 \right) \oplus 17$$

$$= \left((6^{38}) \bmod 23 \right) \oplus 17 = 6 \oplus 17 = 23$$

Now, the receiver A decrypts the message:

$$= \mathrm{H}(\mathrm{f(x)}^{\mathrm{m}}.\mathrm{Cipher}.\mathrm{f(x)}^{\mathrm{n}}) \oplus \mathrm{D}$$

$$= \mathrm{H}\left(\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}^{12} . \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}^{19} \right) \oplus 23$$

$$= \mathrm{H}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \oplus 23$$

$$\xrightarrow{\mathrm{R_2 \to G_2}} \left(\left(\mathrm{g}^{2^0.4+2^1.1+2^2.2+2^3.3} \right) \bmod \mathrm{p} \right) \oplus 23 \qquad [\because \text{ Lemma 2}]$$

$$= \left(\left(6^{2^0.4+2^1.1+2^2.2+2^3.3} \right) \bmod 23 \right) \oplus 23$$

$$= \left((6^{38}) mod\ 23 \right) \oplus 23 = 6 \oplus 23 = 17$$

4.5.5 Security Analysis on Monomials

The security strength analysis as presented in section 4.4.4 for general structure schemes and it also works in a similar fashion for monomials structures like schemes. There are following factors in co-relation to the same which play a crucial role for the cryptographic schemes generation such as: (i) Generation of equivalent monomials ring elements on negative modulo prime behave like semi-ring elements and these are considered as a natural generalization of Noncommutative in the sense that the binary addition and multiplication operations are not required to be commutative. The semi-group action suggests the exponential growth on key, which doesn't have any chance to find the solution, (ii) In hash generation (as Lemma 2) prime factorization of P keeps all the similar analysis results for cryptographic existence as presented in previous section, (iii) Since the generation of private keys and public keys are based on monomials like structured elements, where the working scheme is initiated on monomials semi-ring elements for equivalent group elements. This means that the original information of the group elements is totally in hidden form. The original elements are used for verification purposes only in proposed work. The generated Discrete Log value doesn't keep any significant information for adversaries, (iv) DLP provides a big conflict of interest on randomness and unpredictability generation for secret keys that also maintains a balance between key sizes and

security extents, so in this regards the same brute force attacks and chosen-ciphertext attacks are extremely resisted by the proposed scheme.

4.5.6 Efficiency Issues on General and Monomials Noncommutative Schemes

For Noncommutative monoids, $F_{a^t}{}^{(b)} = a^t.b.\overline{(a^t)}$ it first computes a^t, then its inversion $\overline{(a^t)}$ and finally takes two multiplication in the underlying implementations. Here t represents either to be m or n for the polynomial function F. When t is considered to be in big digits, the computer arithmetic successively does doubling, rather than multiplying 'a' for t times, so in this case the performance evaluation takes $O(log_2(t))$ times to complete the task. In the present scenario 160 bits long t is enough to resist exhaustive attacks. The assumptions apply on length of group elements G (here proposed extra special group is with one of the latest and longest group lengths) such as $a, b, a^t, F_{a^t}{}^{(b)}$ to be a polynomial which is for a system security parameters, where the results are generating using the conventional (bit-by-bit) operations.

Moreover, for the secure and efficient architecture of the group elements, it represents the following facts regarding the same:

- ✓ Using the above described representation of group G element is unique. Otherwise the scheme (proposed) can't work.
- ✓ The transition from group G elements to its equivalent ring elements finishes efficiently. Otherwise, the scheme is impractical.
- ✓ $F_{a^t}{}^{(b)}$ doesn't reveal any information regarding polynomial a^t. Otherwise, the proposed assumptions (in algorithm) can suffer from the length based attacks.

4.6 BASIC LENGTH BASED ATTACKS

It is a heuristic procedure for finding the recipient's secret keys and is representing one of the procedures for recovering each of the conjugating factors as a major goal. The successful procedure results in an actual Conjugator as a product of group elements. The length based attack [89], [44] on Dihedral order 6 is presented in [91]. Our proposed approach is based on Dihedral order 8, i.e., k = 4, number of elements, play an enormous generation of a subset of 8 group elements defined as: $S_G = \{g_1^{\pm 1}, g_2^{\pm 1}, g_3^{\pm 1}, g_4^{\pm 1}\}$. We consider a random input series y =

$g_1 g_2^{-1} g_3 g_4^{-1}$, for length n=4. On chosen input sequence, the operation performs on 2k-ary tree. It starts processing from an empty word e, and searches for one child from 8 group node elements, with successful generation of 8 individual groups. For each element presented in input sequence is traced on successful generation. This procedure repeats until some n input of y_n length chosen for $y = y_1 y_2 \ldots . y_n$ is satisfied, as shown in Figure 4.9. This is based on the n^{th} level that contains $(2k)^n$ leaf-nodes elements. For every leaf-node is likely to be a potential value for y. The fact behind solving the CDP is easy but the fact to solve the CSP is unavailable, so it can be considered to be secure against the brute force search.

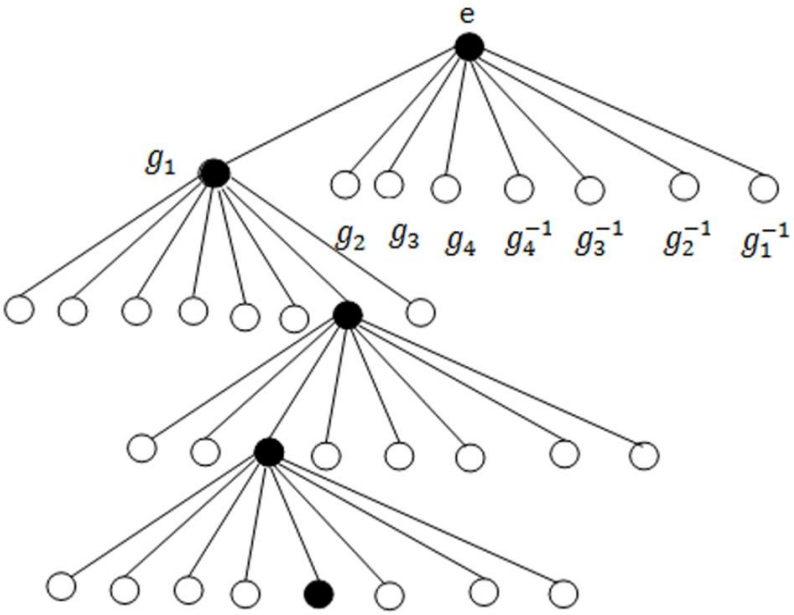


Figure 4.9: Process of generating $y = g_1 g_2^{-1} g_3 g_4^{-1}$

For example, during the process of searching, if there are two children-nodes P and Q with equal length, and if the algorithm wrongly predicts any one of them, the algorithm it makes to fall in exponential growth in the worst case as negligible solution. On average, 8 candidates (in Dihedral order 8) nodes in each level represent the time complexity on $O(8^{2n})$ for all n words per each level length, on the success or failure attempts.

The attack process is reversed for searching an instance for the 2k-ary tree. This means that attack is a reversal procedure, which works on successful cryptanalysis, at first level it should to need to satisfy 64-elements from 8-groups, similarly for the second level, it should again need to satisfy the same, and it should be repeated for word length input. An example is dictated on the target nodes represented as a darken node that are forming as optimal path searched (as shown in

Figure 4.10). The result is to find the attack on the proposed strategies, here which is only an indication on decomposition of y.

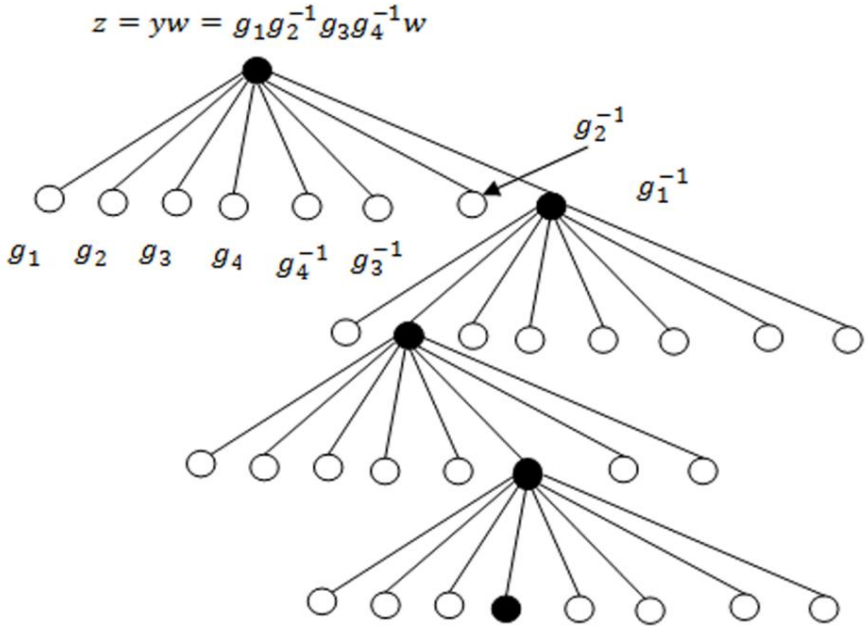


Figure 4.10: Process of decomposing $y = g_1 g_2^{-1} g_3 g_4^{-1}$

4.6.1 Analysis on Length Based Attacks

Dihedral order of *8* uses *4* (four) elements to form one group of *8* elements each, (a total of *8* group formation with a total of *64* elements), so adversaries (attackers) try to obtain the input sequence on level-by-level basis, at the first level an adversary need to satisfy *64* corresponding elements, again for the second level needs to satisfy the next *64* corresponding elements and it will continue to repeat until length reaches the maximum length. So, one can represent its complexity in the worst case as- $O(8^{2n})$. Here Conjugacy Decisional Problem (CDP) can be easily applied according to algorithm for the same, but Conjugacy Search Problem (CSP) doesn't work correctly. The CDP and CSP are the two advantageous approaches for making the exponential impulsiveness and arbitrariness for non-negligible solution. Here no such Conjugacy search problem exists so as to solve such large scaled problems. Therefore, in the concluding remarks it can be mentioned that our proposed problem is making a big impact in regards to cryptographic schemes.

Further, the performance may also improve using the following artillery variations by using memory uses, repetitions avoidance, look-ahead, alternative solutions and Automorphism attacks implementation into the algorithms. A brief idea is presented below:

Memory Uses: To compute the $2kn$-child nodes from the N subtrees, the width of search memory increases that chooses the shortest N one's of the subtrees in computations in next always. As a result, the width search is enhanced in range from 1 to N. According to principle algorithm becomes efficient, and works in exponential. As an example, the algorithm degenerate in its exponential forms and in the N candidates list the right node is difficult enough to generate through any loop. If an input consists of y_j, the condition that satisfies for word length of- $l(y_j w_{j+1}) < l(w_{j+1})$, where- $w_{j+1} = y_{j+1}$ to y_n, say y_j left multiplies w_{j+1} formulate its length gets reduced. So, it can be considered, as corrected node is not present in N list candidates and always increase in child nodes. Therefore, perceptibly on successful attacks (rate) will decrease.

Repetitions Avoidance: Usually repetitions avoiding is an improvement enclosed in research. A hash table is maintained in recording of visited nodes, and chance in the search tree may be the two nodes. If same valued node appeared again, then from candidate list node value of the same will be cancelled. So, to improve the algorithm, avoiding repetition method used in list not only improves efficiency but also prevents trapping through the use of algorithm in a closed loop.

Look-ahead: This increases search in depth, here is a possible way to make a practical choice to avoid attacks through the use of algorithm. For better algorithm this is one of the promising optional problem, the cost of traversing time at n-level subtree is $(2k)^n$. The algorithm increases in length of multiple right nodes for n-steps; the look-ahead problem never finds the right node. Thus, the algorithm again falls into exponential search.

Alternative solutions: The alternative solution is a specific one, which is generating on the monomials like the cryptographic schemes. This type of improvement is much more efficient, and in addition to that it doesn't change the search complexity. It helps to infinitely decrease the search time to find the right nodes. But, one of the basic conditions with this algorithm is that search direction should be correct. A large possibility is there for the fall the algorithm into an exponential search, if once it enters into wrong sub-trees.

Automorphism attacks: Under the parameters selected, the random Automorphism functions are extremely allied to each other on the random polynomial chosen for the participants, so the generation of these values is considered being negligible.

4.7 SUMMARY

In the chapter, the Noncommutative cryptographic scheme on the extra special group for the multidisciplinary perspective has been considered. Regarding this the minimum group of the dihedral changes from D_3 to D_4, which enhances the search space, and provides two additional group benefits of Heisenberg and Quaternion groups, that makes our proposal stronger than all the previously predicted groups. The scheme processed at the Noncommutative platform is for the prospective advantages of typical sparse matrices for general structures like group, ring or semi-ring elements. The proposed security assumptions are based on the hidden subgroup or subfields problem (HSP) on the random polynomials chosen for end users, and monomials generations is presented where Conjugacy search problem (CSP) is likely to be intractable. For the adversary, the attacks like length based, brute-force, Automorphism, becoming negligible.

CHAPTER 5

EFFECTIVE SIGNCRYPTION APPROACH FOR SECURE CONVENTION FOR MULTILAYER CONSENSUS USING ECC

The used algorithm in cryptography represents the facts for computation and/or computation costs in general. The motivation for any problem is the primitive generators that make the protocol a big advantage over the technology augmentation. This chapter presents a methodological approach on session specific challenge-response protocol for a better, improved and stronger security on reduced costs. The basic primitives are applied on Diffie-Hellman and Elliptic Curve Cryptography. The purpose is providing the security properties for protocol compositional logic that focuses on privacy rights in information assessment in multidisciplinary obligations. In addition, we portrait a signcryption approach for password authenticated key exchange protocol for multilayer consensus, which logically combines individual signature and encryption cost in the form of reduced computational cost and communications cost in single stride of operation. The overall computation time potentially is reduced for the proposed methodology on signature and key generation. The results for ECC based multilayer consensus of key generation approach are tested on Automated Validation of Internet Security Protocol Architecture (AVISPA) tool and SPAN tool. Further, by preserving the definition of signcryption, we enhanced the same scheme in comparison to the other proposed schemes.

5.1 INTRODUCTION

The challenge-response (C-R) protocols are one the recent research trends in cryptography; the mathematical modeling is moved around the process calculus. It is included the actions to generate new random numbers, perform encryption and signature, send or/and receive messages, finally performing decryption with verification with matched digital signature. The security proofs allow the protocols using combining of their independent proofs in parts. Secure composition as it designs in such a way that may not degrade and does not affect its own existing security so it has considered itself as a difficult security problem. This philosophy is more amenable for automation of security protocol analysis, where the cryptographic assumption considered being perfect in speedup in computation costs and communication costs, energy

minimization, respective applicability for applications, etc. The major thing is in protocol derivational logic is to develop further derivational system approach on behalf of logical methods, where the protocol analysis concerns to the soundness theorems. Datta [93] has presented an innovative framework for secure composition on its formal methods such as: *Protocol Composition Logic (PCL)* and *Protocol Derivation System (PDS)*. PDS is syntactic support approach in derivations to start from basic components make complex protocols and combines or extends in a sequence of operations over the refinements, transformations and compositions. Floyd-Hoare logic is a foundation of PCL that supports axiomatic proofs for protocol properties [94]. The PCL objective is to form a proof method for every applicable derivation for PDS. Therefore it may also be enabling its security proofs, and may also being applicable in parallel development for others protocols [95]. Any protocol execution contains as assertions associated with the same. The powerful possible observation offers reason to leaving all sprints of the protocol without any logics. The basic operation for ISO-9798-3 based on Diffie-Hellman exponential as (CR) protocol considers, as shown in Figure 5.1, that represents to show the messages how are sent by one and may be received by other. The basis of execution consists of protocol on initiator role and responder role, respectively. The initiator principle role is executing to generate a fresh random number, send the message with its generators to peer; the Responder receive message of its peer (Sender) with source address; verify the same message that contains the signature in anticipated format, and at the end both should be ready to send a subsequent another messages with signature of initiator and responder [96].

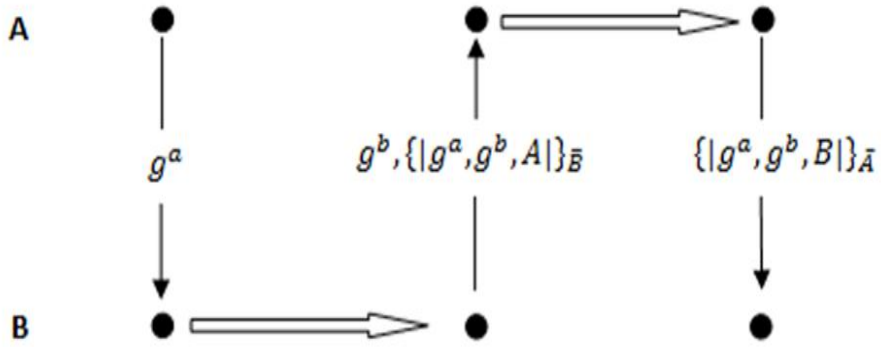


Figure 5.1: ISO-9798-3 Protocol

The backbone of security protocol is the foundational basis that is making certain to forward correctness in many distributed systems to error prone. In relation to presented protocols that contain security redundancies or flaws in the literature of subsequent sections. A simple logic is

described as a consequence of communication and its progression towards the authenticated trustworthy parties involved in authentication protocols. Further, we consequently explained our proposed work formally for a variety of protocol families that ascertain the errors and naunces, and instead of that suggest improvements in them.

We have given a brief idea with intensification of Elliptic Curve Cryptography (ECC) in the next section, which considers multilayer consensus key generations using the same. Afterword's signcryption based approach is applied which reduces the computation cost as well as communications cost.

5.2 ELLIPTIC CURVE CRYPTOGRAPHY

The cryptography heart is fame for its Discrete Logarithmic Problem (DLP), it acts as pivotal role on fundamental basis in security systems. At a lower cost, high speed computational algorithm and an incorporation of the exciting feature that keep with greater significance and is always a demanding issue. For efficient implementation of cryptographic protocols are playing a central role for the same. Cryptographic algorithms used in the approach which are slow in running approach impinged the customer dissatisfaction and inconvenience. It is very clear now that computation and communication security with faster algorithms run are leading in high performance and high speed.

Elliptic Curve Cryptography (ECC) [12] was proposed in 1985 by Neal Koblitz and Victor Miller. With rapid growth as in the recent state of affairs using the ECC algorithm is playing an important role and assumed to be secure according to NIST guidelines released in 2012. These types of contribution are also possible by except of ECC but they require higher key length. Due to this increased length, the computation costs and/or communication costs involved in the method are not longer suitable for short-memory devices. ECC is one of the techniques that are being used to provide the same level of security on shorter sizes key. But, for the research point of view still huge improvement is possible. The possible cost minimization is available in the literatures in overall consideration [13], is one of our motivation.

The core building block of the public key cryptography for DLP on ECC is presented on two P and Q points on the elliptic curve for the secret key k, such that $Q = kP$ [14]. This procedure restrains itself as a repeated point doubling (DBL) and point addition (ADD) operations.

It has been considered as an effective alternative approach relative to RSA algorithm of an already established due to following reasons- low entropy random numbers, lack of forward secrecy, chosen cipher-text attacks, higher complexity, the mathematical attacks etc. It also guarantees services on shorter keys for ECC security. Less arithmetic cost, time saving and less space for key storage are the special benefits, when keys are transmitting the same. These characteristics make ECC is one the right choice in security to incorporate the feature in mobile devices, online banking, smart cards, routers, consumer electronics items, printers, bridges, automotive, network devices, and many more are still be possible. Increased ECC evidence can be evinced by its inclusions in the most credited standards organizations for National Institute of Standards and Technology (NIST), International Standards Organization (ISO), American National Standards Institute (ANSI), and Institute of Electrical and Electronic Engineers (IEEE).

Hardware encryption devices are being used for the cryptographic algorithms that are running on a physical and general purpose security for the most operating systems. These devices are providing high speeds, high performance and at most security services. ECC is mostly best used due to exhaustive where limitation in resources for devices is and prompting for feasibility for high speed demands.

In cryptographic field, ECC has attracted the most attention of researchers in last two-and-half decades and dominating DSA/RSA system approaches. The extension of ECC is providing better performance as it is being used in the cryptosystems because of an improved version of algorithm, the uses of special functionalities and use of specialized curves. The major thought being it works on less memory and has much faster computation. The requirements of memory size execution and code sizes are also smaller. ECC is an appropriate algorithm that works on smaller key length and makes for an efficient practical application. These are based on two fields such as prime and binary fields for ECC. A large amount of published research is offering an interesting standard prime field based alternative in cryptosystems, the reason being that for the same security level, it requires less memory and provide much faster performance. The elliptic curve scalar multiplication is evaluating (on general) by (27) equation-

$$\begin{cases} y^2 = (x^3 + ax + b) \bmod p \text{ where } (x, y) \in \mathbb{Z}_p \\ (\text{for lagre prime field }) \; p > 3 \; a, b \in \mathbb{Z} \text{ and } 4a^3 + 27b^2 \neq 0 \bmod p \end{cases} \tag{27}$$

The scalar multiplication used in the ECC is the backbone for every algorithms used in ECC primitives. These are principally based on three main approaches. The first one is based on prime

or binary field operations in the underlying finite-field, and these are en-routing itself as alternative replacements for better solutions. The second approach is the computation of scalar multiplication on behalf of the applied algorithms that decides its complexity cost [97].

The National Institute of Standard and Technology (NIST) [98] document specifies with an objective as an authentication and integrity in cryptography. It means the discrete logarithmic problem works as key role in the medium and assumptions in the form of unpredictable for almost all applications.

This chapter is presenting the contents into four (04) sections. A protocol derivational approach is presented, in section 5.3. In section 5.4, Multilayer Consensus ECC-based password authenticated key exchange (PAKE) as an auxiliary model is presented for standard ECC protocol. Section 5.5, a formal verification approach is depicted on AVISPA & SPAN tool. Finally in section 5.6 is presented applicability of signcryption with the enrichment to the applications.

