TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

THESIS NO: 070MSCS653

Design and Performance Evaluation of NFC based Mobile Payment System using Lattice Cryptography

by

Anup Devkota

A THESIS

SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SYSTEM AND KNOWLEDGE ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

LALITPUR, NEPAL

APRIL, 2016

Design and Performance Evaluation of NFC based Mobile Payment System using Lattice Cryptography

by

Anup Devkota

070/MSCS/653

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Computer System and Knowledge Engineering

under the supervision of

Prof. Dr. Shashidhar Ram Joshi

Department of Electronics and Computer Engineering

Pulchowk Campus, Institute of Engineering

Tribhuvan University,

Lalitpur, Nepal

April, 2016

COPYRIGHT ©

The author has agreed that the library, Department of Electronics and Computer Engineering, Institute of Engineering Pulchowk campus, may make this thesis freely available for inspection. Moreover the author has agreed that the permission for extensive copying of this thesis work for scholarly purpose may be granted by the professor(s), who supervised the thesis work recorded herein or, in their absence, by the Head of the Department, wherein this thesis was done. It is understood that the recognition will be given to the author of this thesis and to the Department of Electronics and Computer Engineering, Pulchowk campus in any use of the material of this thesis. Copying of publication or other use of this thesis for financial gain without approval of the Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk campus and author's written permission is prohibited.

Request for permission to copy or to make any use of the material in this thesis in whole or part should be addressed to:

Head
Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk campus
Pulchowk, Lalitpur, Nepal

TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

The under signed certify that they have read and recommended to the Department of Electronics and Computer Engineering for acceptance, a thesis entitled "**Design and Performance Evaluation of NFC based Mobile Payment System using Lattice Cryptography"**, submitted by **Anup Devkota** in partial fulfillment to the requirement for the award of the degree of "**Master of Science in Computer System and Knowledge Engineering**".

Defense Date: 25th April, 2016 (13th Baishak, 2073)

Supervisor: Prof. Dr. Shashidhar Ram Joshi
Electronics and Computer Department
Institute of Engineering
Pulchowk campus

External Examiner: Mr. Krishna Prasad Bhandari
Deputy Manager, Nepal Telecom

DEPARTMENTAL ACCEPTANCE

The thesis entitled **“Design and Performance Evaluation of NFC based Mobile Payment System using Lattice Cryptography”,** submitted by **Anup Devkota** in partial fulfillment of the requirement for the award of the degree of “**Master of Science in Computer System an Knowledge Engineering**” has been accepted as a bonafide record of work independently carried out by him in the department.

Dr. Dibakar Raj Pant
Head of the Department
Department of Electronics and Computer Engineering
Pulchowk campus
Tribhuvan University
Nepal

ACKNOWLEDGMENT

I would like to express my deep sense of gratitude to MSCSKE Program Coordinator Dr. Sanjeeb Prasad Panday for granting me permission in carrying my thesis.

I would like to thank Head of Department Dr. Dibakar Raj Pant, Professor Dr. Shashidhar Ram Joshi, Professor Dr. Subarna Shakya, Dr. Aman Shakya, Dr. Arun Timilsina all the faculty members and friends for their kind support and their unequivocal support throughout, as always, for which my mere expression of thanks likewise does not suffice.

This thesis would not have been possible without the help, support and patience of my supervisor, Professor Dr. Shashidhar Ram Joshi, who has helped me in transforming my ideas and guiding properly to achieve my goal. I would like to express my deepest gratitude to him for his excellent guidance, caring, patience, and providing me with an excellent atmosphere for doing research.

Finally, I would like to thank my family, colleagues and friends who were always willing to help and give his best suggestions towards the completion of my thesis.

ABSTRACT

Mobile payment is relatively a new method of payment compared to electronic payment. Smartphones are becoming all in one gadget. Moreover, smartphones with Near Field Communication present an even unique way of making contactless payment with Near Field Communication–Point of Sale. Even though some mobile payment system have been already commercially introduced, they are still far from becoming ubiquitous. The most important issue that arises in any sort of financial transaction is security. The selection of cryptographic tool for mobile payment puts a strict requirement on computational time and security level. The smartphones have relatively less computing power as compared to the PC and also mobile payment should happen in real time, so time constraint most along with the security. The faster key generation and encryption/decryption feature of lattice cryptography compared to other cryptographic tools make it our choice for data security.

In addition to that, the mathematics upon which lattice cryptography is based is entirely different, and no known quantum computing algorithm exists to break it. Along with this strong cryptographic tool we have proposed a security level on top of already secured cellular mobile network for user authorization, authentication, data integrity and non-repudiation, eavesdropping and man in the middle attack.

Keywords: lattice cryptography, Near Field Communication, Security issues

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AuC	Authentication Centre
ASP	Application Service Provider
BTS	Base Transceiver Station
BSC	Base Station Controller
BSI	British Standard Institution
BSS	Base Station Subsystem
CHV	Card Holder Verification
DOS	Denial of Service
ECC	Elliptic Curve Cryptography
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
HLR	Home Location Register
IEC	International Electro technical Commission
LAI	Location Area Identity
IMEI	International Mobile Station Equipment Identity
IMSI	International mobile subscriber identity
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MNO	Mobile Network Operator
MP	Mobile Payment
MSC	Mobile Switching Centre
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	Near Field Communication Interface and Protocol
NIST	National Institute of Standards and Technology
NSS	Network and Switching Subsystem
OMC	Operation and Maintenance Centre
OSS	Operations Support Subsystem

OTA	Over The Air
PIN	Personal Identification Number
POS	Point of Sale
PUK	PIN Unlock Key
RF	Radio Frequency
RFID	Radio Frequency Identification
RTD	Record Type Definition
SIM	Subscriber Identity Module
SMS	Short Message Service
SVP	Shortest vector problem
TNF	Type Name format
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
WCDMA	Wideband Code Division Multiple Access

1. INTRODUCTION

1.1 Background

The very first idea of payment by prepaid cards was envisioned 135 years ago, in 1880 by an American scientist Edward Bellamy. However the transformation of the idea into reality occurred at turtle's pace. Electronic payment system became widely popular only after 1980's. Payment statistics form the last two decades show sharp decline in cash payments and steep increase in electronic payments [1].

Smartphones have replaced watch, camera, audio video player and even means of accessing internet, and day by day the number of internet users that access online content through their smart phones is increasing. Therefore smart phones have evolved into all-in-one gadget all the way from voice call only device, and they are transforming into a convenient payment tool. The mutual ubiquity of smartphones and electronic payments has led to initiatives for mobile payments. Mobile Payment (MP) is a financial transaction which make the use of mobile devices.

The first example of mobile payments came in 1997 when Coca Cola introduced a limited number of vending machines where the customer could make a mobile purchase. The customer would send a text to the vending machine to setup payment and the machine would then vend their product. Later, in 2004, Felica IC was used to provide proximity mobile payments in Japan [2]. Likewise, mobile banking was launched in South Korea, in 2003, by the partnership between LG Telecom and Kookmin bank. Later, in 2007, another Korean mobile operator, SK Telecom, launched new mobile services that enabled subscribers to download credit card and public transportation applications Over The Air (OTA) to a Subscriber Identity Module (SIM) card [2].

The development electronic payment led to the introduction of the concept of digital money. The first digital mobile wallet M-PESA was introduced in 2007, and the first digital currency Bitcoin was introduced in 2009. Mobile payment initiatives use the wireless capabilities of mobile devices (SMS and mobile internet services) to communicate payment information. Furthermore, mobile devices can connect to other mobile devices using Bluetooth, Wi-Fi Direct and Near-field communication (NFC).

The existing wireless payment systems can be classified into three types: account based payment systems, token-based payment systems, mobile POS (point of sale) payment, and mobile wallets payment systems [3].The mobile industry continues to scale rapidly, with a total of 3.6 billion unique mobile subscribers at the end of 2014. Half of the world's population now has a mobile subscription—up from just one in five 10 years ago. An additional one billion subscribers are predicted by 2020, taking the global penetration rate to approximately 60% [4]. These advances in technology mean that the consumers experience is continuing to be even more convenient, faster and efficient.

Nothing could be more convenient than being able to pay for goods and services all from your mobile device from whatever location you need to do so. After this online form of payment, the second most popular form of mobile payment is NFC. NFC is a short-range wireless connectivity technology that evolved from the combination of existing contact less identification and interconnection technologies [5] .With NFC, a low friction and quick transaction can be achieved. Compared to other Radio Frequency (RF) technology, NFC range is much shorter and thus is more secure. After NFC was approved International Organization for Standardization/International Electro technical Commission (ISO/IEC) standard in 2003, adoption of NFC enabled mobile devices has surged because of the vast possibilities for secure and fast services. The phone and reader at a Point of Sale (POS) establish a quick connection via their NFC interfaces when a user waves a phone. User authentication and access to bank information is granted after a successful verification via the mobile network.

NFC is already used as a contactless payment option in many POS locations. On the mobile network side, smartphone will work with current 3G networks and is suitable for 4G networks with added features. The proposed system approach utilizes Lattice Cryptography as a public and private key generating cryptography method.

In the near future MP systems will be as ubiquitous a payment option as smart/credit cards, if not replacing them. With MP services, mobile phones will be larger target for attacks and hacking. An adversary will try many forms of attacks such as eavesdropping, Denial of Service (DoS), modifying and inserting data via air interface, and stealing handset to either retrieve user's sensitive or use it for purchases. Security of MP is a main concern for users as well as service providing companies, and this explains the slow migration to MP [6, 7]. Eventually MP use will go beyond micro payments and it will offer more secure services than currently available payments methods.

1.2 Problem Statement

The mobile payment using NFC is still an undergoing research subject. Even though there are commercially successful payment system, they have their own limitations. In this thesis, we hope to answer the following constraints of mobile payment:

- The encryption mechanism should be fast and efficient for the use in smartphones.
- The encryption mechanism should be secured as per today’s standard and should also be future proof.
- The payment system should not compromise with the security issues associated with the wireless communication.
- The payment system should consider the user authentication and authorization issues in mobile payment.

1.3 Objectives

- To design a mobile payment system architecture based on NFC.
- To implement lattice cryptography as a data encryption method.
- To identify security issues associated with the system.
- To test and evaluate the performance of the system in real world scenario.

2. LITERATURE REVIEW

2.1 NFC

NFC is bidirectional short range radio communication standard used in proximity or as contactless technology. Basic operation of NFC devices is similar to a Radio Frequency Identification (RFID) tag and smart card; devices communicate when brought in close range, less than 10 centimeters or 4 inches. NFC devices operate at 13.56 MHz frequency and a data exchange rate of 106kbps, 212kbps, and 424 kbps with Amplitude Shift Keying modulation [8]. NFC technology has been around for the past 15 years but only in recent years has it become more popular due to standardization by NFC Forum members.

A cellular phone having a NFC device is able to communicate not only with internet via wireless connections but also with smart card readers [9]. NFC technology brings the user experience, convenience and security of contactless technology to the mobile devices, and is enabling quick transactions and services in our day-to-day lives. Around the world many companies are researching on NFC technology and are creating lots of projects focusing on it. There are many ongoing projects using this technology. A common ticket or a coupon are issues of past. Mobile phones can be used as virtual vouchers, transport tickets, or even supermarket loyalty cards [10]. NFC has revolutionized the mobile payments. The major advantage of NFC over other wireless communication technologies is its simplicity: transactions are initialized automatically, simply by touching the reader, another NFC device or an NFC compliant transponder.

NFC was launched as a RF proximity technology in 2004 by the NFC Forum, a non-profit organization with 140 member companies from all over the world involved in the mobile communication, semiconductor, and consumer electronics industries. NFC standards are accepted by ISO/IEC, European Telecommunications Standards Institute (ETSI), and European association for standardizing information and communication systems (ECMA).

The most popular standards Near Field Communication Interface and Protocol (NFCIP-1 and NFCIP-2) are both accepted by ECMA and compatible with (ISO/IES 18092, ETSI TS

102 190) and (ISO/IES 21481, ETSI TS 102 312) respectively [11]. Fast connection speed in less than a tenth of second and close proximity pairing with low friction are the main advantages of NFC over other wireless technology. NFC does not require user intervention and skips multiple steps of establishing connection like Bluetooth or Wi-Fi. Bringing NFC devices within 4 inches triggers data exchange or a tag read via NFC Data Exchange Format (NDEF) [12]. NDEF, Record Type Definition (RTD), and Type Name Format (TNF) are very important issues for the operation of all NFC applications. They show the type of an NFC message, record, and format, respectively [13, 14].

The NFC data exchange format (NDEF) specification defines a data format to exchange information between two NFC enabled devices [13, 14]. NDEF is a lightweight, binary message format that can be used to encapsulate one or more application, defining payloads of arbitrary type and size into a single message construct. Each payload is described by a type, a length, and an optional identifier. Type identifiers may be URIs (uniform resource identifier), MIME (Multipurpose Internet Mail Extensions) media types, or NFC-specific types. Examples of NDEF usage can be experimented when two NFC Forum devices are close each other. An NDEF message is exchanged over the NFC Forum LLCP protocol (Logical Link Control Protocol) [14]. An NDEF message with two attachments is shown in Figure 2.1. When an NFC Forum device is in proximity of an NFC Forum tag, an NDEF message is retrieved from the NFC Forum tag by means of the NFC Forum tag protocols.

<table>
<tr><td colspan="3">NDEF MESSAGE</td></tr>
<tr><td>Email (message/rfc822)</td><td>Pic1.png (image/png)</td><td>Pic2.png (image/png)</td></tr>
</table>

Figure 2.1 Example of NDEF message with two attachments

Record type definition (RTD) is a set of specifications defined by NFC Forum to write NFC tags. “Record type names are used by NDEF applications to identify the semantics and structure of the record content”. NFC Forum suggests the usage of their RTDs and NDEF messages for simplifying NFC Communications [14]. An NDEF Message with Data is shown in Figure 2.2.