5.3 MOTIVATION TOWARDS DERIVATION OF SECURE PROTOCOL COMPOSITION

Protocol Derivation System (PDS) and Secure Composition of Protocol are addressed the two central specification under the security framework [94]. The aspiration is in developing methods for their complex protocols as security aspects by identifying and/or independent combination of their independent proofs. PDS supports logical approach in derivations which initiate from the basic component and extend or combine a component sequence of compositions, transformation and refinements operation. They consider a list of elementary building block elements, encryption set operations which replaces the same with an encrypted nonce for plaintexts, then transfer the same into specific channel and at the end it should be recovered as unintelligible, respectively. It consist a set of roles involment like to be a server, an initiator and a responder, where each plays a role of actions on desired protocol on a sequence of input, output operations. A common shared secrete key is formed on behalf of the executing roles played by their own private signing keys on generated nonces. A component C_1 for Diffie-Hellman is an example that is sharing a key on $g^{ir} \bmod q$ and it gives a sign for communication in between two parties where mostly the passive attacker usually difficult to be discovered. Component C_2 is considered as

signature-based authenticator at the other end as challenge-response signature on its generated nonce [99]. The standard authentication mechanism is shown below-

$$I \rightarrow R: m;\ R \rightarrow I: SIG_R(m) \tag{28}$$

In the cryptography, it is assumed that m is a nonce or fresh value. Public key certificate possessed by responder R to verify it's signature using the transformation and refinements operations. The refinement shows the message component instances replaced by unidentifiable means, such type replacement gives guaranteed freshness, guarantees from internet key exchanges, protection in identity enclosed against from passive attackers, forward secrecy etc. A basic thought of the existing refinements have presented here. For protection in identity, the first refinement $R_1, SIG_x(m) = E_k\big(SIG_x(m)\big)$ works, the second refinement $R_2, SIG_x(m) = SIG_x\big(HMAC_x(m, ID_x)\big)$, proves that the signature term is itself generated from x and in addition key hash proves that x possesses key K. For Internet Key Exchange (IKE) is an important property for mutual authentication. The refinement $R_3, SIG_x(m) = SIG_x(m), HMAC_k(m, ID_x)$, same purpose is served like R_2 but instead of the same it is used for Just Fast Key protocol as a derivation. Refinement $R_4, SIG_x(m) = SIG_x(m, ID_y)$, is assumed for x possess the required information $Y's$ is identified as public key certificate. The refinement $R_5, g^x = g^x, n_x$ where n_x is a spanking new to serve the two purposes (i) to provide guarantee as fresh value for each in order to prevent in replay attack and (ii) to derive the secret key. Refinement $R_6, SIG_{x\,(m)} = SIG_x(m), ID_x$, where Id_x refers to public key certificate for x and the verification keys don't possess them for others. The public key certificate is used in the session key establishment. Further, Refinement $R_7, SIG_x(m) = E_k(m), HMAC_{k'}\big(role, E_k(m)\big)$ where k' and k identify the protocol shared among initiator and responder. Just Fast Key formulation is used using this refinement. A hashed key includes encrypted signature.

Transformations in the other way are classified in three (03) parts such as- Message Content Move T_1, Binding T_2 and Cookie T_3. T_1 message is a move from one state to another but any freshly generated data is not contained by the same. Transformation T_2 adds (in general) binding information from one the protocol to different in some significant form and should be unpredictable state as:

$$\begin{array}{ll} I \rightarrow R: m & I \rightarrow R: m \\ R \rightarrow I: n, SIG_R(m) \quad \Rightarrow & R \rightarrow I: n, SIG_I(m, n) \end{array} \tag{29}$$

$$R \rightarrow I: n, SIG_R(m) \qquad\qquad I \rightarrow R: SIG_I(m, n)$$

The Cookie T_3 transformation is a freshly generated data stored in small that makes a protocol resistant to DOS (blind) attack. When each time user logins to browser it adds cookies back to server that can also are considered on website as previous activity information.

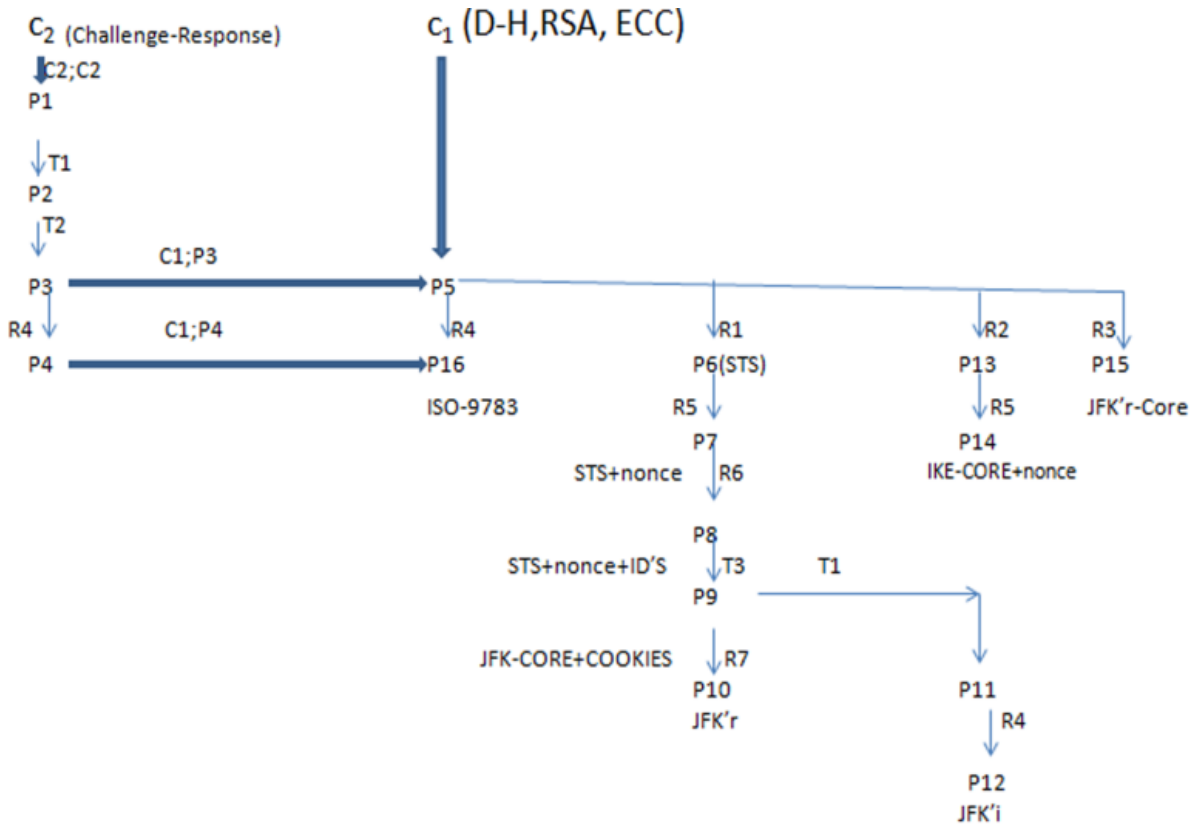


Figure 5.2: Protocol Derivation System (PDS) approach

For protocols derivation of an innovative approach is proposed, as depicted in Figure 5.2, by Datta. We are presenting a broad aspect towards the protocol derivation using compositional logics:

Protocol P_1 obtains from two symmetric component C_2 as sequential composition as:

$$I \rightarrow R: m;\ R \rightarrow I: SIG_R(m);\ I \rightarrow R: n;\ R \rightarrow I: SIG_I(n) \qquad (30)$$

The m and n values assumed as fresh nonse and public key certificates for I and R posessing each other's for verifying the signatures.

Protocol P_2: Transformation T_1 applies on protocol P_1 to get this protocol:

$$I \rightarrow R: m;\ R \rightarrow I: n, SIG_R(m);\ R \rightarrow I: SIG_I(n) \qquad (31)$$

This is a way to reduce the messages complexity length from 4 to 3.

Protocol P_3: This protocol is achieved from protocol P_2 by T_2 by binding operation:

$$I \to R: m;\ R \to I: n, SIG_R(m, n);\ R \to I: SIG_I(m, n) \tag{32}$$

Protocol P_4: This is one of the standard challenge-response protocol for the alternative derivation of ISO-9798-3 protocol, obtained from refinement R_4 is applied over the protocol P_3.

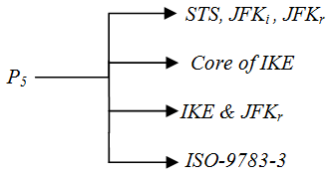
$$I \to R: m;\ R \to I: n, SIG_R(n, m, ID_I);\ R \to I: SIG_I(m, n, ID_R) \tag{33}$$

In such regard protocol P_3 is refined that included inside of the peer's identity signature, from man-in-middle attack, in case of wrong identities verification. Thus it provides the mutual authentication.

Protocol P_5: Component C_1 composes with protocol P_3, here C_1 is Diffie-Hellman component for getting this protocol. ECC or RSA component also works according to the needs and is also applicable provided all remaining things are same.

$$I \to R: g^i;\ R \to I: g^r, SIG_R(g^r, g^i);\ R \to I: SIG_I(g^i, g^r) \tag{34}$$

If responder R is honest, initiator I completes its session with R, then a secret key g^{ir} shares with them. Here man-in-the-middle attack is still possible. But, to overcome this situation four alternative paths for the same are:



Protocol P_6: The protocol is obtained from protocol P_5 by applying the refinement R_1. This is also known as secure-transmission-system (STS) protocol, it keeps all the properties of P_5 and in addition it doesn't provide any identity protection from passive attackers and man-in-middle attacks.

$$I \to R: g^i;\ R \to I: g^r, E_K\left(SIG_R(g^r, g^i)\right);\ R \to I: E_K\left(SIG_I(g^i, g^r)\right) \tag{35}$$

However, possible man-in-middle attack is still proved by Lowe here but he was not able to say anything for mutual authentication breaks remain the same or not.

Protocol P_7: On protocol P_6 refinement R_5 is applied for this protocol:

$$I \to R: g^i, n_i;\ R \to I: g^r, n_r, E_K\left(SIG_R(g^r, n_r, g^i, n_i)\right);\ I \to R: E_K\left(SIG_I(g^i, n_i, g^r, n_r)\right) \tag{36}$$

The exponentials reuse across multiple sessions is computationally more efficient in this protocol is a motivation issue that enables it for the forward secrecy and it doesn't compromise with its secrecy in the long run.

Protocol P_8: It is obtained by using refinements R_6 to protocol P_7, such as

$$I \to R: g^i, n_i;\ R \to I: g^r, n_r, E_K\left(SIG_R\left(g^i, n_i, g^r, n_r\right), ID_R\right); I \to R: E_K\left(SIG_R\left(g^r, n_r, g^i, n_i\right), ID_I\right) \quad (37)$$

After the application of this refinement, the protocol assumption is possessed by a public key certificate that discharges it from exchanging certificates alongside the signature identifiers, and by the other means that no new properties are introduced.

Protocol P_9: This protocol is attained from the cookie transformation T_3 on protocol P_8:

$$\begin{cases} I \to R: g^i, n_i; R \to I: g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right); \\ I \to R: g^i, n_i, g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right), E_K\left(SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right); \\ R \to I: E_K\left(SIG_R\left(g^r, n_r, g^i, n_i\right), ID_R\right) \end{cases}$$

(38)

In addition to protocol properties of P_8, this ensures that additional property is resistant to the blind Denial-of-Service (DoS) attacks.

At this juncture, the derived protocol provides the DoS protection, mutual authentication, key secrecy, computational efficiency and identity protection from initiator & responder, respectively.

Further, the Just Fast Key (JFK) for initiator (I) and responder (R) is obtained from protocol P_9, with the only difference that they offer only identity protection.

Protocol P_{10}: The JFK_R is obtained by applying refinement R_7 to protocol P_9. Instead of that, the protocol has added two more refinements.

$$\begin{cases} I \to R: g^i, n_i; R \to I: g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right); \\ I \to R: g^i, n_i, g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right), \\ E_K\left(SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right), HMAC_K\left(I, SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right); \\ R \to I: E_K\left(SIG_R\left(g^r, n_r, g^i, n_i\right), ID_R\right), HMAC_K\left(R, E_K\left(SIG_I\left(g^i, n_i, g^r, n_r\right), ID_R\right)\right) \end{cases} \quad (39)$$

During computation the keys K and K' require knowledge of g^{ir} that guarantees it to initiate from the Man-in-the-middle attack and it can't be computed by the hashed encrypted signature.

Protocol P_{11}: The JFK_I obtained by applying transformation T_1 to protocol P_9. Instead of same, this protocol has added modifications.

$$\begin{cases} I \to R : g^i, n_i; R \to I : g^r, n_r, ID_R, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right); \\ I \to R : g^i, n_i, g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right), \\ E_K\left(SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right), HMAC_K\left(I, SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right); \\ R \to I : E_K\left(SIG_R\left(g^r, n_r, g^i, n_i\right), ID_R\right) \end{cases} \quad (40)$$

Here, the ID_R message component is shifted, to reason for applying transformation to include the peer's identity inside the signature. In this regards, I's signature possesses the R's identity before it sends the message in the protocol. This also retains all the properties contained in P_9 is different except for identity protection. But, the major drawback is the responder's identity protection.

Protocol P_{12}: The protocol P_{12} is obtained from the protocol P_{11} by applying the refinement R_4. This is equivalent to JFK_i except for one additional signature that is added by using the one more transformation in message and for other end the core security property is ignored.

$$\begin{cases} I \to R : g^i, n_i; R \to I : g^r, n_r, ID_R, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right); \\ I \to R : g^i, n_i, g^r, n_r, HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right), \left(SIG_I\left(g^i, n_i, g^r, n_r\right), ID_I\right), \\ E_K HMAC_K\left(g^i, n_i, g^r, n_r\right), E_K\left(SIG_I, \left(g^i, n_i, g^r, n_r\right), ID_I\right)\left(I, SIG_I, ID_I\right); \\ R \to I : E_K\left(SIG_R\left(g^r, n_r, g^i, n_i\right), ID_I\right) \end{cases} \quad (41)$$

The peer's identities refinement adds are of ID_I and ID_R inside the signatures, respectively. This prevents the attacks, and retains all the properties of protocol P_{11}.

Protocol P_{13}: The Internet Key Exchange (IKE) is one of the protocol that is obtained by applying refinement R_2 to protocol P_5. This is described as the core for IKE as

$$I \to R: g^i;\ R \to I: g^r, SIG_R\left(HMAC_K\left(g^r, g^i, ID_R\right)\right); I \to R: SIG_I\left(HMAC_K\left(g^i, g^r, ID_I\right)\right) \quad (42)$$

Each principal used in the exponentials signs a keyed hash and their own identities. The adversary can't attack on the used hashed key from the secret g^{ir} which is only known to I and R. So, this provides for both the mutual authentication and a shared secret between them.

Protocol P_{14}: This protocol derivation is achieved by using the refinement R_5 when applied to protocol P_{13}. This sensibly parallels the steps for JFK_r and JFK_i where exponential nonces are exchanged.

$$\begin{cases} I \to R : g^i, n_i; R \to I : g^r, n_r, SIG_R\left(HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right)\right); \\ I \to SIG_I\left(HMAC_{HK_R}\left(g^r, n_r, g^i, n_i\right), ID_I\right), \end{cases} \quad (43)$$

The purpose is to allow and reuse the exponential in a more efficient protocol for multiple sessions. Although, it contains one of the tradeoff during the processing, in the loss of perfect forward secrecy.

Protocol P_{15}: It is one of alternative paths for protocol P_5 that consists of the core for JFK_r and $JFK-SIGMA$. This protocol is obtained by using the refinement R_3 to protocol P_5.

$$I \to R: g^i; R \to I: g^r, SIG_R(g^r, g^i), HMAC_K(g^r, g^i, ID_R);$$
$$I \to R: SIG_I(g^i, g^r), HMAC_K(g^i, g^r, ID_I) \quad (44)$$

This is very similar to protocol like P_{13}, and it also possesses the same properties of shared secret and mutual authentication. One of differences observed is in signing the keyed hash and the principals to send the hash separately. So, for adversary can't launch the MAN-IN-MIDDLE ATTACK attack because the computation of the hash requires key only known to I and R.

Protocol P_{16}: This protocol is obtained from protocol P_5 by using refinement R4, and it is also known as ISO-9783-3 protocol:

$$I \to R: g^i; R \to I: g^r, SIG_R(g^r, g^i, ID_I); I \to R: SIG_I(g^i, g^r, ID_R) \quad (45)$$

This protocol set-up is a secret mutual authentication scheme and refers to man-in-middle attack which is not possible, because of its intended identity recipient's signature, attacker doesn't forward identity either to I or to R.

Now, we are applying the recent protocol of ECC-Based Password Authenticated Key Exchange Protocol on Multilayer Consensus as a key part, the next section elaborates the same and is also one of the motivating issues.

5.4 RELATED WORK AND BACKGROUND

ECC-Based Password Authenticated Key Exchange Protocol on Multilayer Consensus is a key of our work and its related idea has been presented in [100]. Password authenticated key exchange protocol (PAKE) is an elementary protocol derivation based on two-steps and it is also known as Simple Authenticated Key Exchange Protocol (SAKA), presented in [101], shown in Figure 5.3. Further, X. Ding et al. presented PAKE on three step to resist password compromise impersonation, compromise on ephemeral key, forward secrecy, and dictionary attack. The IEEE standard 1063.2 was released in 2009; this specifies secrets on shorter key as a strong security transactions and to show a proficiently utilizing password [102]. The basic idea is presented here,

a group generaror G is available, where each party randomly selects its secret keys (as a number) and multiplies the same with G, which shares using the ECC as depicted in $X.1035$ standard that is resistant against to guess the password attack.

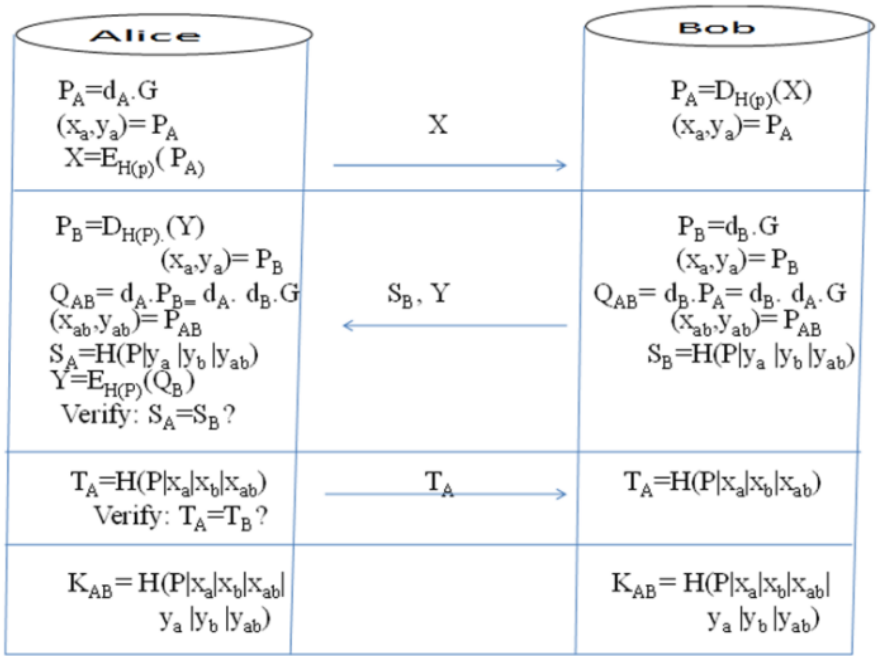


Figure 5.3: Working of ECC-based PAKE (EPAK) protocol in between Alice & Bob

Step I: Assume Alice as an initiator chooses a secret random key d_A, multiplies with group generator G that is public key P_A and represented the same in Elliptic point (x_a, y_a). It further computed hash $H_{(p)}$ with it encrypts P_A as X and is sent it to Bob (20):

$$P_A = d_A.G;\ (x_a, y_a) = P_A;\ X = E_{H(P)}(P) \tag{46}$$

A packet received X, Bob decrypted the same and represented in elliptic point (x_a, y_a) (47):

$$P_A = D_{H(p)}(X);\ (x_a, y_a) = P_A \tag{47}$$

Step II: At other end Bob picks up a secret random key d_B as private key and obtained public key P_B it is multiplied it to group generator G, also appropriates it to Elliptic point in (48):

$$P_B = d_B.G;\ (x_a, y_a) = P_B \tag{48}$$

Again, it is multiplied private key with Alice public key to obtained a shared key Q_{AB} and finds its appropriate EC points $(x_{ab}, y_{ab}) = P_{AB}$ then computes S_B having $Q_A, Q_B\ and\ Q_{AB}$ and finally uses $H_{(P)}$ to encrypt:

$$Q_{AB} = d_B.P_A = d_B.d_A.G;\ (x_{ab}, y_{ab}) = P_{AB};\ S_B = H(P \mid y_a|y_b|y_{ab});\ Y = E_{H(P)}(P_B) \tag{49}$$

To decrypt- Y, Alice used $H_{(P)}$ and obtained Q_B and also the converted elliptic point (x_a, y_a) aligned to Q_B. Again, the Alice private key multiplies with public key sent by Bob Q_B and shares a common shared key Q_{AB} followed by points (x_{ab}, y_{ab}). Finally computed S_A having for verification of $Q_A, Q_B \, and \, Q_{AB}$. Alice is now assured the verification on received the requited values as (50):

$$P_B = D_{H(P)}(Y); Q_{AB} = d_A.P_B = d_A.d_B.G; S_A = H(P|y_a|y_b|y_{ab}) \quad (50)$$

Step III: Bob needed to assure Alice that she has required values as well. So, she needs to performs T_A out of Q_A, Q_B and Q_{AB} and send it to Bob as (51):

$$T_A = (H(P|x_a|x_b|x_{ab}) \quad (51)$$

On the other side Bob calculates T_B and compares it with T_A. If the verification holds good Bob also assures Alice that she also has the required values as well (52):

$$T_B = H(P|x_a|x_b|x_{ab}) \quad (52)$$

Step IV: Therefore, on the generated parameters both parties are verified with each other and calculated the secret shared key as (53):

$$K_{AB} = H(P|x_a|x_b|x_{ab}|y_a|y_b|y_{ab}) \quad (53)$$

Further, here Multilayer Consensus Password Authenticated Key Protocol Exchange (ECPAKE) protocol for key exchange is considered. A key agreement for mutual authentication among (an initiator) appliance network A_N, Home Area Network H_c, Building Area Network B_c, Neighbor Area Network N_c and Central Controller C_c is considered, where all controllers are resulted in individual operations on them and are reported correctly working for all. In this we considered the same approach which is taken the ECC advantage for key generation, as shown in Figure 5.4. If required, it can be extended to a larger layer of security; it is also adopted by the standard $X.1035$.

For PAKE using ECC approach, first iteration in between A_N and H_c. Further, the same philosophy is applied for second, third and fourth consequent layers. These have also been available for ECC based password authenticated key exchange protocol for multilayer consensus. Since the MCEPAK proposed protocol [100] is established on ECC, and X.1035 that contains similar benefits like the Diffie-Hellman procedure. In the proposed work, the security and different attacks have been analyzed and modeled on the same, where an adversary (internal or external) is capable of re-scheduling, re-playing, re-ordering, re-routing, deleting and recording

of the messages is considered. We have done the formal verification of the proposed protocol underneath under the same adversary conditions.

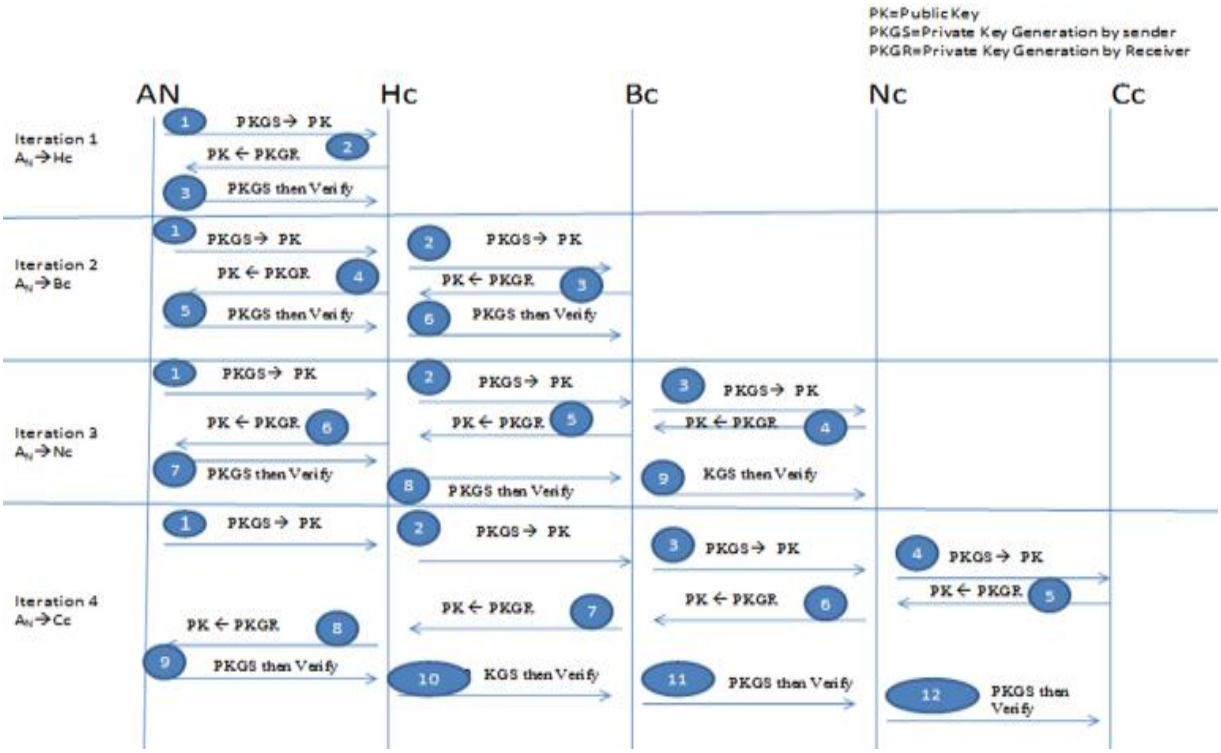


Figure 5.4: Multilayer Consensus Key-Generation Approach

5.5 FORMAL VALIDATION USING SPAN AND AVISPA TOOL

AVISPA [103] is one of the automatic verification and validation tool that used in the cryptography. It is widely used for Internet security applications and its protocols verification. It offers a significant expressive formal language for specifying protocols with their safety measures that is modularized into different four back-ends under the perimeter, the structure is shown in figure 5.5. Its accomplishment is based on the automatic analysis techniques. The High Level Protocol Specification Language (HLPSL) is described to formally validate the security protocols and it specifies the intended security properties. The HLPSL specification is first translated into Intermediate Format (IF) through translator HLPSL2IF. The IF is a lower-level language that is used for directly interpretation for back-ends tool. The IF objective has formulated for developers with the implication to use it for their input language analysis. This happens automatically and is transparent to the user [104].

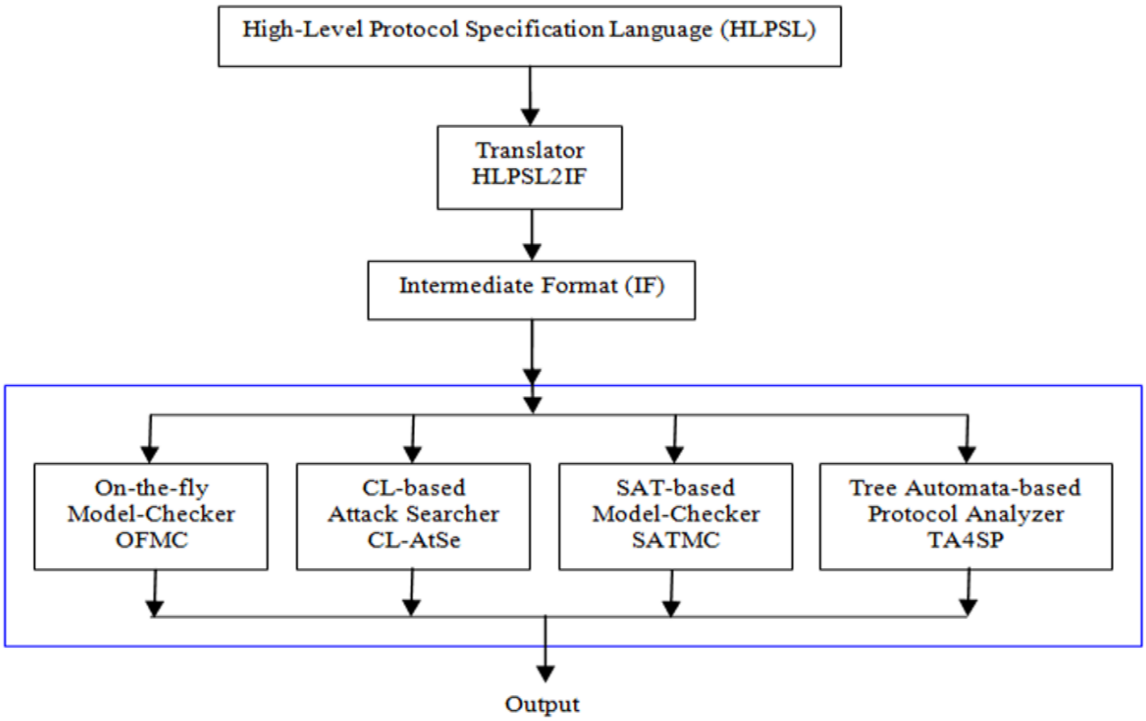


Figure 5.5: AVISPA Structure

Now, the IF specification is analyzed at the back-ends for the satisfied or violated security goals. The AVISPA Tool comprises of four back-ends such as: On-the-fly Model Checker (OFMC) [105], Constraint Logic-based Attack Searcher (CL-AtSe) [106], SAT-based Model Checker (SATMC) [107]-[108], and Tree-Automata Based Protocol Analyzer (TA4SP) [109]. The definition of OFMC says it is a useful debugging tool for protocol specification that allows agents to execute all the required steps for honest run of the protocol and is specific for manual check if needed. CL-ATSE is set of constraints, used to find attacks on protocols where translation and checking are fully automatic that are internally performed by the same i.e. no external tool is used. Its back-end is slightly different format of trace in some aspects of attack other than what OFMC does, it writes an interpretation in the intermediate format (IF) as tests. SATMC's is used to check the executability that includes functionality to confirm the on HLPSL specification. SATMC is strict in particularly for the proper specification; this feature is useful in finding errors. The TA4SP proves secrecy properties with an unbounded number of sessions. From the practical point of view, this works completely automatic and is supported by two (2) tools such as Timbuk and its extensional part. The analysis of four back-ends are harmonized with each other in a sense for some common back-ends procedure, but these are not equivalent

that should return with different results. The proposed MCEPAK protocol running on the tool, as shown in Table 5.1, at back ends of OFMC and CL-AtSe, with safety measures.

An impressive SPAN tool comes with simple editing protocol specifications of web graphical interfaces of AVISPA, and in addition to this it contains honest agents for protocol simulation, intruder simulation for honest agents and an attack simulation. Attack simulation in this is like the same layout in intruder simulation, but attacks are automatically built by using OFMC/CL-AtSe facilities.

Table 5.1: OFMC and Cl-AtSe Back end results on AVISPA

A@ubuntu:~/avispa-1.1$avispa BasicMainHlPsl.hlpsl –ofmc	**A@ubuntu:~/avispa-1.1$ avispa BasicMainHlPsl.hlpsl --cl-atse**
% OFMC % Version of 2006/02/13 SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/A/avispa-1.1/testsuite/results/BasicMainHlPsl.if GOAL as_specified BACKEND OFMC COMMENTS STATISTICS parseTime: 0.00s searchTime: 0.05s visitedNodes: 6 nodes depth: 2 plies	SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL /home/A/avispa-1.1/testsuite/results/BasicMainHlPsl.if GOAL As Specified BACKEND CL-AtSe STATISTICS Analysed : 1 states Reachable : 0 states Translation: 0.02 seconds Computation: 0.00 seconds

The security protocol analysis is the major idea possible through the two specifications such as High Level Protocol Specification Language (HLPSL) and CAS+. HLPSL is a language used for specifying the cryptographic protocols for AVISPA toolset and CAS+ is a light evolution of CASRUL language. The Figure 5.6, depicts the operation on ECC through CAS language and shows the principles of sender pattern as the tool dictates it like the same.

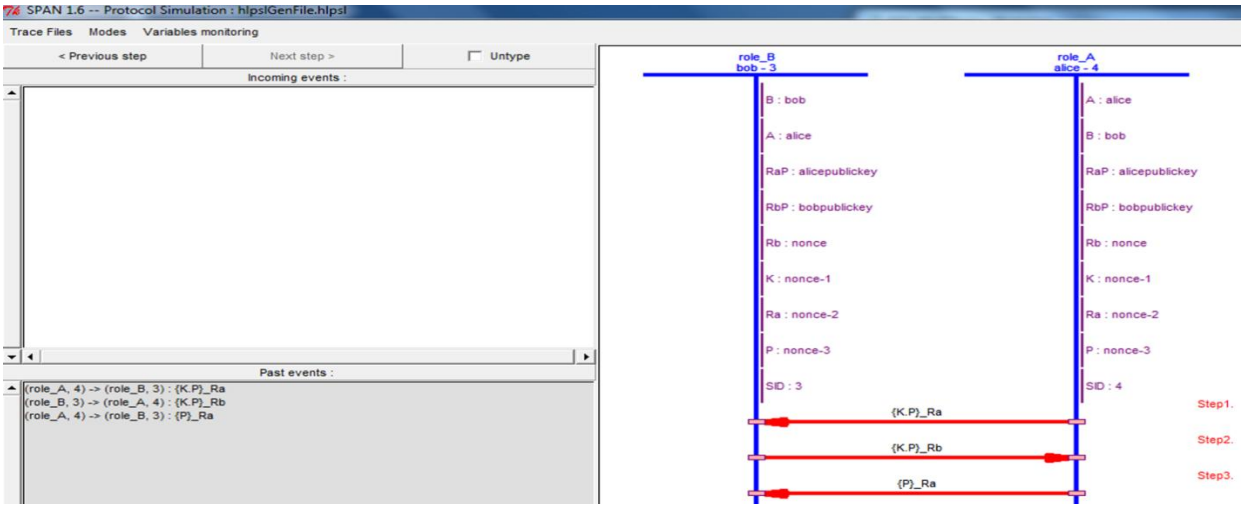


Figure 5.6: ECC Protocol Verification in view of Sender Pattern principal

This specification translates a CAS+ language from Alice-to-Bob for simple and fast specification of security protocols; interactively building a Message Sequence Chart (MSC) [100]-[111] of protocol execution; MSC build attacks automatically on either of HLPSL and CAS+ specifications; and for intruder interactively builds a specific possible attacks.

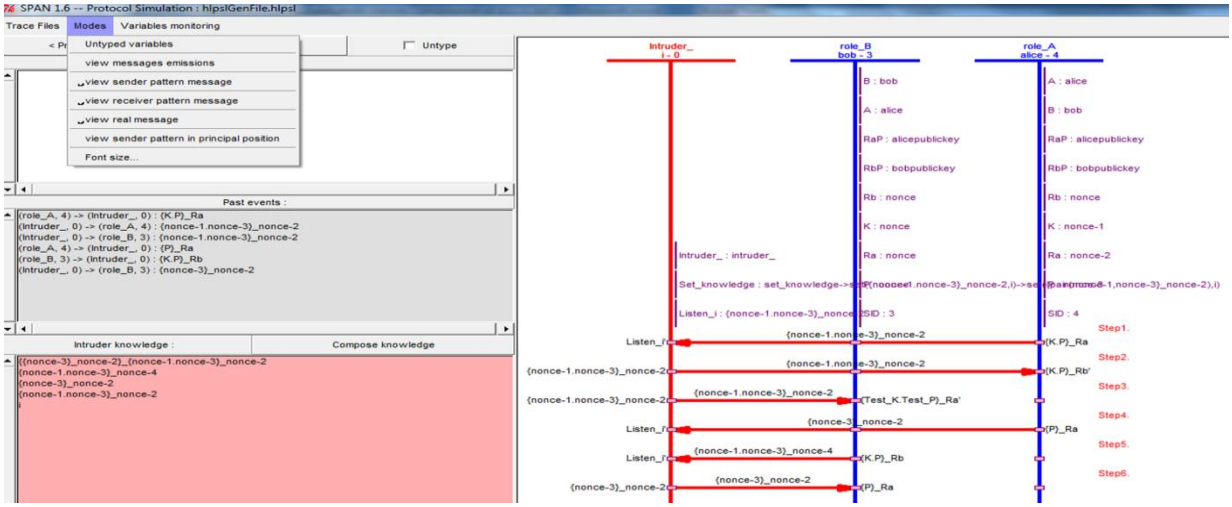


Figure 5.7: Intruder Simulation on ECC in between sender and receiver

Figure 5.7 is shown simulation approach on sender-receiver with an inclusion to intruder pattern generation and is observed as real messages transmission.

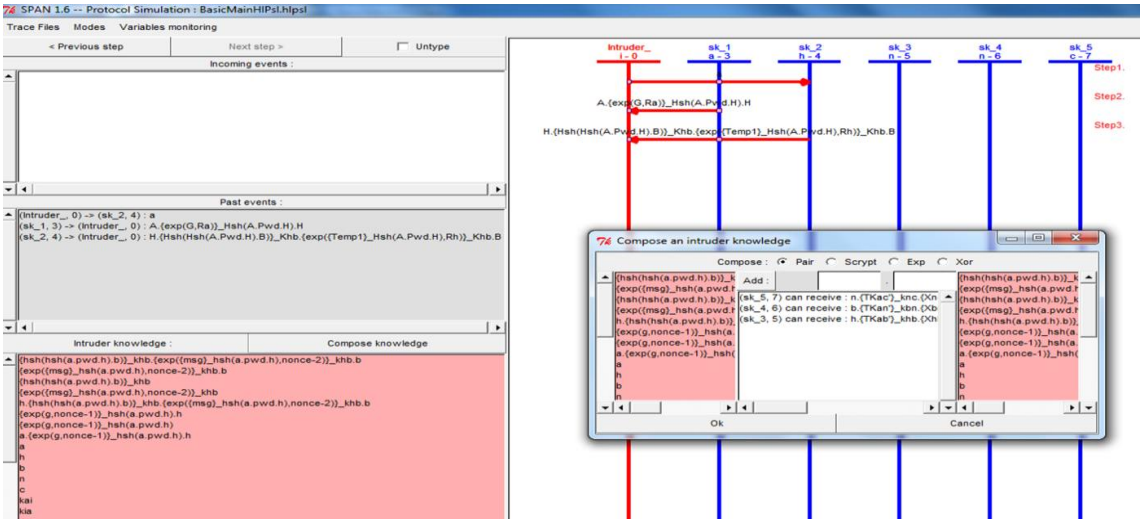


Figure 5.8: Intruder Simulation on Multilayer Consensus protocol

In figure 5.8, we have shown the intruder formal verification for multilayer consensus. The MCEPAKE proposed scheme is an enhancement for multilayer security among the layers of networks. Its percent improvement encryption and decryption time between layers are presented below in Table 5.2.

Table 5.2: Execution Time: Encryption and Decryption

$A_N \leftrightarrow H_C$	$A_N \leftrightarrow B_C$	$A_N \leftrightarrow N_C$	$A_N \leftrightarrow C_C$
$2\times t_0$	$4\times t_0$	$6\times t_0$	$8\times t_0$
$2\times t_0$	$2\times t_0$	$2\times t_0$	$2\times t_0$
0%	50%	66.69%	75%

Using ECC algorithm for encryption and decryption of desired message m with the shared secret key K is used in MCEPAKE protocol to form the ciphertext $C_m = \{KG, m + K.P_B\}$, where P_B is the responder public key used by the initiator. Now, to decrypt ciphertext C_m to find plain texts message as $m = \{m + K.P_B - n_B(K.G)\}$, where n_B is a responder private key [112], is used during the whole procedure.

In the next section, our proposed Signcryption technique is presented in relation to the basics of this technique. This is one of the efficient and modernized techniques that serves two purposes such as digital signature and encryption of transmitted message with reduced computation and communication costs.

5.6 SIGNCRYPTION

In 1997 Zheng [113] first proposed the Signcryption primitive of cryptography. It logically combines digital signature and encryption scheme in a single step in less computational and communication cost. Using the Signcryption, he proposed 58% of less computational cost and 70% less communication cost only when in general it is compared with the individually signature–then-encryption schemes. The parameters used in the schemes contain the respective sizes that decide its cost such as $|p| = 512$ bits, $|q| = 144$ bits and $|hash(.)| = |KH(.)| \cong |q|/2$. Here we have presented in a Table 5.3 that shows the above enrichments in relation to basic signature-then-encryption on Schnoor Signature plus ElGamal Encryption versus Zheng signcryption. Except the exponential (EXP) function, the other functions used in the explanation are equalized with each other so its cost is considered to be negligible. The computational cost represents a reduction in $\{(5.17 - 2.17)/(5.17)\} = 58\%$. Whereas this table concludes $(\{(|\text{hash}(.)| + |\text{p}| + |\text{q}|) - (|\text{KH}(.)| + |\text{p}|)/(|\text{hash}(.)| + |\text{p}| + |\text{q}|)\} = 70\%)$ saving in communicational cost.

Table 5.3: Cost of Signature-then-Encryption versus cost of Signcryption

Schemes	**Computational Cost**	**Communicational Cost**
Signature-then-encryption based on "Schnorr Signature + ElGamal Encryption"	EXP=3, MUL=1,DIV=1,HASH=1,ENC=1 { EXP=2.17, MUL=0,DIV=1,HASH=2,ENC=1} Total Modular Reduction=5.17	$\|hash(.)\| + \|p\| + \|q\|$
Signcryption	EXP=1, MUL=1,DIV=1,HASH=1,ENC=1 { EXP=1.17, MUL=0,DIV=1,HASH=2,ENC=1} Total Modular Reduction=2.17	$\|KH(.)\| + \|p\|$

This is a huge saving for applications in computation and communication cost in the form of secure & authenticated message delivery. There are other applications also that are brought to notice such as authenticated electronic secure transactions, non-repudiated key transportation, video conferencing inclusive of through secure and authenticated multicast services, unforgeable messages fast & compact services.

For the last so many years, many variations of this scheme have been proposed which are having their own problems and limitations, that are offering optimized computational costs and different levels of security. Baek, in 2002, gave the formal proofs of Signcryption in [114]. The real life application of Signcryption is based on old adage "*killing two birds with one stone*". Confidentiality is achieved through encryption, whereas authentication is provided by the integrity of this scheme. Authentications on private key and digital signatures on public key are authentication scheme and are playing an important role.

In general, the objective of Signcryption states that the cost of Signature and Encryption achieved through approach is always be less than the individual cost of Signature and individual cost of Encryption [113]. Further, these are interpreted in a number of ways:

• A combination of digital signatures and encryption scheme, signcryption should be more efficient (computationally).

• A naive combination of digital signatures and ciphertext encryption, signcryption should produce shorter cipher text.

• A naive combination of digital signatures and public-key encryption, signcryption should be endowed with better safety measures and/or bigger functionality when compared.

The signcryption scheme works in five phases such as: Setup phase, Sender Key Generation phase, Responder Key Generation, Signcrypt phase, and in Unsigncrypt phase.

Phase 1: Setup Phase

The setup factor is based on the security and common key generation parameters. The overall parameters factors are made public for all as the summary contains like: p is a large prime; q is a prime factor of $p-1$; g is an integer with order q modulo p in $[1, \dots, p-1]$; KH is a key hashed one way function of hash(k, m); and (E, D) are used for encryption E and decryption D respectively.

Phase 2: Sender Key Generated phase

Alice has the pair of keys $(\mathrm{X_a}, \mathrm{Y_a})$, where X_a Alice's private key randomly chosen from $[1, \dots, q-1]$; Y_a is a generated public key for Alice to modulo prime p; Alice is now ready to send a message to Bob

Phase 3: Responder Key Generation phase

Bob keeps a pair of keys (X_b, Y_b), as private key X_b randomly selected from $[1, .., q-1]$ and his public key Y_b is generated on the prime modulo p. Bob is now ready to send a message to Alice

Phase 4: Signcrypt phase

The initiator and responder accomplish the following operations to message signcrypt:

The key k splits in k_1 and k_2 of equal length parts; Calculate $= hash(k_2, m)$; Calculate $s = x/(r + X_a)$ mod q; Calculate $c = E_{k_1}(m)$ is message m encryption with the key k_1; then Alice send it to Bob as (r, s, c)

Phase 5: Unsigncrypt phase

Finally, to unsigncrypt the signcrypted message, responder accomplishes the following operations:

Calculates $k\ using\ r, s, g, p, Y_a and\ X_b$; $k = hash(Y_a * g^r)^{s*X_b}$mod p; now again Split k in k_1 and k_2 for the verification of original message in the form of appropriate lengths; the message m evaluates it by performing decryption $m = Dk_1(c)$; A valid message m accepted only if $KHk_2(m) = r$ is satisfied.

Table 5.4: Comparison of different algorithm schemes based operations

Schemes	Participant	ECPM	ECPA	DIV	MUL	ADD	HASH
Zheng	Sender	1	-	1	1	1	2
	Receiver	2	1	-	2	-	2
Hwang	Sender	2	-	-	1	1	1
	Receiver	3	1	1	-	-	1
Zhou	Sender	2	2	1	2	1	3
	Receiver	4	4	-	1	1	3
Basu	Sender	2	-	-	2	1	1
	Receiver	3	1	1	1	1	1
Proposed Scheme	Sender	1	1	2	-	1	1
	Receiver	1	-	2	2	-	1

This approach contains the many features as: - it requires much smaller overhead than the conventional sign-then-encrypt schemes, security against unforgeabilty, unsigncryptabilty to verify message. The Table 5.4 is our proposed scheme which shows the improvement over Basu et al. [115] and its related proposed schemes on point multiplication on elliptic curve (ECPM), addition ADD, and Multiplication MUL.

The correctness definition of the scheme is secure, if it satisfies the following conditions:

(iii)Unforgeabilty: For an adaptive attacker, it is computationally infeasible for the dishonest Bob and then allows querying for Alice signcryption to masquerade in creating authentic text messages.

(iv)Non-repudiation: For a third party, it is computationally feasible to settle the dispute between the two events.

(v) Confidentiality: For an attacker it is infeasible to gain an access from signcrypted text. The other party involved may be anyone other than Alice/Bob.