<table>
<tr><td colspan="5">NDEF Message</td></tr>
<tr><td colspan="4">Sp(Smart Poster)</td><td>Application/vcard</td></tr>
<tr><td>URI</td><td>Text</td><td>Action</td><td>Configuration</td><td>Vcard data</td></tr>
</table>

Figure 2.2: Example of NDEF message with data

NFC devices could operate in active or passive modes depending on their power source. In active mode, an NFC device has its own power or battery and acts as an initiator sending out RF signals for other NFC devices in close range. A transponder or passive NFC tag replies back once it is powered from signals an initiator sends out. NFC is bidirectional proximity technology, meaning devices can exchange data back and forth.

NFC technology allows three modes of operations: read/write mode, peer-to-peer mode, and card emulation mode. Then, a NFC device can act as a NFC tag emulator or a tag reader [15].

Reader/Writer Mode

In this mode NFC enabled devices can read and write into an NFC passive transponder, much like reading NFC smart posters or NFC tags. In this mode NFC complies with ISO/IEC 14443 A, ISO/IEC 14443 B and the Felica standard. NDEF or NFC Data Exchange Format supports payloads of up to 256 bytes.

Peer-To-Peer Mode

In Peer-To-Peer mode, NFC, sometimes referred to as NFCIP devices, exchange data in both directions, possibly connecting with other wireless devices through Bluetooth via NFC. It also complies with the ISO/IEC 18092 standard.

Card Emulation Mode

In Card Emulation mode an NFC device acts much like smart card, and is used in public transportation and current contactless payments. This mode is usually optional but available if needed, and no specific Tag type is required.

2.2 Asymmetric Cryptography

The setting of public-key cryptography is also called the “asymmetric” setting due to the asymmetry in key information held by the parties. Namely one party has a secret key while another has the public key that matches this secret key. This is in contrast to the symmetry in the private key setting, where both parties had the same key. Asymmetric encryption is thus another name for public-key encryption, the mechanism for achieving data privacy in the public key or asymmetric setting.

2.2.1 RSA Algorithm

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973 by Clifford Cocks but this was a secret until 1997. The patent taken out by RSA Labs has expired.

The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key [16].

Algortihm:

1. Generate two large random primes, p and q, of approximately equal size such that their product $n = pq$ is of the required bit length, e.g. 1024 bits.
2. Compute $n = pq$ and (phi) $\varphi = (p-1)(q-1)$.
3. Choose an integer e, $1 < e < phi$, such that $gcd(e, phi) = 1$.
4. Find d, such that $de \% m = 1$. Where $d = (1 + m * i)/e$
5. Publish e and n as the Public Key

6. Keep d and n as the Private Key

2.2.1 Elliptic Curve Cryptography

Elliptic curves are polynomials that define points based on the equation:

$$y^2 = x^3 + ax + b \qquad (2.1)$$

for parameters *a*, *b* that specify the exact shape of the curve.

On the real numbers and with parameters *a, b, R* an elliptic curve looks like:

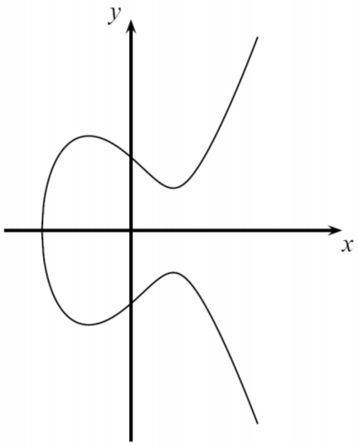


Figure 2.3: Elliptic Curve example

Elliptic curves can't just be defined over the real numbers *R* but over many other types of finite fields. In cryptography, we are interested in elliptic curves module a prime *p*:

Definition: Elliptic Curves over prime fields

The elliptic curve over Z_p , $p>3$ is the set of all pairs $(x,y) \in Z_p$ which fulfill

$$y^2 = x^3 + ax + b \bmod p \qquad (2.2)$$

where $a,b \in Z_p$ and the condition

$$4a^3 + 27b^2 \neq 0 \bmod p \qquad (2.3)$$

Note that Z_p = *{0,1,…, p -1}* is a set of integers with modulo p arithmetic [17]

Computations on Elliptic Curves

The equation of an elliptic curve is given as:

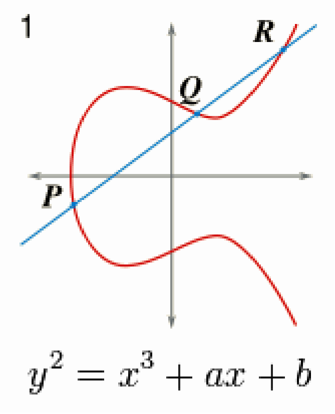


Figure 2.4: Elliptic curve computation example

Few terms that will be used are:

E : Elliptic Curve

P : Point on the curve

n : Maximum limit (This should be a prime number)

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key [18].

Now, we have to select a number *d* within the range of *n*

Using the following equation we can generate the public key

$$Q = d * P \tag{2.4}$$

d : the random number that we have selected within the range of *(*1 to *n*-1*)*

P : is the point on the curve

Q : is the public key and d is the private key

Encryption

Let *m* be the message that we are sending. We have to represent this message on the curve using padding scheme. Consider *m* has the point *M* on the curve *E.* Randomly select *k* from [1 – (*n*-1)].

Two cipher texts will be generated let it be C_1 and C_2 [18].

$$\mathrm{C}_1 = \mathrm{k*P} \tag{2.5}$$

$$\mathrm{C}_2 = \mathrm{M + k*Q} \tag{2.6}$$

C_1 and C_2 both will be send.

Decryption

We have to get back the message m that was send to us [18]

$$\mathrm{M = C_2 – d * C_1} \tag{2.7}$$

M is the original message that we have send.

Proof

From equation (2.7)

$$\mathrm{M = C_2 – d * C_1}$$

From equation (2.5) and (2.6)

$$C_2 – d * C_1 = (M + k * Q) – d * (k * P)$$

$$= M + k * d * P – d * k *P$$

$$= M \ (\text{Original Message})$$

2.3 Lattice Cryptography

Lattice-based cryptography is the generic term for asymmetric cryptographic primitives based on lattices. Unlike more widely used and known public key cryptography such as the RSA or Diffie-Hellman cryptosystems, Lattice-based cryptographic constructions hold a great promise for post-quantum cryptography, as they enjoy very strong security proofs based on worst-case hardness, relatively efficient implementations, as well as great simplicity. In addition, lattice-based cryptography is believed to be secure against quantum computers [19].

A lattice is a set of points in n-dimensional space with a periodic structure, such as the one illustrated in Figure 2.5.