Further, the scheme is generalized into the forms of requirements specifications. It is not only necessary for all messages to require integrity and confidentially, whereas some messages require sign only, while others need to be encrypted. Later on the two cases may provide one of the specific parties to them, despite the fact that conventional signcryption requires both of them. As a result the applications must implement the three individual primitives that include signature, encryption, and signcryption. This scheme has been generalized so that it provides the dual functions with more practicability and flexibility, when simultaneously it requires authenticity and confidentiality. Also, it is endowed with solitary signature or encryption function when authenticity/confidentiality is required without any additional computation and amendments [116].

In the recently scenario, there are many applications that are in light due to their various abilities such as- decreased computation cost, reduced bandwidth, easy applicability to tiny digital phone, handshake on transport layer security, and the connect internet ability. Unforgeable key establishment is the second major application over ATM networks.

5.7 SUMMARY

This chapter contains a secure composition approach that adds and/or makes a way for secure computing techniques. These approaches are widely contributing significantly to the cryptographic applications. Instead of the same our focus is on relative advantages over the signcrypted multilayer consensus based approaches for secure composition. It has been showing in information security, the proposed approach makes scientifically strong security mechanisms in applied cryptography. Our proposed approach has considered the protocol derivational system

and protocol compositional logic approach. The abstract idea presented here is to derive the use of basic components in the formation of Diffie-Hellman, and applicability for secure composition that can be also applied for ECC with its reduced relative cost. In addition to addressing, security concerns without any compromise. Thereafter, by using signcryption primitive that is applied on multilayer consensus ECC based, password-authenticated key exchange protocol approach that significantly reduced both computational and communicational cost. Whereas, new paradigm of signcryption is applied for cost effectiveness, high performance and is favorable for short-memory devices applications and there are many more are the possible advantages of the proposed approaches. Moreover the protocol is formally validated on AVISPA and SPAN tools.

CHAPTER 6

MOTIVATION TOWARDS SIGNCRYPTION RE-CRYPTOGRAPHY: SECURE AND EFFICIENT APPROACH TOWARDS TRUST PROBLEM

Cryptography is a discipline of computer science that directs the requirement specifications for satisfactory protection mechanism with efficient and smooth functioning in the real world. Signcryption is one of the most promising primitives of cryptography that was proposed by Zheng (1997), that rationally combines digital signature and encryption in a single step, lowers the computational and communications cost when compared with the cost of separate signature and encryption schemes. The concept of proxy re-cryptography was first proposed by Blaze at Eurocrypt (1998), and further be dignified by Ateniese and Hohenberger (2005). They defined their model by using two approaches like proxy re-signature and proxy re-encryption. In this chapter, we have directed towards a probably secure and efficient approach regarding the trust problem for third party, who is not directly involved 'called proxy', can be solved by using signcryption re-cryptographic approach. In modern era of cryptography, this is one of the new diverse trends and motivating issues. To solve the crypto logical problems such as trust and ciphertext access control problems, where research focuses on situations under a cryptographic key management by a semi-trusted proxy with special information where data encrypted under one cryptographic key need to be re-encrypted. Further, the proposed work is simulated on AVISPA/SPAN, using the automated formal verification tool.

6.1 INTRODUCTION

Diffie-and-Hellman (1976) [12] first proposed the idea of public key cryptographic protocol wherein the public key infrastructure (PKI) is developed for generating and maintaining the public-keys using the corresponding certificates. However, the PKI suffers from heavy management of public keys and certificates. An alternative solution is Shamir's identity-based crypto systems (IBC). However, shortcoming of IBC is the key escrow problem [117]. The key escrow is a key exchange process in cryptography where a key is held or escrow, by a third party. The key gets compromised or lost by its original user(s) may be used to decrypt encrypted

matter, and allows restoration of the primary matter to its unencrypted state. Somewhere the third party involved is risky in escrow systems. Key escrow enables us to provide a backup source for cryptographic keys. The modern cryptography is an interdisciplinary approach of computer science focusing on the trust problem which is solved by using the proxy re-cryptographic primitive. The concept of proxy re-cryptography was first proposed by Blaze, Bleumer, and Strauss (1998). This approach was formalized by Ateniese and Hohenberger (2005). It consists of two methods as proxy re-encryption and proxy re-signature. The proxy re-encryption goal is to applied encryption again on generated cipher texts, without believing on honest parties and the proxy re-signature goal is applied to sign to transform into different signature on the same message trustworthy without relying on involved parties. In (2006) they proposed enhanced few proxy re-signature schemes and is discussed the potential applications related to same. They predicted that proxy re-signature and proxy re-encryption is played a crucial role. After that many researchers thoroughly are sparked more light in this area. That's how some excellent schemes are proposed; where IEEE P1363.3 standardization group is established on proxy re-encryption, which is giving power to proxy re-cryptography approach [118]. A semi-trusted is an entity to convert cipher texts addressed to those which can be decrypted by using some special information.

For primitives of the proxy re-cryptography such as, signcryption proxy re-signature (SCPRS), signcryption proxy re- encryption (SCPRE), and security models are motivated by the same [139], [98].

In this chapter, a more optimized notion of signcryption with proxy re-cryptographic definition and its formal verification have been resented, and its efficiency motivation is specified. Finally, it provides directions for further research in this area in the concluding section.

6.1.1 Trust Problem

To solve the trustworthy problem within the domain of fully trusted authority to build the absolute trust relationship is a challenging issue. The public-key infrastructure certificate authority releases a public-key certificate to bind with the identity [119]. However, how to build offshore trust relationships between honest, trusted authority domains is a difficult task is a

practical problem. The goal is to solve the problem using proxy who allows in transferring certificates, and the proxy can't generate new certificates. Sometimes it is desired that certificates of authority only transfer in a single direction known as unidirectional transformation. Bidirectional transformation is allowed to authorize in both directions. On the other hand, a trusted domain a requirement is further be extended the process that continues from one of proxy to many more proxies is known as multiuse. Trust problem is the significant asset in cryptographic primitive to solve such problems.

6.1.2 Trusted Server Problem

This problem is emerged with the cloud computing that reduces the cost of software and hardware resources. Almost all cloud storage servers are exerting and are responsible for sensitive information, like electronic storage user's data, and access the cloud server over the data access. In usual the cloud access control server is considered to be fully trusted, but particular requirement doesn't met due two practical reasons. First one is that the provider(s) of control service can't be assumed to be fully trustworthy, the other being it could be corrupted in situations.

A possible solution is to store the encrypted plaintext at the server of cloud storage. The trusted server problem can be solved easily through this. The encrypted cipher texts need to be shared with others and no right to perform decryption by the access control server. Under this condition, the following solution can be conceived: - as the control server access right is to transform the cipher texts therefore only delegated users decrypts cipher texts, but control server access can't decrypt cipher texts. If the access control server under Encryptor authorization can stored information on the cloud storage server in a new form then only designated receivers can decrypt, this is one of the specific case of proxy re-encryption [120]-[121].

6.1.3 Ciphertext Access Control Problem

The data processed under the specific circumstances is somewhere are intended to be stored for the set of users as a security concerns. The most motivating solution is owner data lays down in plaintext at the storage server, and rights for each user's access are designed. The each user

specified by the access control lists services and linked to the access the message through control server. Therefore, security and trust issues are important issues in practice.

Data storage is a trivial method that stored into ciphertext. However, the current encryption system can't allow being efficient shared among a user group on cipher text. It is becoming essential to develop a flexible and efficient method that directly share data based on encrypted plaintexts and it also includes the access policy control services. Bethencourt proposed a ciphertext-policy attribute-based encryption (CP-ABE) [122] approach that is appropriately initiated in solving the ciphertext access control problem [123].

6.2 SIGNCRYPTION

Signcryption is one of the cryptographic primitives, proposed by Zheng (1997), which logically combines digital signature and encryption in a single step on low communication and computational cost [113], [114]. This brings savings in communication and computation. There are various and huge applications of signcryption available that are being widely used for electronic commerce in sheltered and substantiated transactions, invulnerable and validated message delivery, safe, fast and non-repudiable transportation services.

After that many schemes are proposed with their own problems and limitations while they are offering different levels of computational costs and security services. Through the algorithm confidentiality and integrity is achieved [124]. The digital signature (DS) is a fully demonstrates with the mathematical explanation for the authenticity of its message digests. This DS scheme generally consists of the three steps:

The key generation that selects a personal key at random from the possible set of particular keys, that output's private key and its corresponding public value.

i. On behalf of the message and private key it produces the signature and

ii. After this the verification phrase occurs on the message, public keys and signature.

A signcryption scheme that includes DS as well as encryption consists of typically five phases, such as: Setup, Key Generation by Sender, Key Generation by Responder, Signcryption, and Unsigncrypt. Signcryption is extensively accepted in many application areas in ability to

connection to Internet, PDAs digital phones, session key establishment on ATM networks, etc. [27].

6.3 PROXY RE-CRYPTOGRAPHY

This is used to establish the trust relationship in an unsecured environment instead of that there are many applications such as digital-right management (DRM) that prevents the illegal redistribution of digital content. In 2006, Taban [125] proposed an entirely new interoperability architecture or modern module in the existing DRM called the domain interoperability manager (DIM). It applies a unique signature scheme and a particular public key encryption scheme. The traditional public key encryption and signature don't support transformation, but using proxy re-cryptography this can be easily implemented. This scheme contains the two phases as: proxy re-signature and proxy re-encryption. Each phase contains its own properties and definition. A pictorial proxy re-cryptography digests approach is shown in Figure 6.1.

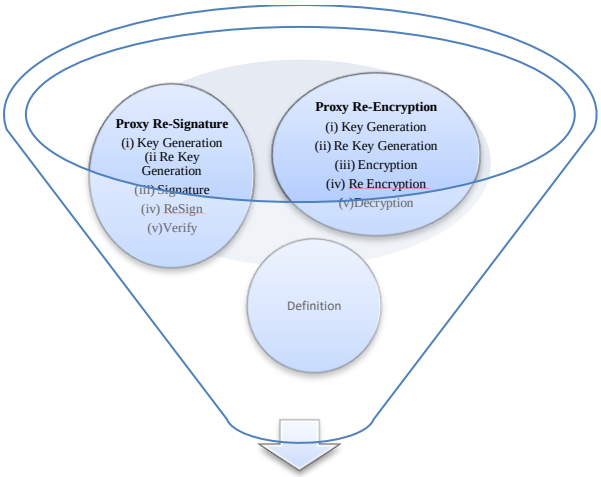


Figure 6.1: Proxy Re-Cryptography Digest

6.3.1 Proxy Re-Signature (PRS)

In this scheme, a delegate's signature transforms his/her signature using a semi-trusted proxy to a delegatee's on the same message by using some additional information. The proxy can't generate an arbitrary signature on behalf of either the delegate or the delegatee.

6.3.1.1 Properties of Proxy Re-Signature

(i) A Unidirectional or Bi-directional: The proxy is to allow for re-signature key either in uni-directional or in bidirectional transformation.

(ii) Multiuse: In this case, the proxy transformed the signature can be re-transformed again by a proxy. Even so, the signature does not transform a single use.

(iii) Private Proxy: In private proxy, the re-signature keys to be secret in scheme.

(iv) Transparent: The scheme should be see-through so that the user(s) does not know about the where proxy is existed.

(v) Key-Optimal: In this, a user is required to protect and store only a small constant amount of secrets, no matter how many signature delegations the user gives for acceptance.

(vi) Non-interactive: The parties involved are an idle and are not required during the commission process.

(vii) Non-transitive: Other than the two, signature can't be generated from anywhere in any case for the same.

(viii) Temporary: The right of re-signing is interim. It is necessary to specify the involment of right to access or right to expire at particular moment.

(ix) Collusion resistance: Via proxy, the delegator consigns the signing rights to the entrusted delegate, instead of keeping the rights decryption for the same public key.

6.3.1.2 Definition of Proxy Re-Signature

The proxy re-signature follows the following five steps:

(i) Key Generation: The security parameter λ is taken as input, and that returns a verification key pk and a signing key sk.

(ii) Re-Key Generation: It takes as an input delegate key pair $(\mathrm{pk_A}, \mathrm{sk_A})$, and a delegatee key $(\mathrm{pk_B}, \mathrm{sk_B})$, and returns a re-signature key $\mathrm{rk_{A\leftarrow B}}$ for the proxy. If the scheme is unidirectional, the delegates signing key are not included in the input. But in the case of bidirectional, the proxy can be easily obtained by $\mathrm{rk_{B\leftarrow A}}$ from $\mathrm{rk_{A\leftarrow B}}$. In many bidirectional schemes $\mathrm{rk_{A\leftarrow B}} = 1/\mathrm{rk_{B\leftarrow A}}$.

(iii) Signature: It takes as input a signing key sk, a positive integer l, and a message m from message space, and returns a signature σ at level l. If this scheme is for single use, then $l \in \{1,2\}$.

(iv) Re-signature: It takes as input a re-signature key $rk_{A\leftarrow B}$, and a signature σ_A, taking place message m under pk_A, on level l, and returns the signature σ_B on the same message m under pk_B, at level $l+1$ if verified $(pk_A, m, pk_B, l) = 1$, or reject otherwise. If the scheme is for single use $l = 1$.

(v) Verify: This takes as input a verification key pk, the message m from the message space, the signature σ and a positive integer l, and returns 1 if σ is a valid signature under pk at level l or otherwise.

6.4 SIGNCRYPTION WITH PROXY RE-ENCRYPTION

The proxy signcryption scheme has the general condition, which is divided into three parties such as delegate signer, proxy signer and the delegatee recipient. In this scheme, the delegate signer generates a proxy credential to the signing authority to a proxy signer. The proxy there after generates signcrypted message using a secret key and its own proxy credentials. Finally, the proxy sends the signcrypted message to an assigned recipient through a network. After receiving the signcrypted message, the recipient recovers the content from the same and also verifies its validity. If any dispute arises, the recipient is free to announce the signature of proxy for public verification.

The notion of signcryption [126] with proxy re-encryption [127] has been presented here. This scheme consists of proxy re-encryption, authenticity and confidentiality in a very efficient way. This primitive have various applications, such as:

(i) Email is the best candidate for applying signcryption. An application of signcryption of proxy re-encryption (SCPRE) is to allow and forward the message for authentication using signcrypted message to be directed to a person when the original receiver is unavailable.

(ii) Another well-known application for secure and authentic distributed storage that can be extended whenever the content stored for authentication is desirable.

The signcryption of proxy re-encryption scheme follows the following steps:

i. Setup: The algorithm accepts a security parameter I and outputs a master secret key s.

ii. Extraction: The algorithm accepts an identity ID_u, and outputs the secret key S_u.

iii. Extract-rekey: It accepts two identities $ID_1\ and\ ID_2$, and outputs the rekey from $ID_1\ and\ ID_2$.

iv. Signcryption: The signcryption accepts messages m, and two identities $ID_1\ and\ ID_2$, and outputs the signcryption for m from $ID_1\ and\ ID_2$

v. De-signcrypt: This accepts a signcryption message φ and identity ID_r, and outputs the de-signcryption of φ by ID_r.

vi. Re-encryption: It accepts a signcryption φ, and an identity ID_r, and outputs the re-encrypted signcryption φ' of φ to ID_r.

vii. De-re-encrypt: This accepts a second-level signcryption φ' and ID_d, and outputs the de-signcryption of φ' by way of ID_d .

6.4.1 The Scheme of signcryption proxy re-encryption (SCPRE)

The SCPRE scheme is derived from the identity-based signcryption scheme; the scheme is presented as follows:

Setup

Let I be the security parameter of the system. Let G_1 and G_2 be two prime ordered groups of order $q = \theta(2^I)$, where G_1 be represented additively, and G_2 be represented multiplicatively. Let P be a generator of G_1.

Let $e: G_1 \times G_2 \rightarrow G_2$, be a bilinear pairing. We assume that the Bilinear Computational Diffie-Hellman (BCDH) assumption holds in $< e, G_1, G_2 >$.

It uses four hash functions $H_0, H_1, H_2\ and\ H_3$, where

$$H_0: \{0,1\}^* \rightarrow G_1,$$

$$H_1: G_1 \times \{0,1\}^n \rightarrow Z_q^*.$$

$$H_2: G_2 \rightarrow \{0,1\}^{n+t}$$

$$H_3: G_1 \times \{0,1\}^* \rightarrow G_1$$

The n is the number of bits in the message, and t is the number of bits used to represent an element in G_1. The private key generator (PKG) chooses the master secret key $s \in R\ Z_q^*$, and sets the master public key $P_{pub} = sP$. The published public parameters are

$< e, G_1, G_2\ , n, q, P, P_{pub}, H_0, H_1, H_2 >$. Each user has his/her identity ID_u, and public key. He/she gets two secret keys S_u, and $S_{u||delegatee}$, by providing ID_u and $ID_{u||"delegatee"}$.

Extract (IDu)

The public key generator (PKG) computes the secret key as $S_u = s.H_0(ID_u)$, where $H_0(ID_u)$, is generally denoted by Q_u

Signcrypt $(\boldsymbol{m, S_A, ID_B})$

User A is to signcrypt a message m from delegator A to delegate B by using the following steps as:

1. Choose $r \in R\ Z_q^*$
2. Compute $X = rQ_A$ and $h = H_1(X||m)$
3. Compute the signature $Z = (r + h)S_A$
4. Choose $k \in R\ G_2$
5. Compute $Z = e(S_A, Q_B)^r$, and set $\lambda = w.k$
6. $y = H_2(k) \oplus (m||Z)$
7. The signcryption is $\emptyset =< X,\ y,\ ID_A >$.

De-signcrypt $(\emptyset =< \boldsymbol{X},\ \boldsymbol{y},\ \boldsymbol{\lambda},\ \boldsymbol{ID_A} >, \boldsymbol{S_B})$

The delegatee receiver B, after receiving the signcryption $\emptyset$, does the following.

1. $w = e(X, S_B)$
2. Compute $k = \lambda.w^{-1}$
3. Recover $m||Z = y \oplus H_2(k)$
4. $h_1 = H_1(X||m)$
5. If $e(Z, P) = e(P_{pub}, X + h_1.Q_A)$, then $< m, (X, Z), ID_A >$ This is the output as the message and signature. Otherwise, $\perp$ is output.

Rekey-Extract $(\boldsymbol{S_B, ID_C})$

B sends $rk_{B\to C} =< -S_B + H_3(e(S_B, Q_{(c||delegate)})) >$, to the proxy.

Re-encrypt $(\emptyset =< X,\ y,\ \lambda,\ ID_A >, rk_{B\to C}, ID_B, ID_C)$

The proxy computes re-encrypted signcryption $\emptyset' =< X, y, \lambda. e(X, rk_{B\to C}), ID_A, ID_B >$, and sends $\emptyset'$ to C.

De-re-encrypt $(\emptyset' =< X, y, \lambda', ID_A, ID_B >, S_{c||delegatee})$

On receipt of a level 2 signcryption, C decodes the algorithm as follows:

1. $w = e\left(X, H_3, \left(e\left(Q_B, S_{c||delegatee}\right)\right)\right)$
2. Compute $k = \lambda' w^{-1}$
3. Recover $m||Z = y \oplus H_2(k)$
4. $h_1 = H_1(X||m)$
5. If $e(Z, P) = e(P_{Pub}, X + h_1 Q_A)$, then output$< m, (X, Z), ID_A >$, else output $\perp$.

A collective thought for proxy re-signature and re-encryption schemes is to establish secures applications scenarios on a long term basis.

6.5 FORMAL VALIDATION USING AVISPA/SPAN TOOL

We simulated signcrypted proxy re-cryptographic approach in CAS implementation language and it is shown with sender principal pattern information executed on OFMC back end tool. It is a useful tool that allows and checks all participated agents to execute all the specified steps as a honest run participants, resultant in form of SAFE state, as depicted in Figure 6.2.

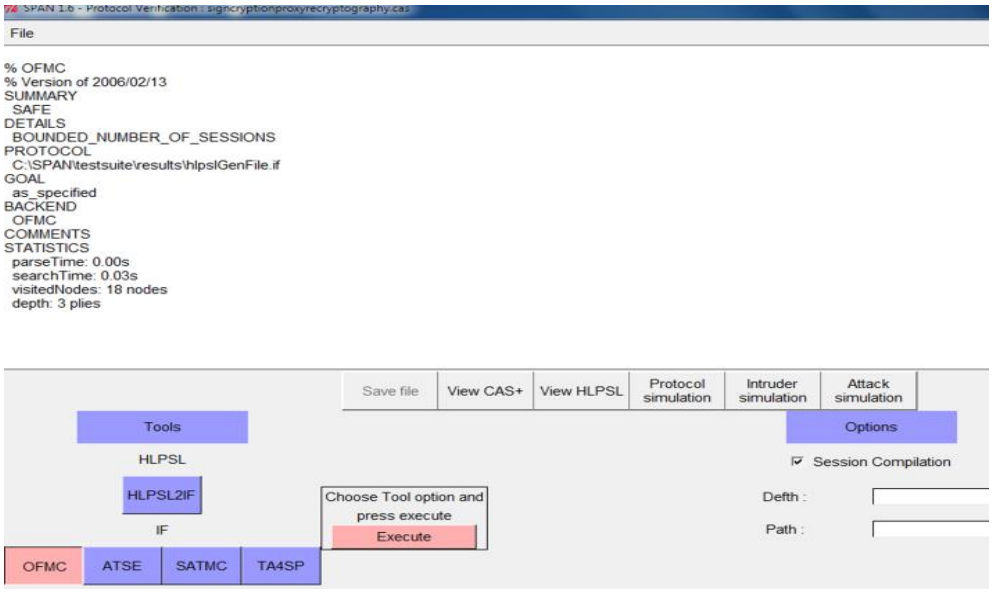


Figure 6.2: SPAN on OFMC Back End

CL-ATSE is a set of constraints, is working under to find attacks on designed protocols. The intermediate translation and checking are work automatic and internally performed on the same. This has executed same on AtSe tool, as shown in Figure 6.3, which is a presentation with negligible possibility of attack.

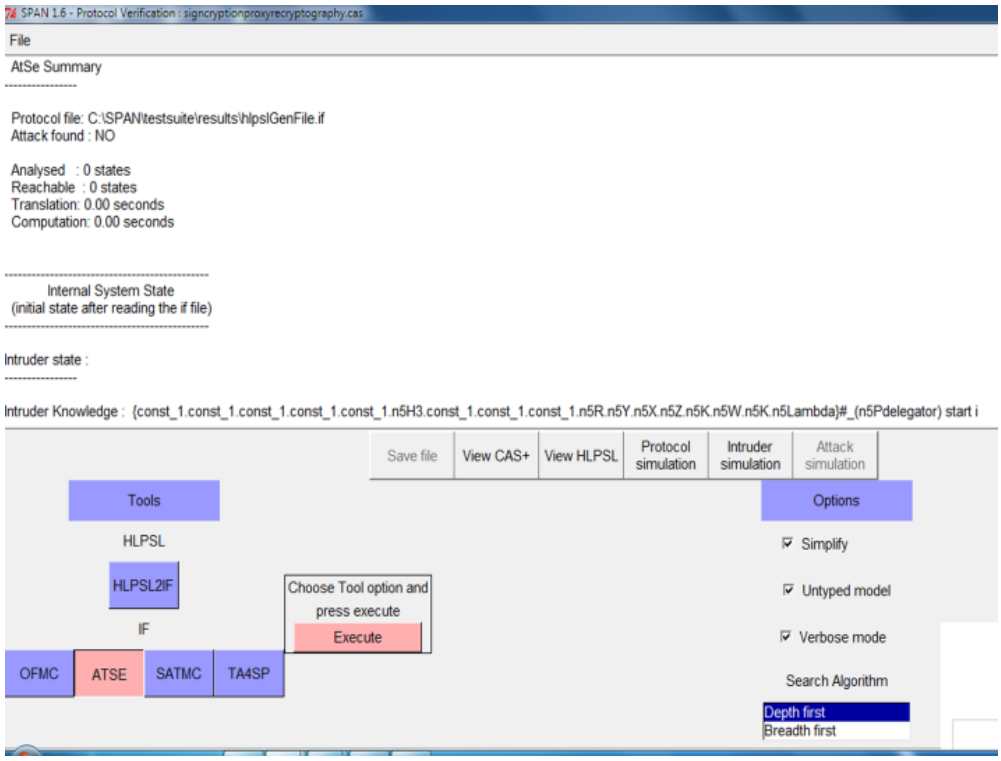


Figure 6.3: SPAN on AtSe Protocol Check

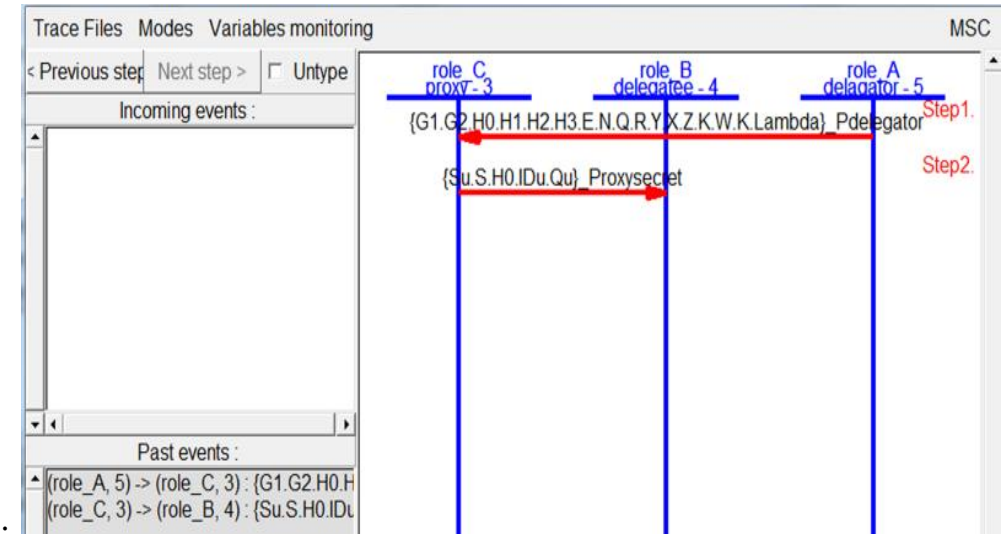


Figure 6.4: Sender pattern principal

The specification is automatically simulated in the proposed approach between delegator and delegatee via a third party of proxy. Here in figure 6.4, the pattern of sender principal is shown according to the above provided definition. The delegator, sends the message to proxy, where secret via proxy is added and sent to the delegatee where it is deciphered.

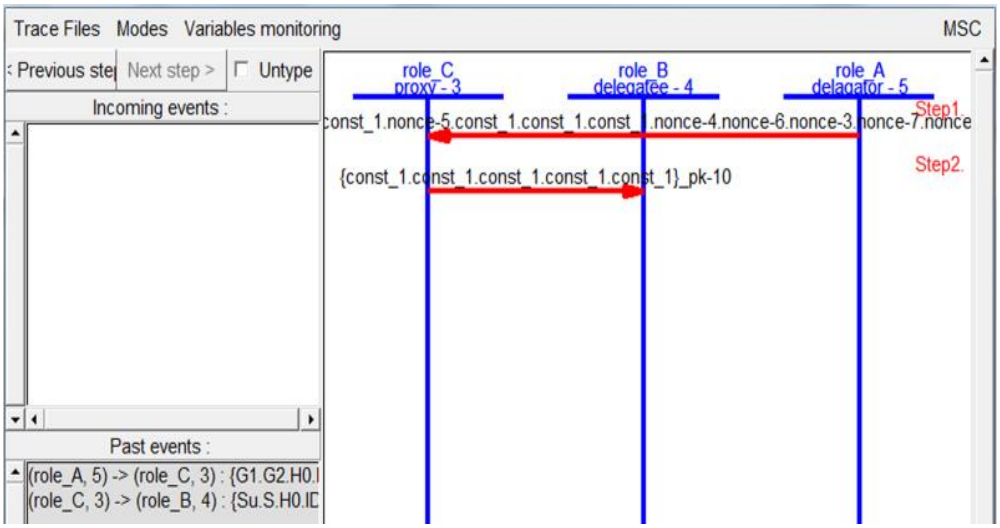


Figure 6.5: Real Type of Sending Messages View

This permits a CAS+ specification to translation for simple and fast specification of security protocols; interactively building a Message Sequence Chart (MSC) [110], [111]. But, originally messages are sent in the form of encrypted form over algorithm, where it is like to be impossible to decrypt, as depicted in Figure 6.5.

The definition has simulated with the Intruder with its knowledge, in Figure 6.6, with the real sender pattern principle.

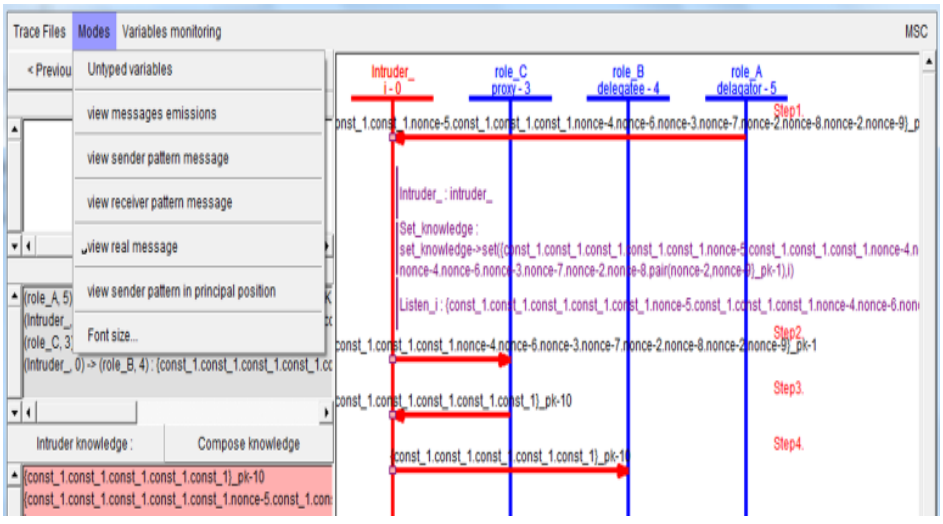


Figure 6.6: Intruder Simulation with knowledge on real messages

Further, in the last but not least, the various additional composition behaviors are also available, as exposed in Figure 6.7.

The analysis of four back-ends are harmonized to each other in a sense for some common back-ends procedure, but these are not equivalent so that should return different results.

Figure 6.7: With Intruder Real Type Pattern with Emissions

6.6 SUMMARY

The presented work is a motivation for the new direction of cryptography using the approach proxy re-cryptography for secure signcryption based protocol. The use of Signcryption approach is the new paradigm that fulfilling the most desired cryptographic applications and demanding due to the most of cost effective in sense of high performance, suits to low memory devices and so on. Further, we are highlighted some of future works as:- (i) to collect for the long-term schemes using proxy re-cryptography into a single location, though researchers can evaluate their suitability for various applications. (ii) The approach for modern cryptography with security requirements have arisen in different distributed environments as the attacks may come either from internal or external objects, (iii) proxy re-cryptography should be the standard model and it is collusion-resistant.

CHAPTER 7

SECURE AND ROBUST TELEMEDICINE USING ECC ON RADIX-8 WITH FORMAL VERIFICATION

The scalar multiplication techniques used in Elliptic curve cryptography (ECC) have great scope for gaining the computation efficiency. This is possible through the reduction of precomputed operations. Finding the more efficient techniques as compared to the most recent or efficient one is the research gap for all schemes. The chapter presented here has an application oriented work for Telemedicine using ECC. It is based on robust application on reduced computational complexity. The methodology we applied for the same is Scalar Multiplication without precomputation on Radix-8. The introduced software and the hardware performance are reported to have a big advantage over all the related proposed techniques. The reason to cover this problem is to provide a path in a fascinating area of ECC on a smaller key size to be applicable for all applications having a same level of security strengths. The smaller length key gives the higher speed and shorter clock cycle to initiate the operation.

7.1 INTRODUCTION

The scenarios for all applications are the concerns of performance and considerable security services in the real life. The security services are using the concept of cryptography as it has been considered to be a discipline of computer science. The performances are achieved through the use of optimized algorithms. The used algorithms are running with the data security techniques. In general, all the developed algorithms have been based on reduced costs of computation and communication cost. The associated researchers and/or cryptographers have shown their matured behavior in the field of security. But for research point of view it is still to excess and it is our motivational issue to enhance the system security services & performance. The general security service applications are in secure transmission of information, unidentified disclosure, and authenticity guarantee of data [11]. The level of ECC security is achieving a bigger marginal enhancement by its algorithms and they also need a very shorter length keys. The shorter length keys compute much faster and are also best suited to low memory devices. For example, for the same level of security RSA uses 1024 bit key whereas ECC uses only 160 bit key sizes [128].

We have considered and analyzed the algorithms for ECC on the core work of cryptography, which shows our proposed problem work on the latest research technological enhancement and in preference to it, it is most challenging to the side-channel attacks are is one most advanced studies is incorporated [140].

Several studies and reports for telemedicine [129], [130] have demonstrated the advantages, cost-savings and efficiency gains that are feasible by implementing technology and by digitizing the systems. The assessment of our purpose is to elaborate the cost effectiveness and contribution significance towards the proposed algorithms. The assessments of telemedicine studies are not of reasonable quality because of the questionable methodologies and techniques presented to date or they contain a narrow focus towards other important outcomes. At present, it is difficult to give a clear statement on the cost effectiveness and effective utilization through the technique advancements.

The organization of this chapter is as follows. Section 7.2 presents an application scenario for telemedicine application and its requirements analysis. Section 7.3 contains the Radix-8 technique for scalar multiplication without precomputation. This shows that the computation cost is shorter and enhances its performance by its related techniques. Section 7.4, gives the handshaking protocol on radix-8 scalar multiplication and encryption-decryption for ECC. The advantages of radix-8 are it offers aligned confrontation with the safe-error fault attacks and simple side channel attacks. In the next section, we gave a formal verification and validation on SPAN tool for our proposed work. Finally, we have summarized the chapter.

7.2 APPLICATION SCENARIOS FOR TELEMEDICINE

Telemedicine is concerned with healthcare services through the use of Information Communications Technologies (ICT) [131]. The participants can be either a health care professional and patients or communication between the two health care professionals. Included services are patient treatments, educating the health workforce, tracking diseases, and conducting research. It is generalized from the eHealth that covered the overall interoperability in ICT, utilization of standard sectors, best use of electronic patient records, Picture and Archiving systems (PACS), Health information systems (HIS), Radiology information systems (RIS), etc. This can also be defined as a discipline of social medical imagination that evaluates information from a part of medical, economic and ethical issues in a systematic manner. An assessment

purpose of telemedicine applications refers to quality care of services that describe effectiveness and produces a basis for decision making. This chapter defines the telemedicine as a brief assessment that is evaluated and is summarized information on ethical and medical in secure issues related to recent communication techniques in a systematic, robust and unbiased manner.

The produced strategies in this area cover to a large extent responsibility for the local health systems, national or regional levels. The challenges and responsibilities are not isolated to one region or one country; these can be taught and brought to achieve success through the designing of overall framework and association of collaboration. Mair and Whitten have said that telemedicine doesn't meet accepted standards [132], Hersch et al. are suggested to number of existing studies aren't well planned on technology augmentation [133], [134], Barlow et al. [135] are perceived on the needs of robust innovations simulation modeling. Further, Barlow et al. [136] called an evaluation review for the development in the field. Rojas at al. present systematic indicators on cost effectiveness in [137]. The ultimately goal is to ensure "confidence and acceptance of telemedicine solutions by health authorities, health professionals and patients".

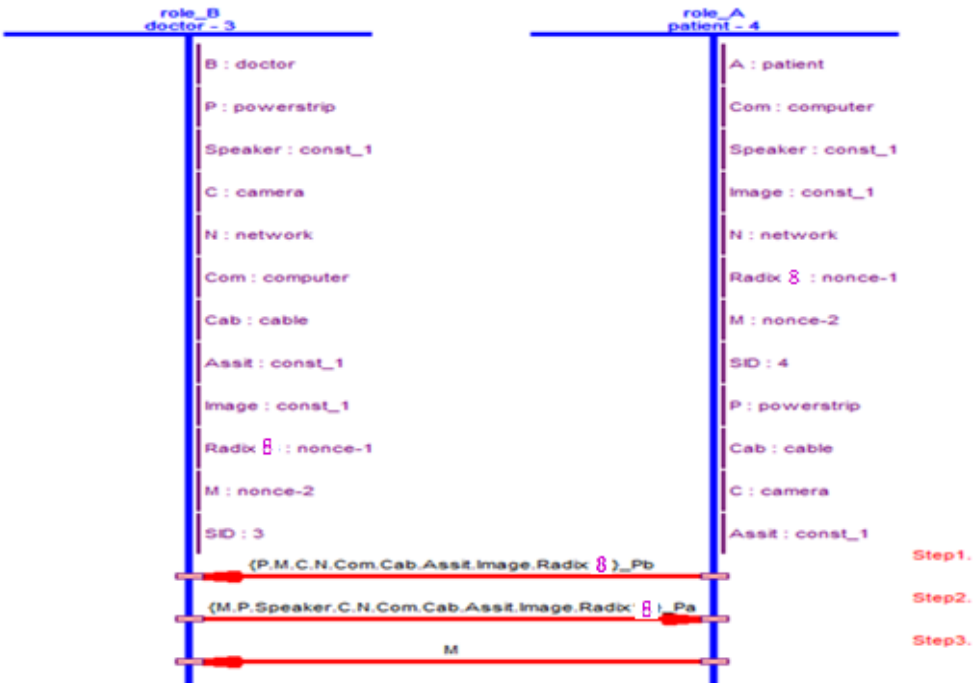


Figure 7.1: Telemedicine Scenario

The communication evidence shows that the effectiveness is based on too small datasets between a patient and doctor. The common sharing resources are computers, speakers, images,

networks, cables, cameras, and our implemented algorithms of radix-8, as shown in figure 7.1. Radix-8 is described in the next section. This demonstration is based on video conference over a network on a two way, where both are not at the same place to discuss a simple medical diagnosis, receive a report of diagnosis, prescription and for follow-ups. The main benefits consist of a direct access to mainstream medicine, whereas hospitals and clinics benefit from having access to specialists, to cover large scale medical facilities, broadening service etc. A similar approach has been proposed by Michael North in 1998 [138]. The scientific evidence can be extended to a large scale setting.

The literature reviewed conducted to build confidence, solve technical issues, bring clarity, accept services and facilitate the market development through the applications on systematic appraisal on costs of telemedicine services and its impacts. Health technology assessment (HTA) has considered a specific focus for the same. The assessment of telemedicine first starts with a strategic assumption on the various levels such as: local, regional, national. The core model should consist of the development of new applications involved in an element of time and dynamic process. The studies of technical and safety feasibility must be done before the clinical, patient related outcomes and economic can be initiated. Transferability assessment focuses on planned telemedicine application and varies with the assessment of the transferability (i.e., scale up the existing approach to large extent) specific results from other studies. The participants give a large number of comments like the model should be clear, e.g., model should be defined and its potential information's to users should be described, purpose should be part of the earlier consideration, and the domains generally considered be relevant, measures outcome of each domain strengthen potential strength that should to include the all considerable issues on the times spent for helping and assisting the patients using application.

Regarding the same, the possible questions are organization, legislation, and local assessment reimbursement should to be made available, or should it be made available at the national or regional level, the economic sustainability using telemedicine, the patients' observation of the telemedicine application and its effects, effects on safety or workflow and co-operation between primary and secondary care and ethical and telemedicine legal aspects. Here we are going to propose a technique that is more advanced than the existing approaches. This is based on reduced instruction set computing, lower bits require processing the information between two or more participants.

7.3 PROPOSES RADIX-8 RECORDING TECHNIQUE

This section presents scalar multiplication on radix-8. The scalar k records in the range of $[-1, 6]$ for discrete logarithmic problem that prevents it from simple side channel attacks..

7.3.1 Proposed Radix-8 Algorithm for Scalar Multiplication

As the non-seven encoded representation stored in array register $a[k_j]$, we use the same to do the scalar multiplication in Figure 7.2. For this reason Lemma 1 is extended, by setting to P_{kP} and P_1. For computing of P_{kp} at $a[k_j]$, with a maximum of Hamming weight added in (54)

$$P_{kP}^{j} = \begin{cases} P_{kP}^{j-1} + a[k_j]P_{ACC}^{j}, & if\ a[k_j] \in \{-1,0,1,2,4\} \\ 8P_{ACC}^{j} - P_1^{j}, & if\ a[k_j] \in \{3,5,6\} \end{cases} \tag{54}$$

Similarly, for P_1 the maximum of $(7 - a[k_j])$, adds in (55)

$$P_1^{j} = \begin{cases} 8P_{ACC}^{j} - P_{kP}^{j}, if\ a[k_j] \in \{-1,0,1,2,4\} \\ (7 - k_j^{'})P_{ACC}^{j} + P_1^{j-1}, & if\ a[k_j] \in \{3,5,6\} \end{cases} \tag{55}$$

At this point, P_{ACC} implicitly tries to be repeat after each of $a[k_j]$ by $P_{ACC} = 8P_{ACC}$. Now, we have done the computation as followed for $a[k_j] \in \{-1,0,1,2,4\}$:

$$\begin{cases} P_{kP} = P_{kP} + a[k_j]P_{ACC} \\ P_{ACC} = 8P_{ACC} \\ P_1 = P_{ACC} - P_{kP} \end{cases} \tag{56}$$

And for $a[k_j] \in \{3,5,6\}$ the operation is followed as:

$$\begin{cases} P_1 = P_1 + (7 - a[k_j])P_{ACC} \\ P_{ACC} = 8P_{ACC} \\ P_{kP} = P_{ACC} - P_1 \end{cases} \tag{57}$$

As the algorithm shown in Figure 7.3 does the scalar multiplication any point P considered to be available on the curve. It starts as initial assumptions as $P_{kP} = 0,\ P_1 = P,\ P_{ACC} = P$ registers and sequence counter set to the number of digits in non-seven encoded. Now, scan the non-seven representation from right-to-left i.e, the least significant bit first as $k_j = 0$ up to the most significant bit. The computation procedure iterated until SC reached to zero, the final result of P_{kP} is returned as output.

The used approached is validated through numerical example. Suppose scalar $k = 14715$ and its octal form is $(034673)_8$. Again, the same is represented in non-seven encoded form as

$(0346\bar{1}3)$. Table 7.1 is demonstrated as computational process. The computational time t for the taken scalar is $t = \lceil log_8 14715 \rceil + 1 = 6$. From the computational point of view, the computation cost t at radix-8 for scalar k, we can define its cost $t = \lceil log_8 k \rceil + 1$. This shows an average improvement over the most reduced computational complexity for a scalar multiplication.

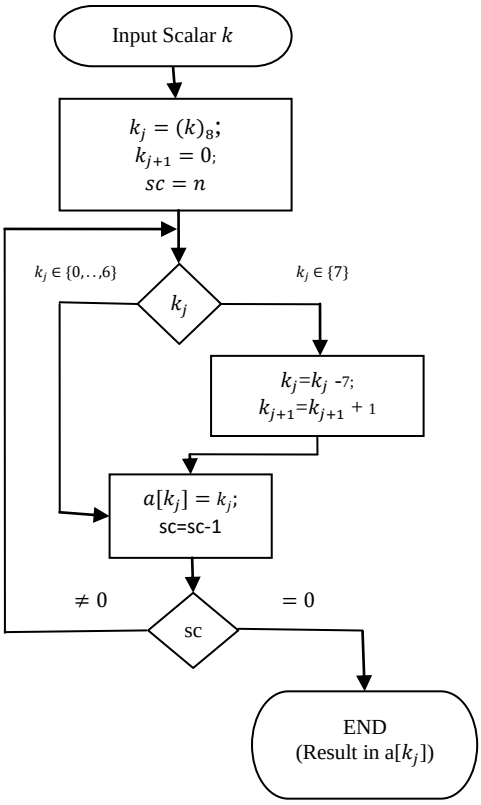


Figure 7.2: Non-Seven Encoding Representation

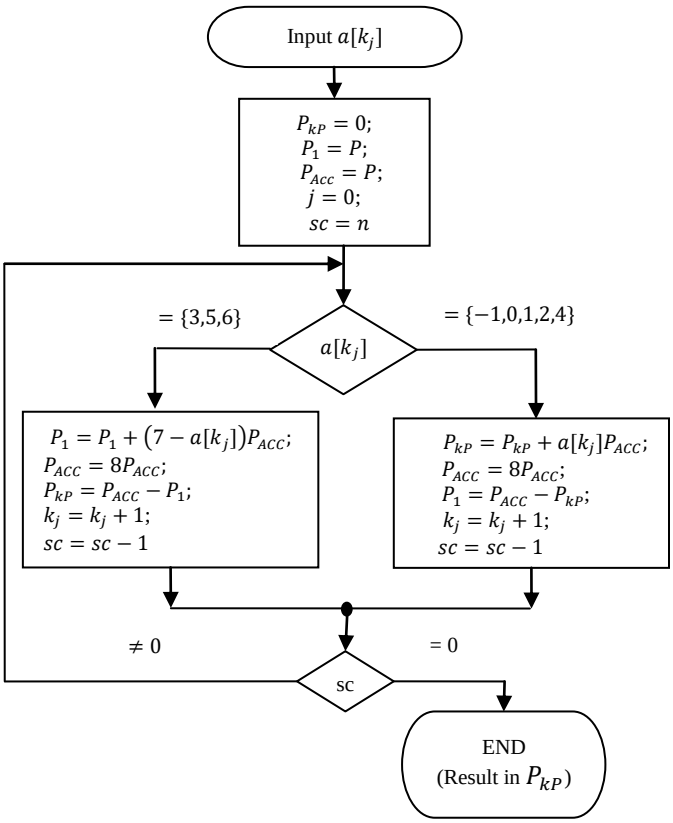


Figure 7.3: Radix-8 Scalar Multiplication

Tab1e 7.1: Numerical example of scalar multiplication on Radix-8

Register Array	**Initialization**	**(Iteration from Right-to-Left)**					
		SC=6, $a[k_j] = 3$	SC=5, $a[k_j] = -1$	SC=4, $a[k_j] = 6$	SC=3, $a[k_j] = 4$	SC=2, $a[k_j] = 3$	SC=1, $a[k_j] = 0$
$\mathbf{a[k_j]} \in \{-1,0,1,2,4,7,8,9,10,12\}$	$P_{kP} = 0$; $P_1 = P$; $P_{Acc} = P$		$P_{kP} = -5P$ $P_{Acc} = 64P$ $P_1 = 69P$		$P_{kP} = 2427P$ $P_{Acc} = 4096P$ $P_1 = 1669P$		$P_{kP} = 14715P$ $P_{Acc} = 262144P$ $P_1 = 247429P$
$\mathbf{a[k_j]} \in \{3,5,6,11,13,14\}$		$P_1 = 5P$ $P_{Acc} = 8P$ $P_{kP} = 3P$		$P_1 = 133P$ $P_{Acc} = 512P$ $P_{kP} = 379P$		$P_1 = 18053P$ $P_{Acc} = 32768P$ $P_{kP} = 14715P$	