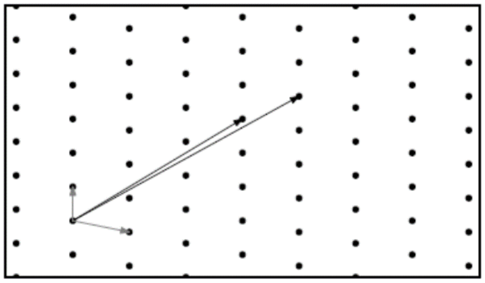


Figure 2.5: A two-dimensional lattice and two possible bases [19]

More formally, given n-linearly independent vectors $b_1, . . . , b_n \in R^n$, the lattice generated by them is the set of vectors

$$L(b_1, . . . , b_n) = \sum_{i=1}^{n} x_i b_i \quad ; x \in Z \qquad (2.8)$$

The vectors $b_1, \ldots, b_n$ are known as a basis of the lattice. Lattice-based cryptographic constructions are based on the presumed hardness of lattice problems, the most basic of which is the shortest vector problem (SVP).Given an input lattice represented by an arbitrary basis, and our goal is to output the shortest nonzero vector in it. In fact, one typically considers the approximation variant of SVP where the goal is to output a lattice vector whose length is at most some approximation factor γ(n) times the length of the shortest nonzero vector, where n is the dimension of the lattice [19].

The most well-known and widely studied algorithm for lattice problems is the LLL algorithm, developed in 1982 by Lenstra, Lenstra, and Lov´asz [20]. This is a polynomial time algorithm for SVP (and for most other basic lattice problems) that achieves an approximation factor of $2^{O(n)}$ where n is the dimension of the lattice. As bad as this might seem, the LLL algorithm is surprisingly useful, with applications ranging from factoring polynomials over the rational numbers, to integer programming, as well as many applications in cryptanalysis (such as attacks on knapsack-based cryptosystems and special cases of RSA) [20].

Lattice-based cryptography has some interesting properties when compared to conventional cryptosystems. Firstly, the trapdoor function upon which it is based is proven to be hard, whereas the other cryptosystems' trapdoors are assumed to be. Secondly, it is known that quantum computers can be used to break conventional cryptosystems, but this is not known for lattice-based cryptosystems. Thirdly, lattice systems have been used to enable fully homomorphic cryptosystems [21], which has potential as a basis for fundamentally different and divisible payment systems.

2.3.1 The LLL algorithm

Lattice reduction in dimensions higher than two is much more difficult. One of the most successful algorithms was invented by A. Lenstra, H. Lenstra, and L. Lovasz and is called the LLL algorithm. In many problems, a short vector is needed, and it is not necessary that the vector be the shortest. The LLL algorithm takes this approach and looks for short vectors that are almost as short as possible [22]. This modified approach makes the algorithm run very quickly (in what is known as polynomial time). The algorithm performs calculations similar to those in the two-dimensional case.

Theorem: Let *L* be the n-dimensional lattice generated by $v_1 \ldots\ldots\ldots\ldots\ldots v_n$ in $\boldsymbol{R^n}$. Define the determinant of lattice to be

$$D = \left|det(v_1 \ldots\ldots\ldots v_{n)}\right| \qquad (2.9)$$

Let λ be the length of a shortest nonzero vector in *L*. The LLL algorithm produces a basis $\{b_1 \ldots\ldots\ldots\ldots b_n\}$ of *L* satisfying

1. $\|b_1\| \leq 2^{(n-1)/4} D^{1/n}$

2. $\|b_1\| \leq 2^{(n-1)/2}$ λ

3. $\|b_1\| \|b_2\| \ldots\ldots.. \|b_n\| \leq 2^{n(n-1)/4} D$

Statement (2) says that b_1 is close to being a shortest vector, at least when the dimension n is small. Statement (3) say that the new basis vectors are in some sense close to being orthogonal.

More precisely, if the vectors $b_1 \ldots\ldots\ldots\ldots b_n$ are orthogonal, then the volume *D* equals the product $\|b_1\| \|b_2\| \ldots\ldots.. \|b_n\|$ .The fact that this product is no more than $2^{(n-1)/4}$ times *D* says that the vectors are mostly close to orthogonal.

The running time of the LLL algorithm is less than a constant times $n^6 \log^3$ B, where n is the dimension and B is a bound on the lengths of the original basis vectors. In practice it is much faster than this bound. This estimate shows that the running time is quite good with respect to the size of the vectors, but potentially not efficient when the dimension gets large.

2.3.2 NTRU

If the dimension n is large, say n > 100, the LLL algorithm is not effective in finding short vectors. This allows lattices to be used in cryptographic constructions. Several cryptosystems based on lattices have been proposed. One of the most successful current systems is NTRU [22].

First, we need some preliminaries. Choose an integer *N*. We will work with the set of polynomials of degree less than *N*.

Let

$$f = a_{N-1}X^{N-1} + \cdots + a_0 \qquad (2.10)$$

and

$$g = b_{N-1}X^{N-1} + \cdots + b_0 \qquad (2.11)$$

be two such polynomials.

Define

$$h = f * g = c_{N-1}X^{N-1} + \cdots + c_0 \qquad (2.12)$$

where

$$c_i = \sum_{j+k=i} a_j \, b_k$$

The summation is over all pairs *j, k* with *j* + *k* = *i* (mod *N*).

NTRU works with certain sets of polynomials with small coefficients, so it is convenient to have a notation for them. Let

L(j,k) = the set of polynomials of degree < *N*

= with *j* coefficients equal to +1

= and *k* coefficients equal to —1

The remaining coefficients are 0.

We can now describe the NTRU algorithm. Alice wants to send a message to Bob, so Bob needs to set up his public key. He chooses three integers *N, p, q* with the requirements that gcd (*p, q*) = 1 and that *p* is much smaller than *q*. Recommended choices are

$$(N, p, q) = (107, 3, 64)$$

For moderate security and

$$(N, p, q) = (503, 3,256)$$

for very high security. Of course, these parameters will need to be adjusted as attacks improve. Bob then chooses two secret polynomials f and g with small coefficients. Moreover, f should be invertible mod p and mod q, which means that there exist polynomials F_p and F_q of degree less than N such that

$$F_p * f \equiv 1 \quad (mod\ p)$$

$$F_q * f \equiv 1 \quad (mod\ p)$$

Bob calculates:

$$h \equiv F_q * g \quad (mod\ q) \tag{2.13}$$

Bob‘s public key is:

$$(N, p, q, h)$$

His private key is *f*. Although F_p can be calculated easily from *f*, he should store (secretly) F_p since he will need it in the decryption process.

Since

$$g \ \equiv f * h \ \ (mod\ q) \tag{2.14}$$

Alice can now send her message. She represents the message, by some prearranged procedure, as a polynomial *m* of degree less than N with coefficients of absolute value at most (p — l)/2. When p = 3, this means that m has coefficients -1, 0, 1. Alice then chooses a small polynomial γ and computes

$$c \equiv p\gamma * h + m \quad (mod\ q) \tag{2.15}$$

She sends the ciphertext c to Bob. Bob decrypts by first computing

$$a \equiv f * c \quad (mod\ q) \tag{2.16}$$

with all coefficients of the polynomial a of absolute value at most q/2, then recovering the message as

$$m \equiv F_p * a \quad (mod\ p) \tag{2.17}$$

2.4 Mobile Technology

The idea of today’s cellular mobile network dates back to post Second World War era when an engineer William Rae Young (Bell Labs engineer that was part of AT&T), made the proposal of setting up radio towers in a hexagonal pattern to support a network of phones [23]. Several developments continued, but the real breakthrough in the cellular mobile network technology was in 1973 When Dr. Martin Cooper placed the world’s first cell phone call to Dr. Joel Engel on April 3rd, 1973, the technology used by the device became known as a 1G or first generation mobile phone.