7.4 KEY-EXCHANGE AND ENCRYPTION-DECRYPTION OVER ECC

Password Authenticated Key Exchange (PAKE) is simply a protocol derivational approach. It is based on a two-step process also known Simple Authenticated Key Exchange (SAKA), presented in [101]. We apply this approach for Elliptic Curve Cryptography on Telemedicine Application. In our approach we consider two such parties between a patient and doctor, in addition to this we pass information through unsecured medium. Each party is free to choose a random number and multiply it with group generator which creates a public key for each other according to standard $X.1035$. The generation of DLP is based on the prime factorization P and that are resisting guessing the password. Ding et al. have presented (03) three step PAKE to password impersonation compromise resistance to ephemeral key compromise, forward secrecy and dictionary attack. The IEEE 1063.2 released standard in 2009 is specified to more utilization of passwords and basis with stronger security for securing transactions [102], [100]. The set-up protocol works step-by-step as given in Figure 7.4:

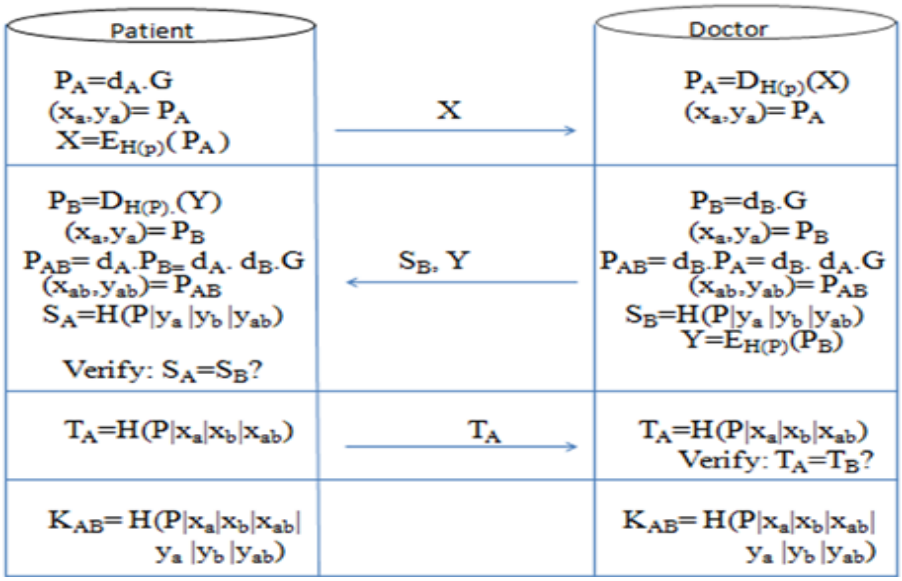


Figure 7.4: ECC-based PAKE (EPAK) protocol b/w Patient and Doctor

Step I: Patient is free to choose a random d_A as private key and is multiplied it to the global elements G and the obtained public key P_A. The same has been represented in Elliptic point (x_a, y_a). Now, hash of $H_{(P)}$ computes a symmetric key of P_A as X and sends it to Doctor.

$$P_A = d_A.G; (x_a, y_a) = P_A; X = E_{H(P)}(P_A) \quad (58)$$

A packet X is received by doctor, decrypted it and corresponding elliptic points as (x_a, y_a).

$$P_A = D_{H(p)}(X);\ (x_a, y_a) = P_A \quad (59)$$

Step II: Now, Doctor picked a random d_B as private key and multiplied to generator G, to generated public key P_B. This P_B is evaluated in Elliptic point (x_a, y_a):

$$P_B = d_B.G;\ (x_a, y_a) = P_B \quad (60)$$

Then, multiplied private key to Patient public key to obtained a shared key Q_{AB} and finded its appropriate EC points $(x_{ab}, y_{ab}) = P_{AB}$ then computed S_B having Q_A, Q_B and Q_{AB} and at end uses $H_{(P)}$ to encrypt:

$$Q_{AB} = d_B.P_A = d_B.d_A.G;\ (x_{ab}, y_{ab}) = P_{AB};\ S_B = H(P \mid y_a|y_b|y_{ab});\ Y = E_{H(P)}(P_B) \quad (61)$$

Patient used $H_{(P)}$ to decrypt Y, obtained Q_B and then transferred it in Elliptic point (x_a, y_a). Then, multiplied her/her private key to Doctor's public key Q_B to obtained a shared key Q_{AB} followed by (x_{ab}, y_{ab}). Finally computed S_A for verification of $Q_A, Q_B\ and\ Q_{AB}$. It verification held, then Doctor is the required information:

$$P_B = D_{H(P)}(Y);\ Q_{AB} = d_A.P_B = d_A.d_B.G;\ S_A = H(P|y_a|y_b|y_{ab}) \quad (62)$$

Step III: Patient calculated T_A out of Q_A, Q_B and Q_{AB} and sent to Doctor

$$T_A = (H(P|x_a|x_b|x_{ab}) \quad (63)$$

At other end Doctor evaluated T_B and compared with T_A. If the verification proper held, Doctor is then assured that Patient is required values as well:

$$T_B = H(P|x_a|x_b|x_{ab}) \quad (64)$$

Step IV: Therefore, intended parties are the required values and verified from both end. Finally, to evaluate a secret shared key as:

$$K_{AB} = H(P|x_a|x_b|x_{ab}\,|y_a|y_b|y_{ab}) \quad (65)$$

In the proposed work, the security and different attacks have been analyzed and modeled on the same, where an adversary (internal or external) is capable of recording, re-playing, deleting, re-routing, re-scheduling and re-ordering the messages. Instead of same, we are finding our approach is safe from all of these. We do the formal verification of the proposed scenario under the adversary conditions.

7.5 FORMAL VERIFICATION AND VALIDATION ON SPAN AND AVISPA TOOL

A SPAN is an impressive tool, works on simple editing protocol specifications. In addition to this, it also contains all the properties of AVISPA supported tool. In relation to the previous chapter for SPAN and AVISPA, it works on the automatic analysis technique. The language it uses is a High Level Protocol Specification Language (HLPSL). It specifyies intended security properties as it first translates into Intermediate Format (IF) through the translator HLPSL2IF. Where IF is a lower-level language and is directly interpreting the back-ends tools. This happens automatically and treatment is transparent to the user [104]. It comprises of four back-ends such as: On-the-fly Model Checker (OFMC) [105], Constraint Logic-based Attack Searcher (CL-AtSe) [106], SAT-based Model Checker (SATMC) [107], [108], and Tree-Automata Based Protocol Analyzer (TA4SP) [109].

The proposed Telemedicine application on tool shows it in the safe state, as shown in Figure 7.5, at back ends of OFMC and CL-AtSe relates to its safety measures.

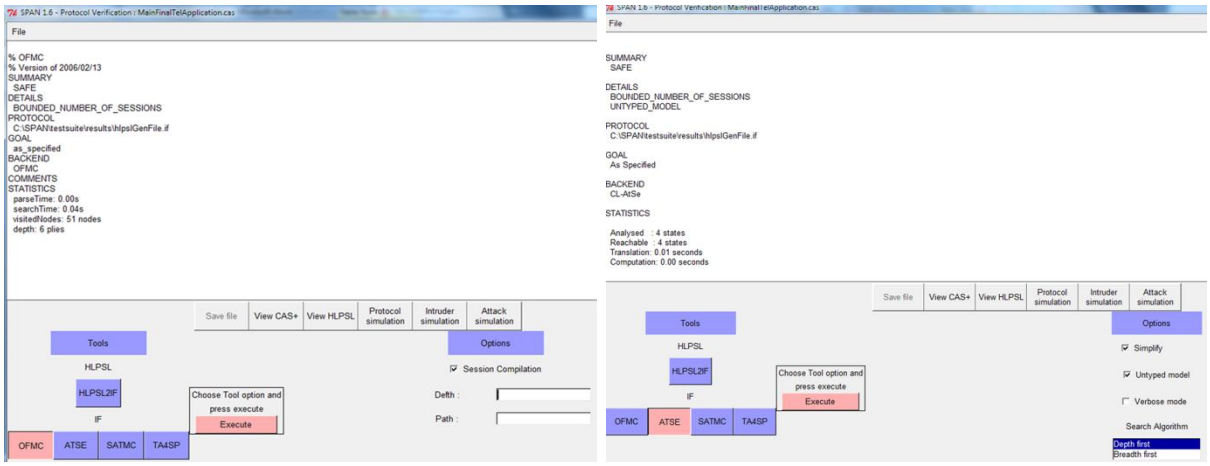


Figure 7.5: Results on OFMC & CL-ATSE

HLPSL is specifying the cryptographic protocols on AVISPA and CAS+ used for SPAN. This is translated into CAS+ specification from Patient-vs.-Doctor for fast and interactive specification of security protocols; building a Message Sequence Chart (MSC) [10], [31] of protocol execution; automatically builds attacks on MSC on HLPSL and CAS+ specifications, that are interactively built on specific attacks for the intruder. The Figure 7.6 is representing our protocol simulation on the real message flow during the processing. Attack simulation works on the same layout as intruder simulation, but attacks may be possible on OFMC/CL-AtSe.

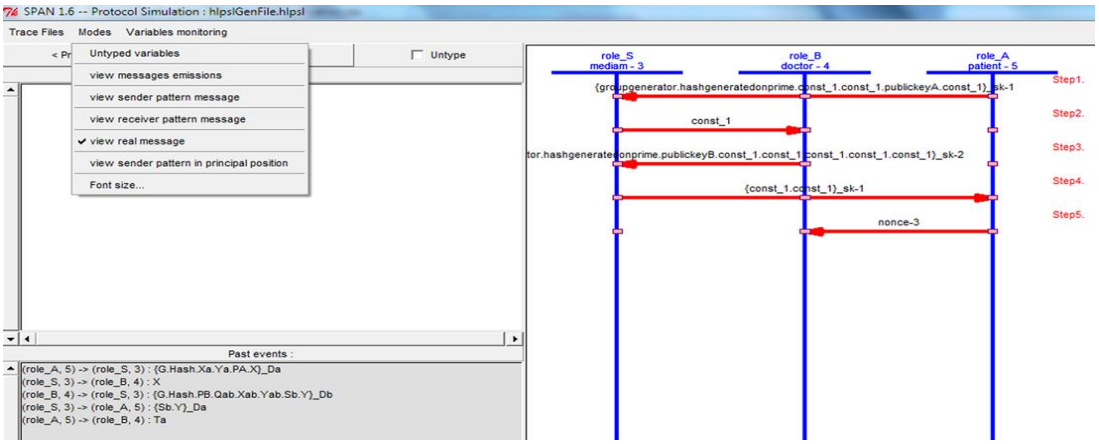


Figure 7.6: Protocol Simulation on Simple Message Transmission

Figure 7.7 shows the application prediction in presence of intruder, the state affairs says the passive attack on the proposed model is negligible to attack from the same instead the intruders know about the working principles of the protocol.

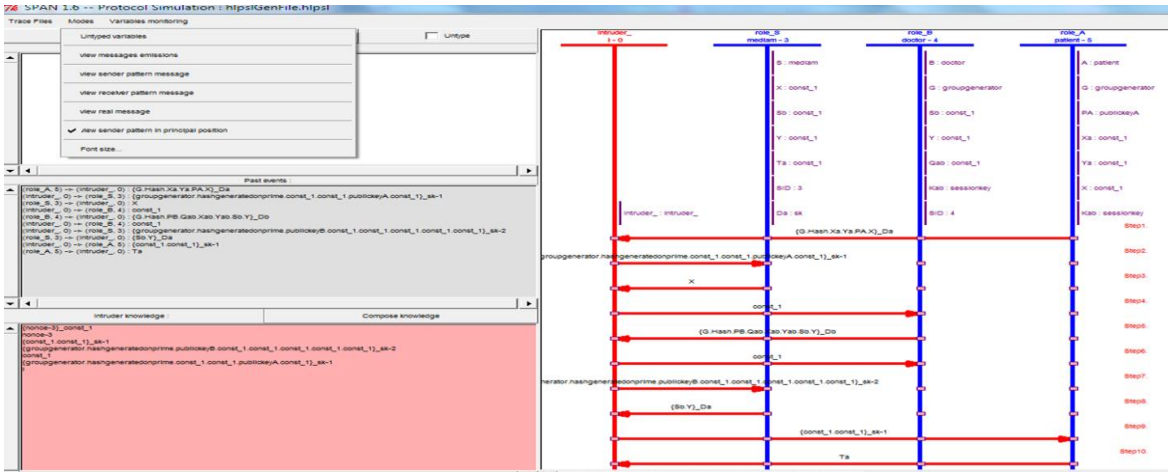


Figure 7.7: Intruder Simulation with actual sender, receiver and real messages view

7.6 SUMMARY

In this chapter, the application scenario for telemedicine is simulated on the most efficient technique proposed on radix-8 scalar multiplication without pre-computed operations for ECC. This scheme works on regular basis for all applications. The mathematical suitability best suits for discrete logarithmic problem for all digits contained in computation. On performance and securities considerations for short memory devices approach are in the most demanding requirements. Therefore, assumed application is the best suited application scenario for reduced instruction set computing. In addition to it, it offers to safe error fault attack and simple side channel attack, where the adversaries are capable of re-ordering, re-routing, recording, deleting, re-scheduling and re-playing with the messages.

CONCLUSION AND FUTURE WORK

The thesis presented advancement of the Discrete Logarithmic Problem (DLP) in the following four primitives of cryptography such as: Elliptic Curve Cryptography (ECC), Twisted Edwards Curves, Noncommutative Cryptography (NCC), multilayer key generation for ECC using signcryption, and proxy re-cryptographic approach in correlation with the signcryption. All these primitives, on behalf of the research gap, have formulated into five objectives. The chapter 1 presents an introduction related to all the five objectives. The respective objectives are concluded as below from (i) to (v):

(i) The first objective, chapter 2, pertains to Radix-16 scalar multiplication without pre-computation for ECC as a regular scheme. This radix shows the more appropriateness for reduced instruction set computing (RISC) architecture devices and is particular suitable for low memory devices. The proposed approach is against the attacks from simple side channel attacks and safe-error fault attacks. The approach is considered to be on high demanding with respect to software and hardware performance considerations. The major distinction is its computing speed 6.25% faster than recently proposed Radix-8 scalar multiplication technique without pre-computation. A hardware schematic is presented that can be applied for any applications. In reference to this the performance also gets improved by 8.33% on the proposed radix.

(ii) The second objective, chapter 3, contains the architecture of prime Edwards curves and extended Twisted Edwards curves on 4 and 8-processors to solve the Edwards curves and extended Twisted Edwards curves problem for scalar multiplication on reduced computation cost with significant improvements. The comparative reduction cost on the 4-processors is $2M + 1S + 1D + 3A$ to $2M + 1S + 1D + 2A$ and on the 8-processors is $2M + 3A$ to $2M + 2A$. This claims a significant improvement having gained the computational efficiency for Elliptic Curve Cryptography (ECC). The ECC is justifying the security strength and effectiveness on the shorter key lengths.

(iii)The third objective, chapter 4, pertains on Noncommutative Cryptography (NCC), which is a fascinating area on security and performance enhancement. A proposed scheme is based on the extra special group for finding the solution of an open problem for the most appropriate

Noncommutative platform. Regarding this the minimum group of the dihedral order, changes from D_3 to D_4, enhances the search space and makes the proposal stronger than all the previously predicted group. The basis of this group is established on the Hidden subgroup or subfield problem (HSP), where Conjugacy search problem (CSP) is likely to be intractable. The working principle is based on the random polynomials chosen by the communicating parties to secure key-exchange, encryption-decryption and authentication schemes on NCC. Further, this is enhanced from the general group elements to equivalent ring elements, known by the monomials generations for the cryptographic schemes. The group of orders is more challenging to attack like length based automorphism and brute-force attacks. It provides a high level of safety measures.

(iv)The fourth objective, chapter 5, is based on the secure composition derivation approach for multilayered consensus on key generation with significant improvement using the signcryption primitive. The results for ECC and multilayer consensus key generation approach tested on SPAN and Automated Validation of Internet Security Protocol Architecture (AVISAP) tool. It is showing in information security the proposed approach makes scientifically strong security mechanisms in applied cryptography.

(v) The fifth objective, a combined effort as represented in chapter 6-7, covers a probably secure and efficient approach with regards to the trust problem for third party, who is not directly involved 'called proxy', can be solved using signcryption re-cryptographic approach. In modern era of cryptography, this is one of the new diverse trends and motivating issues. Research interest focuses on situations under a cryptographic key management by a semi-trusted proxy with special information where data encrypted under one cryptographic key need to be re-encrypted. In correlation to the same, the presented work is a motivation for the new direction of cryptograph using signcryption. Further, same work is simulated on AVISPA/SPAN, using the automated formal verification tool. An application scenario for Telemedicine has also been simulated on above tool.

In addition, in regards to the proposed work, still future works are: (i) To give a more efficient technique than the radix-16 scalar multiplication without Precomputation. (ii) To make a more feasible solution for Edward's and twisted Edward's curve is a demanding issue. (iii) For noncommutative platform to give the solution for open problem. (iv) To give a more insight in

collection of the collect the long-term schemes using proxy re-cryptography applications that best evaluate their suitability for various applications at a single location (v) The approach for modern cryptography with security requirements is arisen in different distributed environments as the attacks may come either from internal or external objects, (v) Using the standard model of proxy re-cryptography make it to more efficient and collusion-resistant to till date, and etc.

REFERENCES

[1] Oded Goldreich, "*Foundations of Cryptography Basic Tools*," Vol. 1, Cambridge University Press, UK, 2004

[2] Oded Goldreich, "*Foundations of Cryptography Basic Applications*," Vol. 2, Cambridge University Press, UK, 2010

[3] W. Diffie and M. E. Hellman, "*Privacy and authentication: An introduction to cryptography*," Proc. IEEE, vol. 67, pp. 397–427, March 1979.

[4] J. Baek, "*Construction and Formal Security Analysis of Cryptographic Schemes in the Public Key Setting*," PhD Thesis, Monash University, 2004.

[5] Y. Desmedt, "*Cryptographic foundations*" In M. Atallah (Ed.), Handbook of Algorithms and Theory of Computation, chapter 38, CRC, Boca Raton, FL, 1998.

[6] Y. Glouche, T. Genet, O. Heen and O. Courtay "*A Security Protocol Animator Tool for AVISPA*" In *ARTIST2* Workshop on Security Specification and Verification of Embedded Systems, Pisa, May 2006.

[7] R. Saillard and T. Genet, "*CAS+*", Institute for Research in Computer Science and Random Systems, March 21, 2011. [Online: http://www.irisa.fr/celtique/genet/span/CAS_manual.pdf]

[8] Kevin S. McCurley, "*The Discrete Logarithm Problem*," Proceedings of Symposia in Applied Mathematics, Vol. 42, pp. 49-74, 1990. [Online: http://www.mccurley.org/papers/dlog.pdf]

[9] A. Joux, A. Odlyzko, C. Pierrot, "*The Past, evolving Present and Future of Discrete Logarithm*" Open Problems in Mathematics and Computational Science, Springer International Publishing, pp 5-36, 2014. DOI: 10.1007/978-3-319-10683-0_2

[10] A. M. Odlyzko, "*Discrete logarithms in finite fields and their cryptographic significance*" Advances in Cryptology: Proceedings of EUROCRYPT 84, ACM Digital Library, pp. 224–314, 1985.

[11] V. Jirasek, "*Practical Application of Information Security Models*," Information Security Technical Report, vol. 17, Issues 1–2, pp. 1-8, Feb. 2012. DOI: 10.1016/j.istr.2011.12.004

[12] W. Diffie and M.E. Hellman, "*New Directions in Cryptography*," IEEE Transaction on Information Theory, vol. 22, No. 6, pp. 644-654, Nov. 1976. DOI: 10.1109/TIT.1976.1055638

[13] K. Jarvinen and J. Skytta, "*Parallelization of High-Speed processor for Elliptic Curve Cryptography*," IEEE Transaction on VLSI, vol. 16, No. 9, pp. 1162-1175, Sep. 2008.

[14] N. Koblitz, "*Elliptic Curve Cryptosystems*," Math Computation, vol. 48, No. 177, pp. 203-209, 1987.

[15] V.S. Miller, "*Use of Elliptic Curves in Cryptography*," Advances in Cryptology, pp. 417-426, 1986. DOI: 10.1007/3-540-39799-X_31

[16] E.W. Knudsen, "*Elliptic Scalar Multiplication Using Point Halving*," in ASIACRYPT-99, LNCS 1716, pp. 135-149, 1999. DOI: 10.1007/978-3-540-48000-6_12

[17] I.F. Blake, V. Kumar Murty, and G. Xu, "*A note on window τ-adic NAF algorithm, in Information Processing letters*," vol. 95, pp. 496-502, Sep. 2005. DOI: 10.1016/j.ipl.2005.05.013

[18] D.R. Hankerson, A Menezes and S. Vanstone, "*Guide to Elliptic Curve Cryptography*," Springer, 2004. DOI: 10.1007/b97644

[19] S. Arno and F.S. Wheeler, "*Signed Digit Representations of Minimal Hamming Weight*," IEEE Transaction on Computers, vol. 2, No. 8, pp. 1007-1010, Aug. 1993. DOI: 10.1109/12.238495

[20] P. Longa and A. Miri, "*Fast and Flexible Elliptic Curve Point Arithmetic over Prime fields*," IEEE Transaction on Computers, vol. 57, No. 3, pp. 289–302, Mar. 2008.

[21] H. Hisil, K. K. H. Wong, G. Carter, and E. Dawson, "*Twisted Edwards curves Revisited*," Lecture Notes in Computer Science, vol. 5350, pp. 326-343, 2008. DOI: 10.1007/978-3-540-89255-7_20

[22] T. Izu and T. Takagi, "*Fast Elliptic Curve Multiplications with SIMD operations*," Information and Communication Security, Lecture Notes in Computer Science, vol. 2513, pp. 217-230, Dec. 2002. DOI: 10.1.1.97.5074.

[23] W. Fischer, C. Giraud, E. W. Knudsen, and J. -P. Seifert, "*Parallel Scalar Multiplication on General Elliptic Curves over F(p) hedged against Non-Differential Side-Channel Attacks*," IACR (2002/007), Cryptology ePrint Archive. [Online: http://eprint.iacr.org/2002/007].