This first cell phone weighed approximately two pounds and was named the Motorola Dyna-Tac._This technology would later be called as 1G (First generation cellular mobile network).

The first generation cellular mobile network was analog. The following advancement was digital cellular mobile network, which is called GSM and has been categorized as 2G. GSM was followed by UMTS which is categorized as 3G. UMTS is being followed by 4G cellular mobile technology LTE.

2.4.1 Mobile Network Architecture

Mobile Network Architecture gives holistic picture of entire cellular mobile communication, how the call originates, how does it process, how the call switching occurs, authentication and authorization of the user and overall security of the network.

GSM Architecture

GSM architecture can be divided into three broad functional areas: the Base Station Subsystem (BSS), the Network and Switching Subsystems (NSS), and the Operations Support Subsystem (OSS). Each of the subsystems is comprised of functional entities that communicate through various interfaces using specified protocols.

The BSS is comprised of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BSS provides transmission paths between the Mobile Stations (MSs) and the NSS, and manages the transmission paths. The NSS is the brain of the entire GSM network and is comprised of the Mobile Switching Center (MSC) and four intelligent network nodes known as the Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AuC). The OSS consists of Operation and Maintenance Centers (OMCs) that are used for remote and centralized operation, administration, and maintenance (OAM) tasks. The OSS provides means for a service provider to control and manage the network [24].

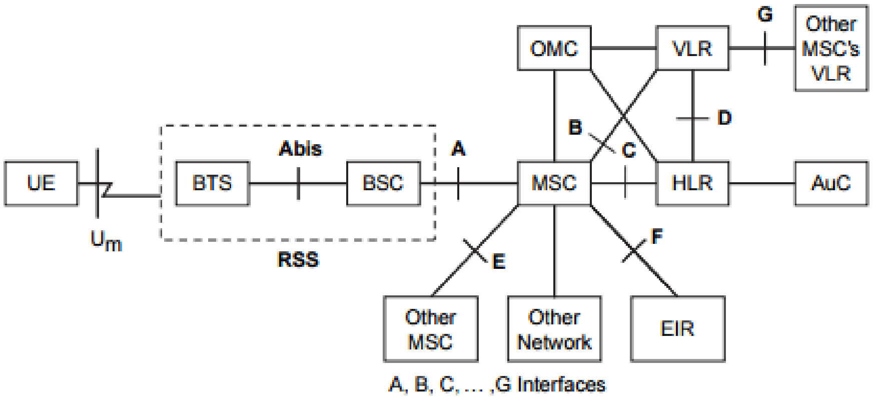


Figure 2.6: GSM Architecture [25]

Subscriber Identity Module (SIM)

SIM cards are like credit cards and identify the user to the GSM network. They can be used with any GSM handset to provide phone access, ensure delivery of appropriate services to that user, and automatically bill the subscriber's network usage back to the home network.

As previously stated, GSM distinguishes between the subscriber and the MS. The SIM determines the subscriber's cellular number, thus permitting the subscriber to use other equipment (change MS) while maintaining one number and one bill. The SIM is a chip that is embedded in a card approximately the size of a credit card, or around a quarter of the size (the former tends to be outdated).

The SIM is the component that communicates directly with the VLR and indirectly with the HLR. These two critical networks components are described as [26].

Base Transceiver Station (BTS)

The base transceiver stations provide the connectively between the cellular network and the MS via the Air interface. The BTS houses the radio transceivers that define a cell and handles the radio interface protocols with the mobile station.

Base Station Controller (BSC)

A number of BTSs are connected to the BSC on an interface that is known as the Abis interface. It manages the radio interface channels, such as setup, release, frequency hopping, and handovers.

Mobile Switching Centre (MSC)

The MSC is the network subsystem's central component. Because a large number of BSCs are connected to an MSC, an MSC is effectively a regular ISDN switch that connects to the BSCs via the A-interface. The MSC provides routing of incoming and outgoing calls and assigns user channels on the A-interface.

It acts like a normal switching node of the PSTN or ISDN and provides all the necessary functionality for handling a mobile station, including registration, authentication, location updating, inter-MSC handovers, and call routing to a roaming subscriber.

The MSC also provides the connection to the public fixed networks. Together with the MSC, the HLR and VLR provide GSM call routing and roaming capabilities.

Home Location Register (HLR)

The HLR can be regarded as a huge database that contains the information for hundreds of thousands of subscribers. Every PLMN has at least one HLR. While there is logically one HLR per GSM network, it might be implemented as a distributed database.

The HLR contains all administrative data that is related to each subscriber, who is registered in the corresponding GSM network, along with his current location. The location of each mobile station that belongs to the HLR is stored in order to be able to route calls to the mobile subscribers served by that HLR. The location information is simply the VLR address that currently serves the subscriber. An HLR does not have direct control of MSCs.

Two numbers that are attached to each mobile subscription and stored in the HLR include the IMSI and the MSISDN. The HLR also stores additional information, including the location information (VLR), supplementary services, basic service subscription information, and service restrictions (such as roaming permission). GSM 03.08 details the subscriber data's organization.

Visitor Location Register (VLR)

Like the HLR, the VLR contains subscriber data. However, it only contains a subset (selected administrative information) of the data that is necessary for call control and provision of the subscribed services for each mobile that is currently located in the geographical area controlled by the VLR. The VLR data is only temporarily stored while the subscriber is in the area that is served by a particular VLR. A VLR is responsible for one or several MSC areas. When a subscriber roams into a new MSC area, a location updating procedure is applied. When the subscriber roams out of the area that is served by the VLR, the HLR requests that it remove the subscriber-related data.

Although the VLR can be implemented as an independent unit, to date, all manufacturers of switching equipment implement the VLR with the MSC so the geographical area controlled by the MSC corresponds to that which is controlled by the VLR. The proximity of the VLR information to the MSC speeds up access to information that the MSC requires during a call.

Equipment Identity Register (EIR)

The EIR is a database that contains a list of all valid mobile equipment on the network. Each MS is identified by its IMEI. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

The EIR contains a list of stolen MSs. Because the subscriber identity can simply be changed by inserting a new SIM, the theft of GSM MSs is attractive. The EIR allows a call bar to be placed on stolen MSs. This is possible because each MS has a unique IMEI.

Authentication Center (AuC)

The AuC is a protected database that stores a copy of the secret key that is stored in the subscriber's SIM card and is used for authentication and ciphering on the radio channel.

3G - UMTS Architecture

To understand the threats to a network, one must understand the network infrastructure. UMTS is considered the most important 3G proposal. It is being developed as an evolution of GSM and therefore based on the GPRS network which is a 2.5G technology and the UTRA radio interface [27].

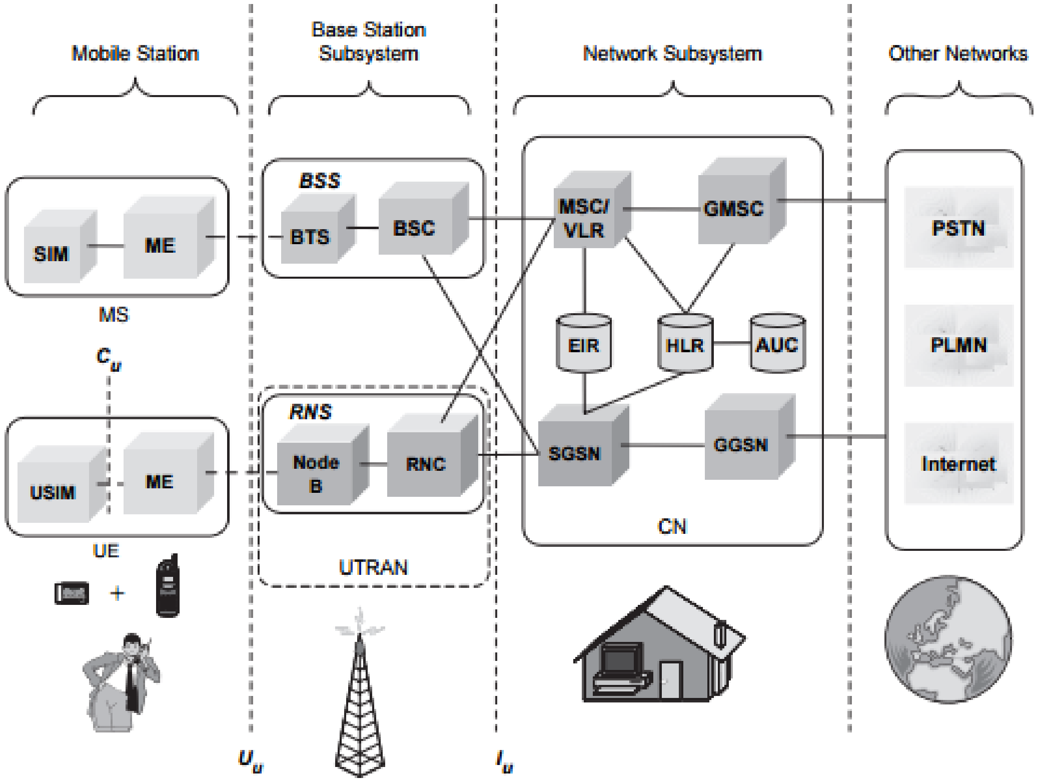


Figure 2.7: 3G-UMTS Architecture [25]

As can be seen in Figure above, the 3G network has two main parts

1. The Radio Access Network (RAN)
2. The Core Network (CN)

The RAN consists of the existing GPRS/GSM RAN system which is connected to the Packet Switched Network (PS-CN) and also to the circuit switched network (CS-CN). The PS-CN will eventually connect to the UTRAN system as part of the full transition to 3G. The UTRAN consists of subsystems, with each subsystem consisting of one Radio Network Controller (RNC) which is connected to several Base Transceiver Stations (BTS). The GRPS RAN has a similar architecture.

The Core Network consists of the PS-CN and the CS-CN. The PS-CN consists of several information servers, the SGSN and the GGSN. Each SGSN connects one or more RSC and BSC with the PS-CN. Its functionality includes access control, mobility management, paging and route management. The GGSN is the logical gateway to the Internet. The BG interface can be used to connect to another PS-CN or to another carrier. The information servers provide several functions. The Home Location Register (HLR) maintains subscriber information and the Authentication Center (AuC) maintains authentication information. There are also IP based servers such as DNS, DHCP and RADIUS servers which interact with the SGSN/GGSN and provide control and management functions.

2.4.2 Mobile Network Security Architecture

SIM Card

Subscriber Identity Module Card is a piece of smart card similar to a mini-computer with its own operating system, storage, some RAM, and built-in security features. When configured with up-to-date cryptography: it’s able to make DES calculations, as recommended by NIST, BSI, ANSSI, etc., SIM cards provide a level of security that is state-of-the-art. The SIM card can add, delete and manipulate information within its memory, on top of sending and receiving data. A regular SIM measures 15 millimeters x 25 mm and a newer, smaller version of the SIM, called the micro SIM or 3FF SIM card is 12mm x 15mm. As the identity module, SIM card takes excellent physical protection and stores sensitive personal info including PIN (Personal Identification Number), PUK (PIN Unlock Key), and IMSI (International Mobile Subscriber Identity). If PIN protection is enabled, the PIN will need to be entered each time phone is switched on. If the PIN is entered incorrectly 3 times in a row, the SIM card will be blocked requiring a PUK from the network/service provider. If PUK is entered 10 times incorrectly, the SIM card is permanently disabled and must be exchanged.

With the evolution of WCDMA/3G network, a new type of SIM, USIM (Universal Subscriber Identity Module), has been developed. New algorithm has been introduced in USIM to prevent unauthorized access to the phone and to encrypt voice and internet traffic with stronger encryption keys.

The SIM provides storage of three types of subscriber related:

- Data attached during the administrative phase; e.g. IMSI, subscriber authentication key and access control class.
- Temporary network data; e.g. TMSI, LAI, Kc
- Other service related data; e.g. Language preferences, advice of charge, telephone numbers etc.

The SIM also contains some pre-installed keys and algorithms provided by the operator:

- Subscriber authentication key (Ki)
- Authentication algorithm (A3)
- Cipher key generation algorithm (A8)
- Personal Identification number (PIN)

Subscriber authentication key (Ki)

Ki is a 128 bit key used for authentication of the subscriber by the operator. The safety of GSM depends on the secrecy of this key. If Ki is compromised it is possible to clone the SIM-card. Therefore it is only stored two places: On the tamper resistant SIM-card and in the secure AuC. To keep it secret Ki is never transferred directly over the air interface. It is only used in combination with other keys and input parameters. Since no one else in the GSM network knows this key, AuC is the only one who is able to compute the triplet needed in the authentication of the subscriber [27, 28].

Authentication algorithm (A3)

A3 is a one-way function and is located in the SIM card and in the AuC. It is used in the challenge-response mechanism of the SIM authentication.

Cipher key generation algorithm (A8)

The A8 algorithm is also a one-way function using the same mechanism as A3, to establish a cipher key Kc for encrypting user and signaling data on the radio path. It generates a 64 bit session key (Kc) from the 128 bit RAND and 128 bit Ki.

Personal Identification number (PIN)

The PIN or Card Holder Verification (CHV) is a 4 to 8 digit code used to authenticate the subscriber against the SIM card. The PIN is provided by the operator and is stored on the SIM card.