[24] P. K. Mishra, "*Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems (Extended Version)*," IEEE Transaction on Computers, vol. 55, No. 8, pp. 1000–1010, Aug. 2006. DOI: 10.1109/TC.2006.129

[25] C.H. Gebotys, "*Elliptic Curve Cryptography*," Security in Embedded Devices, Springer, 2010, pp. 75-109. DOI: 10.1007/978-1-4419-1530-6

[26] C. Heuberger and H. Pondinger, "*Analysis of Alternatives Digits Sets for Non-Adjacent Representation*," SIAM Journal on Discrete Mathematics, vol. 19, No. 1, pp. 165–191, 2006. DOI: 10.1137/S0895480103437651
[27] C. Vuillaume, K. Okeya and T. Takagi, "*Short-Memory Scalar Multiplication for Koblitz Curve*," IEEE Transaction on Computers, vol. 57, No. 4, pp. 481-489, April 2008. DOI: 10.1109/TC.2007.70824
[28] M. Ciet, T. Lange, F. Sica, J Quisquater, "*Improved Algorithms for Efficient Arithmetic on Elliptic Curves using Fast Endomorphisms*," Advances in Cryptology-Proceeding of Eurocrypt, pp. 390-400, 2003. DOI: 10.1.1.113.3891
[29] R. M. Avanzi, C Heuberger, H Podinger, "*On Redundant τ-adic Expansions and Non-Adjacent Digit Sets*," Selected Areas in Cryptography, Springer-Verlag, pp. 285-301, 2007. DOI: 10.1007/978-3-540-74462-7_20
[30] E.A.H. Abdurrahman and A. R-Masoleh, "*New Regular Radix-8 Scheme for Elliptic Curve Scalar Multiplication without Pre-Computation*," IEEE Transaction on Computers, vol. 64, No. 2, pp. 438-451, Feb. 2015. DOI: 10.1109/TC.2013.213
[31] B. Parhami, Computer Arithmetic: Algorithms and Hardware Designs, 2nd Edition (2010), Oxford University Press.
[32] D. G. Han and T. Takagi, "*Some analysis of radix- representations*," IACR, Cryptology ePrint Archive, 2005. [Online Available]: http://eprint.iacr.org/2005/402.
[33] A. Kargl and G. Wiesend, "*On Randomized Addition-Subtraction Chains to Counteract Differential Power Attacks*," in the Information Communication Security, Lecture Notes in Computer Science, vol. 3269, pp. 278–290, 2004. DOI: 10.1007/978-3-540-30191-2_22
[34] C. Giraud and V. Verneuil, "*Atomicity Improvement for Elliptic Curve Scalar Multiplication*," LNCS 6035 (CARDIS 2010), pp. 80-101, 2010. [Online: https://hal.archives-ouvertes.fr/inria-00459461/document]
[35] J. S. Coron, "*Resistance against differential power analysis for elliptic curve cryptosystems*," Cryptographic Hardware and Embedded Systems, Springer Berlin Heidelberg, vol. 1717, pp. 292–302, Aug. 1999. DOI: 10.1007/3-540-48059-5_25.
[36] C. Clavier and M. Joye, "*Universal Exponentiation Algorithm A First Step towards Provable SPA-Resistance*," LNCS 2162 (CHES 2001), pp. 300-308.
[37] B. Moller, "*Securing elliptic curve point multiplication against side-channel attacks*," LNCS 2200 (ISC 2001), pp. 324-334. 2001.
[38] K. Okeya and T. Takagi, "*The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks*," in LNCS 2612 (CT-RSA 2003), pp. 328-343.
[39] J. Lopez and R. Dahab, "*Fast Multiplication on Elliptic Curves over GF (*2^m*) without Precomputation*," in LNCS 1717 (1999), pp. 316-327.
[40] P. L. Montgomery, "*Speeding the Pollard and elliptic curve methods of factorization*," Mathematical Computation, vol. 48 (Jan. 1987), No. 177, pp. 243–264.
[41] K. Okeya, H. Kurumatani, and K. Sakurai, "*Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications*," LNCS 1751 (2000), pp. 238-257.
[42] M. Joye and S. M. Yen, "*The Montgomery Powering Ladder, in Cryptographic Hardware Embedded Systems*," Lecture Notes in Computer Science, Springer-Verlag, Vol. 2523 (CHES-2003), pp. 291-302.
[43] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "*Twisted Edwards curves revisited*," in (ASIACRYPT'08) Proceedings International Conference Theory and Application of Cryptology and Information Security: Advances in Cryptology (Jun. 2008), pp. 326–343. DOI: 10.1007/978-3-540-89255-7_20
[44] HM Edwards, "*A Normal Form of Elliptic Curves*," Bulletin American Mathematical Society, vol. 44 (July 2009), No. 3, pp. 339-442.
[45] B. Baldwin, R. Mononey, A. Byrne, G. McGuire, "*A Hardware Analysis of Twisted Edwards Curves for an Elliptic Curve Cryptography*," in International Workshop on Application Reconfigeration Computing (2009). [Online: https://eprint.iacr.org/2009/001.pdf]
[46] D.J. Bernstein, T. Lange, "*Faster addition and doubling on elliptic curves*," in ASIACRYPT 2007, Vol. 4833, K. Kurosawa (Ed.), Lecture Notes in Computer Science, Springer, 2007, pp. 29–50.
[47] D.J. Bernstein, T. Lange, "*Inverted Edwards coordinates*," in AAECC-17, Vol. 4851, S. Boztas and H.F. Lu (Eds.), Lecture Notes in Computer Science, Springer, 2007, pp. 20–27.
[48] D.J. Bernstein, T. Lange, "*Analysis and Optimization of elliptic-curve single scalar multiplication*," Contemporary Mathematics. [Online: http://www.hyperelliptic.org/EFD/precomp.pdf]
[49] V.S. Miller, "*Use of elliptic curves in cryptography*," In Proceedings of CRYPTO '85 Advances in Cryptology, ACM, New York, NY, pp. 417-426, 1985. DOI: dl.acm.org/citation.cfm?id=704566

[50] P.W. Shor, "*Algorithms for Quantum Computation: Discrete logarithms and Factorings*," In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994. DOI:10.1109/SFCS.1994.365700

[51] A. Kitaev, "*Quantum Measurements and the Abelian Stabilizer Problem. Electronic Colloquium on Computational Complexity*," Vol. 3, 1996. DOI: http://eccc.hpi-web.de/eccc-reports/1996/TR96-003/index.html

[52] E. Lee, "*Braid groups in Cryptology*," ICICE Transactions on Fundamentals, Vol. E87-A, no. 5, pp. 986-992, 2004.

[53] J. Proos and C. Zalka, "*Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curve*," Quantum Information & Computation, Vol. 3, pp. 317-344, 2003. DOI: http://dl.acm.org/citation.cfm?id=2011531

[54] M. Rotteler, "*Quantum Algorithm: A Survey of Some Recent Results*," Information Forensic Entw., Vol. 21, pp. 3-20, 2006. DOI: http://link.springer.com/content/pdf/10.1007%2Fs00450-006-0008-7.pdf

[55] N.R. Wagner and M.R. Magyarik, "*A Public-Key Cryptosystem based on the Word Problem*," George Robert Blakley, and David Chaum (Eds.), CRYPTO'84, Vol. 196. LNCS, Springer-Verlag, Germany, pp. 19-36, 1985. DOI: http://link.springer.com/chapter/10.1007%2F3-540-39568-7_3

[56] J.C. Birget, S. S. Magliveras, and M. Sramka, "*On Public-Key Cryptosystems based on Combinatorial Group Theory*," International Journal of Cryptographic Research, 2005. DOI: https://eprint.iacr.org/2005/070.pdf

[57] I. Anshel, M. Anshel, and D. Goldfeld, "*An algebraic method for public-key cryptography*," Mathematical Research Letters, Vol. 6, pp. 287-291, 1999. DOI: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6801

[58] K.H. Ko, S.J. Lee, J.H. Cheon, J. W. Han, J.S. Kang, and C. Park, "*New Public-Key Cryptosystem Using Braid Groups*," In: M. Bellare (Eds.): CRYPTO 2000, LNCS, Springer-Verlag, Germany, Vol. 1880, pp. 166-183, 2000. DOI: http://www.math.snu.ac.kr/~jhcheon/publications/2000/LNCS_Crypto00_KLC.pdf

[59] P. Dehornoy, "*Braid-based Cryptography*," Contemporary Mathematics, Vol. 360, pp. 5-33, 2004. DOI: www.math.unicaen.fr/~dehornoy/Surveys/Dgw.pdf

[60] I. Anshel, M. Anshel, and D. Goldfeld, "*Non-abelian key agreement protocols*," Discrete Applied Mathematics. Elsevier, Vol. 130, pp. 3-12, Aug 2003. DOI: 10.1016/S0166-218X(02)00585-1

[61] I. Anshel, M. Anshel, and D. Goldfeld, "*A Linear Time Matrix Key Agreement Protocol over Small Finite Fields*," AAECC, 2006. DOI: http://link.springer.com/content/pdf/10.1007/s00200-006-0001-1.pdf

[62] J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, and J.H. Cheon, "*An Efficient Implementation of Braid Groups*," C. Boyd (Ed.): ASIACRYPTO 2001, Vol. 2248, pp. 144-156, LNCS, Springer-Verlag, 2001. DOI: http://link.springer.com/chapter/10.1007%2F3-540-45682-1_9#page-1

[63] K. H. Ko, D.H. Choi, M.S. Cho, and J.W. Lee, "*New Signature Scheme using Conjugacy Problem*," Cryptology ePrint Archive: Report 2002/168, 2002. DOI: https://eprint.iacr.org/2002/168

[64] J.H. Cheon and B. Jun, "*A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem*," In proceeding of CRYPTO-2003, D. Boneh (Ed.), LNCS, Springer-Verlag, Germany, Vol. 2729, pp. 212-225, 2003. DOI: http://link.springer.com/book/10.1007/b11817

[65] J. Hughes and A. Tannenbaum, "*Length-Based Attacks for Certain Group Based Encryption Rewriting Systems*," Institute for Mathematics and Its Application, 2000. DOI: http://purl.umn.edu/3443

[66] J.M. Bohli, B. Glas, and R. Steinwandt, "*Towards Provable Secure Group Key Agreement Building on Group Theory*," Cryptology ePrint Archive: Report 2006/079, 2006. DOI: https://eprint.iacr.org/2006/079

[67] P. Dehornoy, "*Braid-based Cryptography, in: Group Theory, Statistics, and Cryptography*," Alexei G Myasnikov, Vladimir Shpilrain (Eds.), Contemporary Mathematics, Vol. 360, pp. 5-33, 2004.

[68] S.H Paeng, K.C Ha, J.H Kim, S. Chee, and C. Park, "*New Public Key Cryptosystem using Finite Non Abelian Groups*," In Proceeding of CRYPTO-2001: J. Kilian (Ed.), LNCS, Springer-Verlag., Germany, Vol. 2139, pp. 470-485, 2001.

[69] S.S. Magliveras, D.R. Stinson, and T.V Trung, "*New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups*," Journal of Cryptology, Vol. 15, pp. 347-373, 2002.

[70] M.I.G. Vasco, C. Martinez, and R. Steinwandt, "*Towards a Uniform Description of Several Group based Cryptographic Primitives*," Cryptology ePrint Archive: Report 2002/048, 2002.

[71] S.S. Magliveras, D.R. Stinson, T.V Trung, "*New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trap-Doors in Finite Groups*," Journal of Cryptology, Vol. 15, pp. 285-297, 2002. DOI: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.7868.

[72] D. Grigoriey and I.V. Ponomarenko, "*On Non-Abelian Homomorphic Public-Key Cryptosystems*," preprint arXiv: cs.CR/0207079, 2002.

[73] D. Grigoriey and I.V. Ponomarenko, "*Homomorphic Public-Key Cryptosystems over Groups and Rings*," CoRR, cs.CR/0309010, 2003. DOI: http://arxiv.org/pdf/cs/0309010.pdf
[74] B. Eick and D. Kahrobaei, "*Polycyclic Groups: A New Platform for Cryptography*," Preprint arXiv: math.GR/0411077, 2004. DOI: http://arxiv.org/pdf/math/0411077
[75] V. Shpilrain and A. Ushakov, "*Thompson's Group and Public Key Cryptography*," In proceedings of the 3rd. International Conference on Applied Cryptography and Network Security (ICACNS'05). Springer-Verlag Berlin, Heidelberg, pp. 151-163, 2005. DOI: http://dl.acm.org/citation.cfm?id=2134543
[76] A. Mahalanobis, "*The Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups*," Ph.D. Dissertation, Florida Atlantic University, Boca Raton, Florida, 2005. DOI: https://eprint.iacr.org/2005/223.pdf
[77] L. Wang, L. Wang, Z. Cao, E. Okamoto, and J.n Shao, "*New Constructions of Public-Key Encryption Schemes from Conjugacy Search Problems*," Lectures Notes in Computer Science, Springer-Verlag, Heidelberg Vol. 6584 , pp. 1-17, 2010. DOI: http://link.springer.com/chapter/10.1007%2F978-3-642-21518-6_1
[78] Z. Cao, X. Dong, and L. Wang, "*New Public Key Cryptosystems Using Polynomials over Noncommutative Rings*," Int. J. Crypto. Research, Vol. 9, pp. 1-35, 2007. DOI: https://eprint.iacr.org/2007/009.pdf
[79] J. Kubo, "*The Dihedral Group as a Family Group*," Quantum Field Theory and beyond, Wolfhart Zimmermann, Erhard Seiler, Klaus Sibold (Eds.), World Science Publication, Hackensack, NJ, pp. 46–63, 2008. DOI: http://www.worldscientific.com/worldscibooks/10.1142/6963
[80] P. V. Reddy, G.S.G.N. Anjaneyulu, D.V. Ramakoti Reddy, and M. Padmavathamma, "*New Digital Signature Scheme using Polynomials over Noncommutative Groups*," International Journal of Computer Science and Network Security, Vol. 8, pp. 245-250, 2008. DOI: http://paper.ijcsns.org/07_book/200801/20080135.pdf
[81] D.N. Moldovyan and N.A. Moldovyan, "*A New Hard Problem over Noncommutative Finite Groups for Cryptographic Protocols*," Lecture Notes in Computer Science, Springer-Verlag Heidelberg, New York, Vol. 6258, pp. 183-194, 2010. DOI: 10.1007/978-3-642-14706-7_14
[82] A.D. Myasnikov and A. Ushakov, "*Cryptanalysis of Matrix Conjugation Schemes*," Journal of Mathematical Cryptology, Vol. 8, pp. 95-114, 2014. DOI: 10.1515/jmc-2012-0033
[83] K. Svozil, "*Non-Contextual Chocolate Balls versus Value Indefinite Quantum Cryptography*," Theoretical Computer Science, Elsevier, Vol. 560, pp. 82–90, 2014. DOI: http://tph.tuwien.ac.at/~svozil/publ/2013-qchocolate-j.pdf
[84] S.R. Blackburn, "*Groups of Prime Power Order with Werived Subgroup of Prime Order*," Journal of Algebra, Vol. 219, pp. 625–657, 1999. DOI:10.1006/jabr.1998.7909
[85] B.C. Hall, "*Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*," Springer, New York, Vol. 222, 2003. DOI: http://link.springer.com/book/10.1007%2F978-0-387-21554-9
[86] D.S Dummit and R.M. Foote, "*Abstract Algebra (3rd ed.)*," John Wiley & Sons, Hoboken, NJ, 2004.
[87] Tsit Yuen Lam (Ed.), "*Introduction to Quadratic Forms over Fields Quaternion algebras and their norm forms*," American Mathematical Society, University of California, Berkeley, CA, Vol. 67, 2005.
[88] William Stallings (Ed.), "*Diffie-Hellman Algorithm*," in Cryptography and Network Security: Principles and Practice, (5th. ed.), Pearson Education, New York, Chapter 10, 2011.
[89] D. Ruinskiy, A. Shamir, and B. Tsaban, "*Length-based Cryptanalysis: The case of Thompson's group*," Journal of Mathematical Cryptology. Vol. 1, pp. 359-372, 2007. DOI: 10.1515/jmc.2007.018
[90] A. D. Myasnikov and A. Ushakov, "*Length Based Attack and Braid Groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key Exchange Protocol*," Lecture Notes in Computer Science, Springer-Verlag, Heidelberg, Berlin, Vol. 4450, 2007. DOI: http://link.springer.com/chapter/10.1007%2F978-3-540-71677-8_6
[91] Zhenfu Cao (Ed.), "*Noncommutative Cryptography*" in New Directions of Modern Cryptography, CRC Press, 2013.
[92] M. Uno and M. Kano, "*Visual Cryptography Schemes with Dihedral Group Access Structure*," In Proc. Of ISPEC'07, Springer-Verlag, pp. 344-359, 2007. DOI: http://dl.acm.org/citation.cfm?id=1759542
[93] A. Datta, "*Security Analysis of Network Protocol: Compositional Reasoning and Complexity-Theoretic Foundations*," PhD Thesis, Department of Computer Science Stanford University, 2005. Online: http://seclab.stanford.edu/pcl/papers/datta-thesis.pdf
[94] A. Datta, A. Derek, J.C Mitchell, and A. Roy, "*Protocol Composition Logic*," Electronics Notes in Theoretical Computer Science (ENTCS), Elsevier, vol. 172, pp. 311-358, April 2007. DOI: 10.1016/j.entcs.2007.02.012
[95] A. Datta, A. Derek, J.C Mitchell, and D. Pavlovic , "*A Derivation System for Security Protocols and its Logical Formalization*," in Proceeding of 16th IEEE Computer Security Foundations Workshop, pp. 109-125, 2003.

[96] M. Borrows, M. Abadi, and R. Needham "*A logic of authentication*," ACM Transaction on Computer Systems, vol. 8, pp. 18-36,1990.
[97] E. Amini, Z. Jeddi, and M. Bayoumi, "*A High-Throughput ECC Architecture*," in 19th IEEE Int'l Conf. on Electronic, Circuits and Systems, pp. 901-904, Dec. 2012. DOI: 10.1007/978-3-540-89255-7_20
[98] : *Introduction to NISTIR 7628 guidelines for smart grid cyber security*. National Institute of Standards and Technology (NIST), 2010. [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.
[99] Z. You, J. Tao, and X. Li, "*Extension and Application of Protocol Composition Logic*" in Proceeding ICCET, IEEE, vol. 4, pp. V4-77-V4-81, 2010. DOI: 10.11.9/ICCET.2010.5485720
[100] H. Nicanfar and V.C.M Leung, "*Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System*" IEEE Transactions on Smart Grid, pp. 1-12, 2012.
[101] D.H. Seo, and P. Sweeney, "*Simple authenticated key agreement algorithm*" Electronic Letters, Institution of Engineering and technology, vol. 35, pp. 1073–1074, 1999. DOI: 10.1049/el:19990724.
[102] D. Xiao-fei, M. Chuan-gui, and C. Qing-feng, "*Password authenticated key exchange protocol with stronger security*" in 1st Int'l Workshop (Wuhan, Hubei, China) Education Technology and Computer Science (ETCS'09), IEEE, vol. 2, pp. 678-681, 2009. DOI: 10.1109/ETCS.2009.411
[103] : *AVISPA-Automated Validation of Internet Security Protocols* [online] Available: http://www.avispa-project.org.
[104] V. Sperschneider and G. Antoniou, "*Logic: A Foundation for Computer Science*," 1st ed., Addison-Wesley Longman, USA, 1991.
[105] D. Basin, S. Modersheim, and L. Vigano, "*OFMC: A Symbolic Model-Checker for Security Protocols*", International Journal of Information Security, vol. 4, pp. 181-208, 2005. DOI: 10.1007/s10207-004-0055-7
[106] M. Turuani, "*The CL-AtSe Protocol Analyzer*", Lecture Notes in Computer Science, vol. 4098, F. Pfenning, Eds. in RTE, 2006, pp. 277-286. DOI: 10.1007/11805618_21
[107] A. Armando and L. Compagna, "*Automatic SAT-Compilation of Protocol Insecurity Problems via Reduction to Planning*", in Proceedings of FORTE 2002, Lecture Notes in Computer Science, vol. 2529, pp. 210–225, 2002. DOI:10.1007/3-540-36135-9_14
[108] A. Armando and L. Compagna, "*Abstraction-driven SAT-based Analysis of Security Protocols*," in Proceedings of TAST, Lecture Notes in Computer Science, vol. 2919, pp. 257-271, 2004. DOI:10.1007/978-3-540-24605-3_20
[109] Y. Boichut, N. Kosmatov, and L. Vigneron, "*Validation of Prouve Protocols using the Automatic Tool TA4SP*," in 3rd Taiwanese-French Conf. on Information Technology, pp. 467-480, 2006.
[110] D. Harel and P.S Thiagarajan, "*Message Sequence Charts*," UML for Real: Design of Embedded Real-time Systems, 2003.
[111] D. Dolev and A. Yao "*On security of Public key protocols*," IEEE Transactions on Information Theory, vol. 29, 1983. DOI: 10.1109/TIT.1983.1056650.
[112] W. Stallings, *Cryptography and Network Security*, Principles and Practices, 3rd Ed., Pearson Education, 2004.
[113] Y. Zheng, "*Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)*," in Advances in Cryptology-CRYPTO'97, Lecture Notes in Computer Science, Springer-Verlag, vol. 1294, pp. 165-179, 1997.
[114] J. Baek, R. Steinfeld, and Y. Zheng, "*Formal Proofs for the Security of Signcryption*," in Public Key Cryptography (PKC 2002), Lecture Notes in Computer Science, Springer-Verlag, vol. 2274, pp. 80-98, 2002.
[115] A Basu, I Sengupta, and J.K Sing, "*Formal Security Verification of Secured ECC Based Signcryption Scheme*,"Advances in Intelligent Systems and Computing, Springer Berlin, vol. 167, pp. 713-725, 2012 [Digests proceedings of the 2nd Int'l Conf. on Computer Science, Engineering & Applications, (ICCSEA), 2012]. DOI: 10.1007/978-3-642-30111-7_68
[116] Y. Han, and X. Yang, "*ECGSC: Elliptic Curve based Generalized Signcryption Scheme*," Journal of Cryptology, 2006. [Available: https://eprint.iacr.org/2006.pdf]
[117] Islam, S.K.H., and Biswas, G.P., "*Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairing*," Journal of King Saud University, vol. 25, 51-62, 2011. DOI: 10.1016/j. jksuci.2012.06.003
[118] Z. Cao, "*New Directions of Modern Cryptography, Proxy Re-cryptography*," CRC Press. Taylor & Francis Group, Chap. 2, 2013.
[119] G. Ateniese, K. Fu, M. Green, S. Hohenberger, "*Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage*," Proceedings of the 12th Annual Network and Distributed Systems Security Symposium NDSS'05, San Diego, California, 2005. Available at: http://spar.isi.jhu.edu/~mgreen/proxy.pdf

[120] J. Shao, Z. Cao, "*Multiuse unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption*," Journal Information Sciences, 206, 83-95, 2012. DOI: dl.acm.org/citation.cfm?id=2228798
[121] M. Blaze, G. Bleumer, and M. Strauss, "*Divertible protocols and atomic proxy cryptography*," In EUROCRYPT 1998, volume 1403, LNCS, pp. 127–144, 1998. DOI: 10.1007/BFb0054122
[122] M. Green, G. Ateniese, "*Identity-Based Proxy Re-Encryption*," Applied Cryptography and Network Security Conference, vol. 4521, pp. 288-306, 2007. Available: http://eprint.iacr.org/eprint-bin/cite.pl?entry= 2006/473
[123] F. Li, M.K. Khan, K. Alghathbar, T. Takagi, "*Identity-based online/offline signcryption for low power devices*," Journal of Network and Computer Applications, 35 (1), 340-347, 2012. DOI: 10.1016/j. junkie.2011.08.001
[124] Z. Wang, X. Du, Y. Sun, "*Group Key Management Scheme of Proxy Re-cryptography for Near Space Network*," IEEE Int'l conf., 1-5, 2011.
[125] G. Taban, A.A Cardenas, and V.D Gligor, "*Towards a secure DRM Architecture*," DRM'06, October 30, Alexandria, Virginia, USA. DOI: 10.1.1.85.360, 2006.
[126] Y. Zheng, "*Signcryption and Its Applications in Efficient Public Key Solutions*," Information Security Workshop (ISW'97), Lecture Notes in Computer Science, Springer-Verlag, Vol.1397, pp.291-312, 1998. DOI: 10.1.1.101.3826
[127] S. Ohata, Y. Kawai, Y., T. Matsuda, G. Hanaoka, and K. Matsuura, "*Re-encryption Verifiability: How to Detect Malicious Activities of a Proxy in Proxy Re-encryption*," Springer, Journal of Cryptology, 2015. Available: https://eprint.iacr.org/2015/112.pdf
[128] J.W. Bos, M.E Kaihara, T. Kleinjung, A.K. Lenstra, P.L Montgomery, "*On the security of 1024-bit rsa and 160-bit elliptic curve cryptography*", IACR Cryptology ePrint Archive, 2009:389. [online: http://lacal.epfl.ch/files/content/sites/lacal/files/papers/ecdl2.pdf]
[129] A. Broderick and D. Lindeman, "*Case Studies in Telehealth Adoption*" Jan. 2013[Online: http://www.commonwealthfund.org/~/media/Files/Publications/Case%20Study/2013/Jan/1654_Broderick_telehealth_adoption_synthesis.pdf]
[130] M.A. Hein, "*Telemedicine: An Important Force in the Transformation of Healthcare*," June 2009 [Online: http://www.trade.gov/td/health/telemedicine_2009.pdf]
[131] : *Telemedicine Opportunities and Developments in Members States, Second Global Survey on eHealth*, 2010 [Online: http://www.who.int/goe/publications/goe_telemedicine_2010.pdf].
[132] F. Mair F, and P. Whitten P, "*Systematic review of studies of patient satisfaction with telemedicine*," British Medical Journal, 320:1517-1520, 2000.
[133] W.R. Hersh, M. Helfand, J. Wallace, D. Kraemer, P. Patterson, S. Shapiro and M. Greenlick, "*Clinical outcomes resulting from telemedicine intervention: a systematic review*," BMC Medical Informatics and Decision Making 1:5, 2001
[134] W.R. Hersch, D.H Hickam, S.M. Severance, T. L. Dana, K.P. Krages and M. Helfand , "*Telemedicine for the Medicare population: Update. 2006 Evidence Report/Technology Assessment*," No. 131 (Prepared by the Oregon Evidence-based Practice Center under Contract No. 290-02-0024.) AHRQ Publication No. 06-E007. Rockville, MD: Agency for Healthcare Research and Quality
[135] J. Barlow, S. Bayer, B. Castleton, R. Curry, "*Meeting government objectives for telecare in moving from local implementation to mainstream services*," Journal of Telemedicine and Telecare, 11, S1:49-51, 2005.
[136] J. Barlow, "*Building an Evidence Base for Successful Telecare Implementation – Updated Report of the Evidence Working Group of the Telecare Policy Collaborative*," [Online:http://ssia.wlga.gov.uk/media/pdf/f/4/APPENDIX_B_CSIP_Telecare.pdf. 2006]
[137] S.V. Rojas and M.P. Gagnon MP, "*A systematic review of the key indicators for assessing telehomecare cost-effectiveness*," Telemed J E Health 14(9): 896-904, 2008.
[138] M. North, "*Telemedicine sample script and specifications for a demonstration of simple medical diagnosis and treatment using live two-way video on a computer network*," Available at: www.greenstar.org/2scenario.pdf, Retrieved on: 19th February, 2016.
[139] S. Chadrasekhar, K. Ambika, C.P. Rangan, "*Signcryption with Proxy Re-encryption*," Journal of Cryptology, IACR Eprint, 1-19, 2008. DOI: http://eprint. iacr.org /2008 /276
[140] S.D. Jao, S.R. Raju, and R. Venkatesan, "*Digit set randomization in Elliptic Curve Cryptography*", Lecture Notes in Computer Science, Volume 4665, pp 105-117, 2007. DOI: 10.1007/978-3-540-74871-7_10
[141] [Online: Atmel-8951-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-WhitePaper.pdf]

APPENDIX

Appendix 1: Lemma proof works as follows:

Rearranges equation (7) by $r^{j+1}P = P_1^j + P_{kP}^j$, now replaces j to $j-1$ gives:

$$r^j P = P_1^{j-1} + P_{kP}^{j-1} \quad \text{(i)}$$

Substitute $r^j P$ in equation (4):

$$P_{kP}^j = k_i'\left(P_1^{j-1} + P_{kP}^{j-1}\right) + P_{kP}^{j-1};\ P_{kP}^j = k_i' P_1^{j-1} + \left(k_i' + 1\right)P_{kP}^{j-1} \quad \text{(ii)}$$

Again rearranges (7) from j to $j-1$ as $P_{kP}^{j-1} = r^j P - P_1^{j-1}$, use P_{kP}^j from (ii) and put the same in equation (4):

$$P_1^j = r^{j+1}P - \left(k_i' P_1^{j-1} + \left(k_i' + 1\right)P_{kP}^{j-1}\right) \quad \text{(iii)}$$

Further, substitute P_{kP}^{j-1} from (i) in (iii), here $P_{kP}^{j-1} = r^j P - P_1^{j-1}$:

$$P_1^j = r^{j+1}P - \left(k_i' P_1^{j-1} + \left(k_i' + 1\right)P_{kP}^{j-1}\right)$$

$$P_1^j = r^{j+1}P - \left(k_i' P_1^{j-1} + \left(k_i' + 1\right)\left(r^j P - P_1^{j-1}\right)\right)$$

$$P_1^j = r^{j+1}P - k_i' r^j P - r^j P + P_1^{j-1}$$

$$P_1^j = r.\, r^j P - k_i' r^j P - r^j P + P_1^{j-1}$$

$$P_1^j = \left(r - \left(k_i' + 1\right)\right) r^j P + P_1^{j-1} \quad \text{(iv)}$$

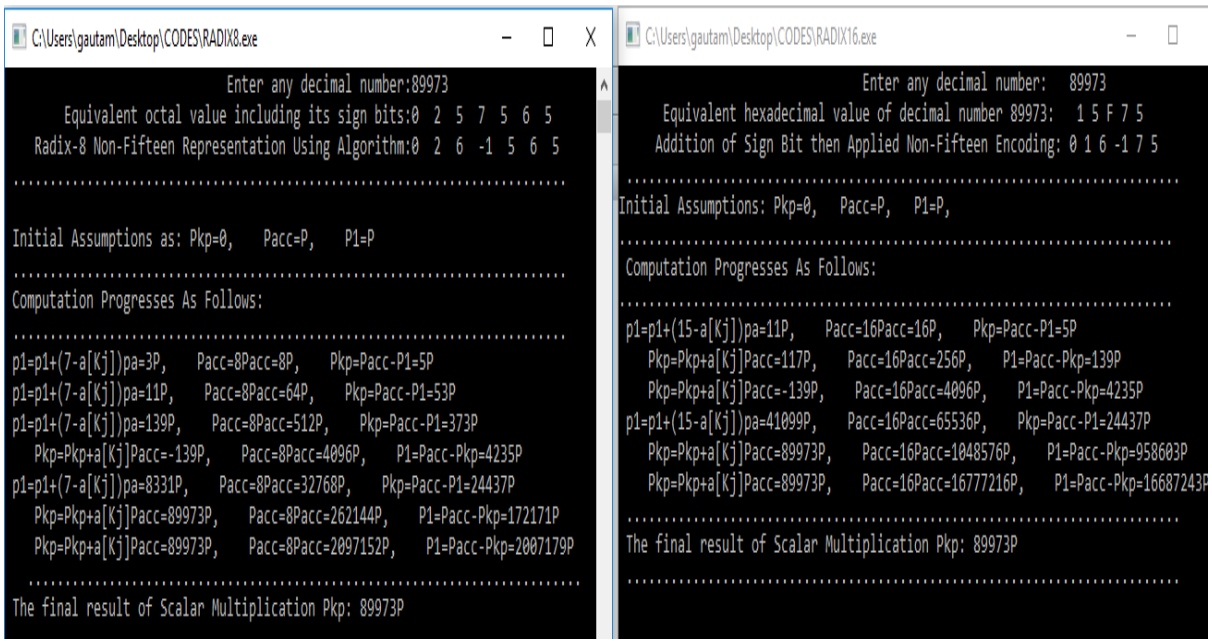
Use equation (5), replaces $r^j P$ to P_{ACC}^j:

$$P_1^j = \left(r - \left(k_i' + 1\right)\right) P_{ACC}^j + P_1^{j-1} \quad \text{(v)}$$

For equation (8) to satisfy it uses (7) $P_1^j = r^{j+1}P - P_{kP}^j \xrightarrow{\Delta} P_{kP}^j = r.\, r^j P - P_1^j$; again uses (5) for $P_{kP}^j = r.\, P_{ACC}^j - P_1^j$ and for second equation it uses (4) as: $P_{kP}^j = k_i' r^i P + P_{kP}^{j-1} \xrightarrow{\Delta} P_{kP}^j = k_i' P_{ACC}^j + P_{kP}^{j-1}$. For equation (9) to satisfy it uses (7) $P_1^j = r^{j+1}P - P_{kP}^j$; $P_1^j = r.\, r^j P - P_{kP}^j$, now uses (5) $P_1^j = r.\, P_{ACC}^j - P_{kP}^j$ and for second equation of (9), it uses (iv) as $P_1^j = \left(r - \left(k_i' + 1\right)\right) r^j P + P_1^{j-1}$. Here Lemma1 proofs complete.

Appendix 2: Experimental Result verification in C programming in Comparison to Radix-8 and Radix-16 Scalar Multiplication.

Implementation of Radix-8 and Radix-16 we implemented in C programming. So, both of these two implementations validate our experimental proof. Schematic is shown here (below):



Radix-8 and Radix-16 Simulation on C Programming

Appendix 3: If SIMD limitation is not proposed on results of Figure 3.3 the following consequences may occur: (i) we may not be able to make a co-relation on the already proposed solutions, so it will likely to be missing research track, if limitation is not given. (ii) Most modern CPU designs (particularly applicable to all common system) include SIMD instructions in order to improve the performance, so if SIMD limitation is not proposed it may lead to change in CPU design architectures at many levels. At that time one researcher may not be able to show the comparisons in this context. (iii) SIMD execution imposes computations in parallel in locked fashion, and its execution is easy to understand and implement. So, we followed the standard procedure in all regards. Therefore in relation to previous proposed works we are strict on the SIMD limitation.

LIST OF PUBLICATIONS

Published:

1. **Gautam Kumar** and Hemraj Saini, "**Novel Noncommutative Cryptography Scheme using Extra Special Group,**" **Security and Communication Networks**, John Wiley & Sons, Vol. 2017, Issue 5, pp. 1-21, January 2017. DOI: 10.1155/2017/9036382. [**Major Indexing:** ***Science Citation Index Expanded***, **SCOPUS**, DBLP, Compendex], SJR: 0.3, Impact Factor: 1.06
2. **Gautam Kumar** and Hemraj Saini, "**Secure and Robust Telemedicine using ECC on Radix-8 with Formal Verification**" **International Journal of Information Security and Privacy**, IGI Global Publishing, Vol. 12, Issue 1, pp. 13-28, 2018. [**Major Indexing:** ACM Digital Library, **SCOPUS**, Thompson Reuters, DBLP], SJR: 0.11, Impact Factor: 0.26
3. **Gautam Kumar** and Hemraj Saini, **"Effective Signcryption Approach for Secure Convention for Multilayer Consensus using ECC," International Journal of Information Security and its Applications,** Vol. 10, No. 7, pp. 287-306, Aug 2016. [**Major Indexing:** EICompendex, **SCOPUS**, Emerging Source Citation Index [Part of Science Citation Index Expanded and Thompson Reuters], SJR: 0.27, Impact Factor: 0.39
4. **Gautam Kumar** and Hemraj Saini**, "Reduced Precomputed Scalar Multiplication Cost for ECC" Contemporary Engineering Sciences, Hikari Ltd.,** Vol. 9, No. 18, pp. 897-904, 2016. [**Major Indexing:** CrossRef, **SCOPUS,** Google Scholar], SJR: 0.24, Impact Factor: 0.47.
5. **Gautam Kumar** and Hemraj Saini, **"Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem," International Journal of Applied Engineering Research,** Vol. 10, No. 24, pp. 44271-44277, 2015. [**Major Indexing:** Thompson Reuters, **SCOPUS,** & Google Scholar], SJR: 0.13, Impact Factor: 0.12
6. **Gautam Kumar** and Hemraj Saini, "**On Reduced Computation Cost for Edwards and extended Twisted Edwards Curves**" **Indian Journal of Science and Technology**, Vol. 9(44), November-2016. DOI: 10.17485/ijst/2016/v9i44/105071. [**Major Indexing:** Thompson Reuters, **SCOPUS**, Index Copernicus, DOAJ], SJR: 0.26, Impact Factor: 0.87.

International Conference

1. **Gautam Kumar** and Hemraj Saini, **"Secure Composition of ECC-PAKE Protocol for Multilayer Consensus using Signcryption,**" **International Conference on Communication Systems and Network Technologies (CSNT)**, IEEE Computer Society, pp. 740-745, April 2015. DOI: 10.1109/CSNT.2015.91, **[Major Indexing: SCOPUS]**

2. **Gautam Kumar** and Hemraj Saini **"Secure and Efficient ECC: Radix-16 Scalar Multiplication without Pre-Computation," International Conference on Big Data and Advanced Wireless Technologies,** ACM - Digital Library, New York, USA**,** 10 November 2016. **ISBN: 978-1-4503-4779-2. DOI: http://dx.doi.org/10.1145/3010089.3010105 [*Major Indexing:*** ACM Digital Library, **SCOPUS**, DBLP**]**

Book Chapter

1. **Gautam Kumar** and Hemraj Saini, "Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem'' **Advanced Engineering Research and Applications**, (Ed.) Hongseok Choi, Ch. 6, pp. 99-118, 2017. ISBN No. 978-93-84443-42-9. [*Major Indexing: Google Scholar, Advanced Science Index, Academia.edu*]

BIBLIOGRAPHY

Name: **Gautam Kumar**
E-mail: gautam.kumar@mail.juit.ac.in, gautam21ujrb@gmail.com

PROFESSIONAL QUALIFICATION:

- **PhD*** [Computer Science & Engineering]: Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh (INDIA). [YoR: July 2013]
- **M. Tech** [Computer Science & Engineering] from Rajasthan Technical University, Kota [2012] (INDIA)
- **B.E** [Computer Science & Engineering] from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal [2005] (INDIA)

JOURNAL'S

(i) **Gautam Kumar** and Hemraj Saini, "Novel Noncommutative Cryptography Scheme using Extra Special Group," ***Security and Communication Networks,*** John Wiley & Sons, Vol. 2017, Issue 5, pp. 1-21, January 2017. DOI: 10.1155/2017/9036382. *[**Major Indexing:** Science Citation Index Expanded, Scopus, DBLP, Compendex]*

(ii) **Gautam Kumar** and Hemraj Saini "Secure and Robust Telemedicine using ECC on Radix-8 with Formal Verification," **International Journal of Information Security and Privacy**, IGI Global Publishing, Vol. 12, Issue 1, pp. 13-28, 2018. [***Major Indexing:*** *Scopus, ACM Digital Library, Thompson Reuters, DBLP*]

(iii) **Gautam Kumar** and Hemraj Saini "Effective Signcryption Approach for Secure Convention for Multilayer Consensus using ECC," **International Journal of Security and its Applications,** Science & Engineering Research Support Society, Vol. 10, No. 7, pp. 287-306, 2016. [*Major Indexing: Scopus, EICompendex, Emerging SCI, Thompson Reuters*]

(iv) **Gautam Kumar** a**nd Hemraj Saini, "Reduced Precomputed Scalar Multiplication Cost for ECC**" **Contemporary Engineering Sciences**, Hikari Ltd., Vol. 9, No. 18, pp. 897-904, 2016. [Major Indexing: *Scopus, CrossRef, Google Scholar*].

(v) **Gautam Kumar and Hemraj Saini "Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem, "**International Journal of Applied Engineering Research, **Research India Publication,** Vol. 10, Number 24, PP. 44271-44277, 2015**. [**Major Indexing: **Scopus, Thompson Reuters]**

(vi) **Gautam Kumar** and Hemraj Saini "On Reduced Computation Cost for Edwards and extended Twisted Edwards Curves," **Indian Journal of Science and Technology,** Indian Society for Education and Environment, India, Vol. 9, Issue 44, November-2016. DOI: 10.17485/ijst/2016/v9i44/105071 [Major Indexing: Scopus, Thompson Reuters, Index Copernicus, DOAJ]

(vii) **Gautam Kumar,** Pratap Singh Patwal and Yogesh Gupta, "Performance Optimization using Fuzzy Modular Arithmetic in Short-Memory Scalar Multiplication for Koblitz Curve," **International Journal of Advances in Engineering Sciences**, Vol. 1, Issue 1, January 2011. [Major Indexing: DOAJ & Google Scholar]

(viii) **Gautam Kumar**, Shailendra Pratap Singh & Shadab Pasha "Performance Optimization Using Fuzzy Modular Arithmetic In Short-Memory Scalar Multiplication And Division of Binary Numbers Calculation For Koblitz Curve," **National Journal of Engineering Science And Management**, **Vol. 1, No. 1, July 2011. [ISSN: 2249-0264, LNCT, Bhopal].**

INTERNATIONAL CONFERENCES

(i) **Gautam Kumar** and Hemraj Saini **"**Secure and Efficient ECC: Radix-16 Scalar Multiplication without Pre-Computation," **International Conference on Big Data and Advanced Wireless Technologies**, ACM Digital Library, New York, USA, Nov. 2016. Online: **http://dx.doi.org/10.1145/3010089.3010105**. **ISBN:** 978-1-4503-4779-2 *[**Major Indexing:** ACM Digital Library, SCOPUS, DBLP]*.

(ii) **Gautam Kumar** and Hemraj Saini **"**Secure Composition of ECC-PAKE Protocol for Multilayer Consensus Using Signcryption," **Fifth IEEE International Conference on Communication Systems and Network Technologies**, IEEE Computer Society, Gwalior, M.P, pp. 740-745, 4-6 April 2015. DOI: 10.1109/CSNT.2015.91 *[**Major Indexing:** Scopus]*

(iii) **Gautam Kumar** and Hemraj Saini **"**Monomials Cryptographic Approach and Advanced Scenario for Length Based Attacks," in **International Conference on Cyber Security**, International Journal of Advanced Studies in Computer Science and Engineering, The Institution of Engineering and Technology (IET), Vol. 6, Issue 9, 2017. *[**Major Indexing:** IET, Index Copernicus, Google Scholar]* **[Accepted]**

(iv) **Gautam Kumar** & Pratap Singh Patwal, "Performance Optimization using Fuzzy Modular Arithmetic in Short-Memory Scalar Multiplication for Koblitz Curve" **International Conference in Sciences & Engineering**, Rohtak, India, 21-22 Jan. 2011. ***[Conf. Proceeding]***

(v) **Gautam Kumar**, Pratap Singh Patwal & Amit Kumar, "Short-Term Scalar Multiplication for Koblitz Curve" **International Conference on Emerging Trends in Engineering & Technology (IETET-2010),** Geeta Institute of Management & Technology, Kanipla, Kurukshetra, 14-16 October 2010. ***[Conf. Proceeding]***

(vi) **Gautam Kumar**, Pratap Singh Patwal & Amit Kumar "Short-Term Scalar Multiplication for Koblitz Curve" **International Conference on Reliability, Infocom Technology and Optimization (ICRITO-2010)** (Trends and Future Direction), Lingaya's University, Faridabad, Haryana, 1-3 November 2010. ***[Conf. Proceeding]***.

(vii) **Gautam Kumar**, Mahendra Kumar Verma & Yogesh Chand Gupta, "Short-Term Scalar Multiplication for Koblitz Curve" **International Conference on Computer Engineering and Technology (ICCET' 10),** Jodhpur Institute of Engineering & Technology, 13-14 November 2010. ***[Conf. Proceeding]***.

(viii) LK Sharma, Jeetendar Saini, Yogesh Chand Gupta, **Gautam Kumar**, "Importance of Digital Signature with an Enhanced Exchange of Information," **International Conference on VLSI, Communication & Networking,** IET, Alwar, Rajasthan, 24-25 December 2011. ***[Conf. Proceeding]***

NATIONAL CONFERENCES

(i) **Gautam Kumar**, Pratap Singh Patwal, LK Sharma, Robins Yadav, "A Comparative Analysis of ECC Development and an Implementation" **National Conference on Communication, Networking & Security**, 26-27 Feb 2011 [participated & presented a research paper: Institute of Engineering & Technology]. ***[Conf. Proceeding]***

(ii) Shailendra Pratap Singh, **Gautam Kumar**, Amar Nayak, "Optimization and Simulation of Routing Algorithm in Wireless Sensor Networks" **National Conference on Communication, Networking & Security,** 26-27 Feb 2011 [Participated and Presented a research paper: Institute of Engineering & Technology]. ***[Conf. Proceeding]***

(iii) Shailendra Pratap Singh, Amar Nayak, **Gautam Kumar**, "Analysis and Design of an Efficient Algorithm for K-Means Clustering" **National Conference on Communication, Networking & Security**, 26-27 Feb 2011 [participated & presented a research paper: Institute of Engineering & Technology]. ***[Conf. Proceeding]***

Book Chapter

(i) **Gautam Kumar** and Hemraj Saini, "Formal Verification on Signcryption Re-Cryptography: Secure and Efficient Approach towards Trust Problem'' **Advanced Engineering Research and Applications**, (Ed.) Hongseok Choi, Ch. 6, pp. 99-118, 2017. ISBN No. 978-93-84443-42-9. [*Major Indexing: Google Scholar, Advanced Science Index, Academia.edu*]