Subscriber-SIM authentication

The subscriber is first met by a simple one-token authentication mechanism. A 4 to 8 digit Card Holder Verification (CHV), also known as Personal Identification Number (PIN). The PIN is stored on the SIM-card and is usually shipped to the subscriber independent of the SIM-card. Such a mechanism is useless in a radio environment, since listening once to this PIN is enough to break the protection. But this mechanism is only used at the client side and thus it is never transmitted via the radio path. By authenticating the user to the SIM, the system provides a simple but effective protection against the use of stolen cards. The user is allowed to change the PIN or even remove the protection. If a wrong PIN is typed more than 3 times, the SIM card will be locked until an 8 digit Unblock CHV / Personal Unblocking Key (PUK) is entered. If the PUK is entered wrong 10 times, the SIM will be permanently blocked and completely unrecoverable.

Depending on the requirements of the SIM issuer, and subject to the features incorporated in the SIM, a second CHV (PIN2) may be provided. Like PIN, the PIN2 shall consist of 4 to 8 digits. There shall be no provision for the subscriber to disable PIN2. Another requirement according to the specifications is that it shall not be possible to read the PIN or PUK [28] .When the user is authenticated against the SIM, the SIM must authenticate against the GSM network before the subscriber is allowed to use the GSM services.

3G / UMTS security architecture

Secure communication between an MS and a BS in 3G mobile networks is reached via an Authentication and Key Agreement Protocol (AKA), which provides a much more secure communication channel than 2G networks where authentication is required only for an MS.

3. METHODOLOGY

3.1 Proposed Model

We have considered an example scenario of POS checkout point at a store. A simple payment system would require at least three parties MS, POS and bank to settle the payment. In addition to that, we have proposed the authentication and authorization of the user via MNO. The MNO servers (HLR, VLR, EIR and AuC) along with the Payment Service provider's server check whether the user is authorized to subscribe the payment service, and whether the user is genuine and not the imposter. For this the user is bind with the unique SSN, IMSI and IMEI, and also he has to input the PIN at the time of the transaction whose hashed value is checked against the hashed value at the Service provider database. For protection against data tampering the transaction message is transmitted along with its digital signature thus ensuring against data modification and non-repudiation. The Certification Authority checks for the authenticity of the merchant.

The figure 3.1 shows architecture of the Payment system. During a checkout process, a user waives his/her phone over NFC reader at POS and clicks on Mobile Payment icon. During a quick wave, contact is established between a phone and reader at a POS and message exchange takes place. The MS sends request to the reader at the store and to the MNO server. The reader at the POS replies back with its public key. The MS then uses this key to encrypt the financial transaction message. This encrypted message is then decrypted by the POS by using its private key. Similar sort of communication happen between MS and MNO servers. The MNO servers also facilitates the authentication and authorization of the users. Finally when two identical transaction arrive at the Payment gateway, payment process is terminated with necessary updates and signing of the payment voucher by the buyer for protection against future non-repudiation case.

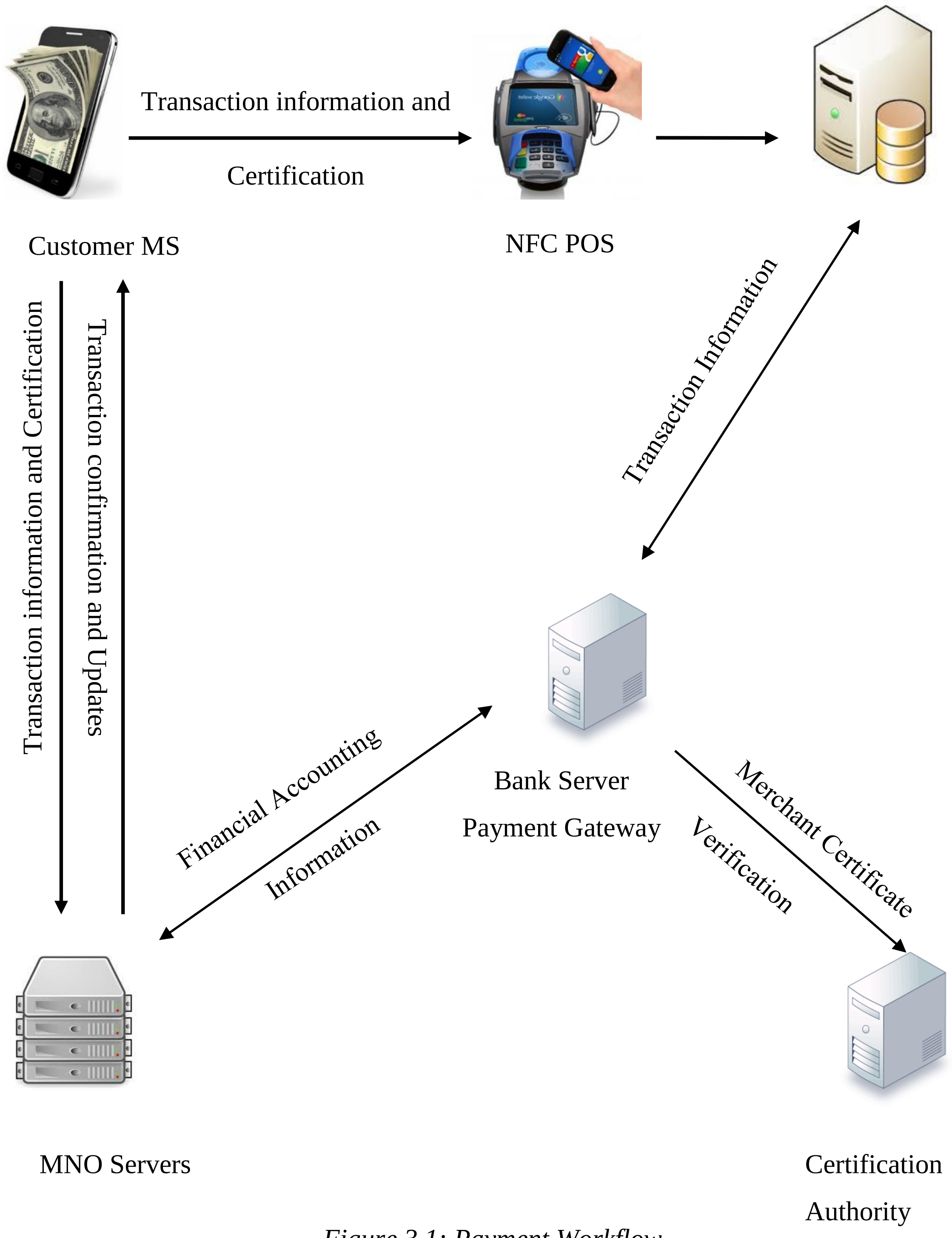


Figure 3.1: Payment Workflow

The payment system consists of the following components: NFC enabled user handset or cell phone, NFC reader enabled POS, back end database at the merchant, Mobile Network Operator (MNO), Bank Server or Payment Gateway (PG), and Certification Authority.

NFC creators advise the usage of a secure element to turn payment and ticketing applications more secure. A secure element is used to store confidential and sensitive information like a credit card pin. At this moment, there are only three places that can be used as secure element: the subscriber identity module (SIM) card, the external memory card, or a phone’s embedded NFC chip.

User registers to the service using his mobile number which will be his/her user id and SIM serial number which is printed in the SIM.

3.2 System Workflow

Step 1

During payment process, user needs to input the SIM PIN to secure the mobile device from unauthorized access. The payment application in the mobile then send request to the NFC POS

Step 2

NFC POS responds with its merchant Identification number Mid and its public key PkNFC

Step 3

The MS sends its User Identification Uid, Total Amount TA, Time stamp TS and Bank Account Information BAI and secured hashed PIN encrypted with PKNFC to the NFC POS ; <Uid, TS, TA, BAI, H(PIN)>PKNFC

Step 4

NFC POS then decrypts the message with its private key and sends the transaction information to the bank server; <Mid, Uid, TS, TA, BAI, H(PIN)>

Step 5

In the meantime, MS sends request to the MNO server via OTA (Over The Air)

Step 6

The MNO server responds with its public key PKMNO

Step 7

The MS then sends Merchant id Mid, User Id Uid, International Mobile Subscriber Identity IMSI, SIM Serial Number SSN, International Mobile Equipment Identity IMEI, Total Amount TA, Bank Account Information BAI and Time Stamp TS encrypted with public key of MNO <Mid,Uid,IMSI,SSN,IMEI,TA,BAI,TS>PKMNO

Step 8

MNO then decrypts the message with its private key and sends the transaction information to the bank server; <Mid Uid, TS, TA, BAI>

Step 9

If a purchase request is valid, the bank should receive two identical requests, one from an MNO and another from a NFC POS, and upon verification of customer authentication by PIN and sufficiency of available funds, the bank settles the financial transaction.

Step10

The payment process finishes with the account update information and delivery of e-receipt to the user.

The payment sequence described above is illustrated diagrammatically below.

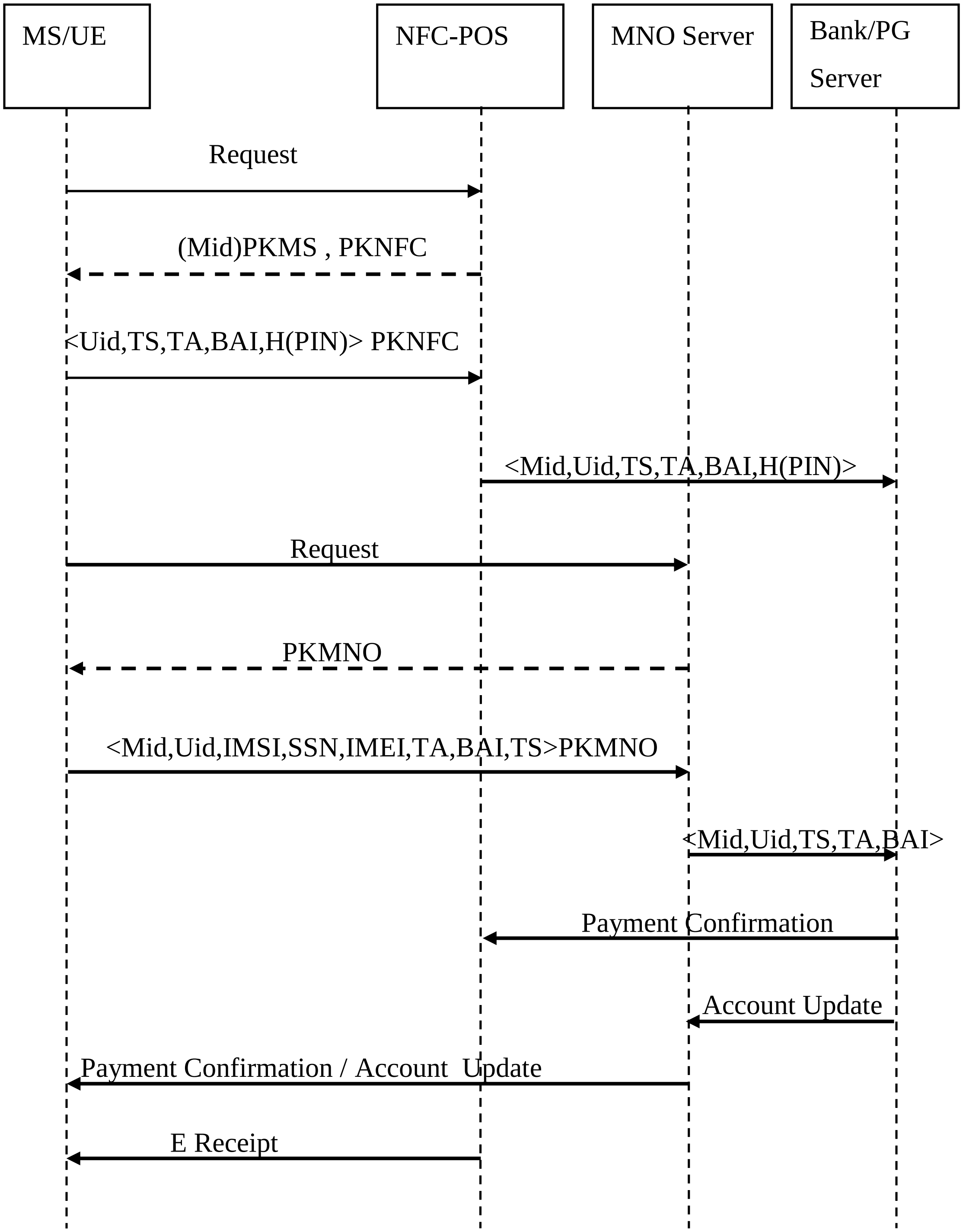


Figure 3.2: Payment Sequence Diagram

3.3 System Security Architecture

Our mobile payment system has two wireless interfaces where the data transfer occur: interface between MS and NFC-POS and interface between MS and MNO servers. These two wireless interfaces have their own constraints and are the most vulnerable for data security. For this reason we have designed different security feature for these two interfaces in our mobile payment model.

Interface between MS and MNO servers

SIM is our primary secure element. It is the basic mean of authorization. The payment application running in the smartphone will be SIM PIN locked. PIN is usually 4 to 6 digit long and is known only to the user. Wrong entry of PIN for 3 times will lead to SIM lock. Once SIM is locked PUK will be required to unlock the SIM. PUK is 8 digits long. Subsequent entry of wrong PUK for 10 times will result in permanent damage of the SIM. So without the authorized user, one cannot even enter into the payment application. The User registers the service with ASP (Application Service Provider) using SSN. The SSN thus will be known only to the user and ASP.

Cellular mobile network has built-in security features for the authentication of the user. 3G-UMTS network is much more secure because authentication happens between MS and MNO on both sides as compared to 2G networks where authentication is required only for an MS.

As financial transaction is very sensitive matter and requires outmost security, we have proposed new security layer on top of the secured 3G-UMTS network. Using OTA technology, we implement cryptographic feature to encrypt and digitally sign the financial transaction along with the information like IMSI, IMEI and SSN and TS which will later be verified with the MNO servers, so that on top of the built in authentication requirement in cellular mobile network, a more secured user authentication can be performed.

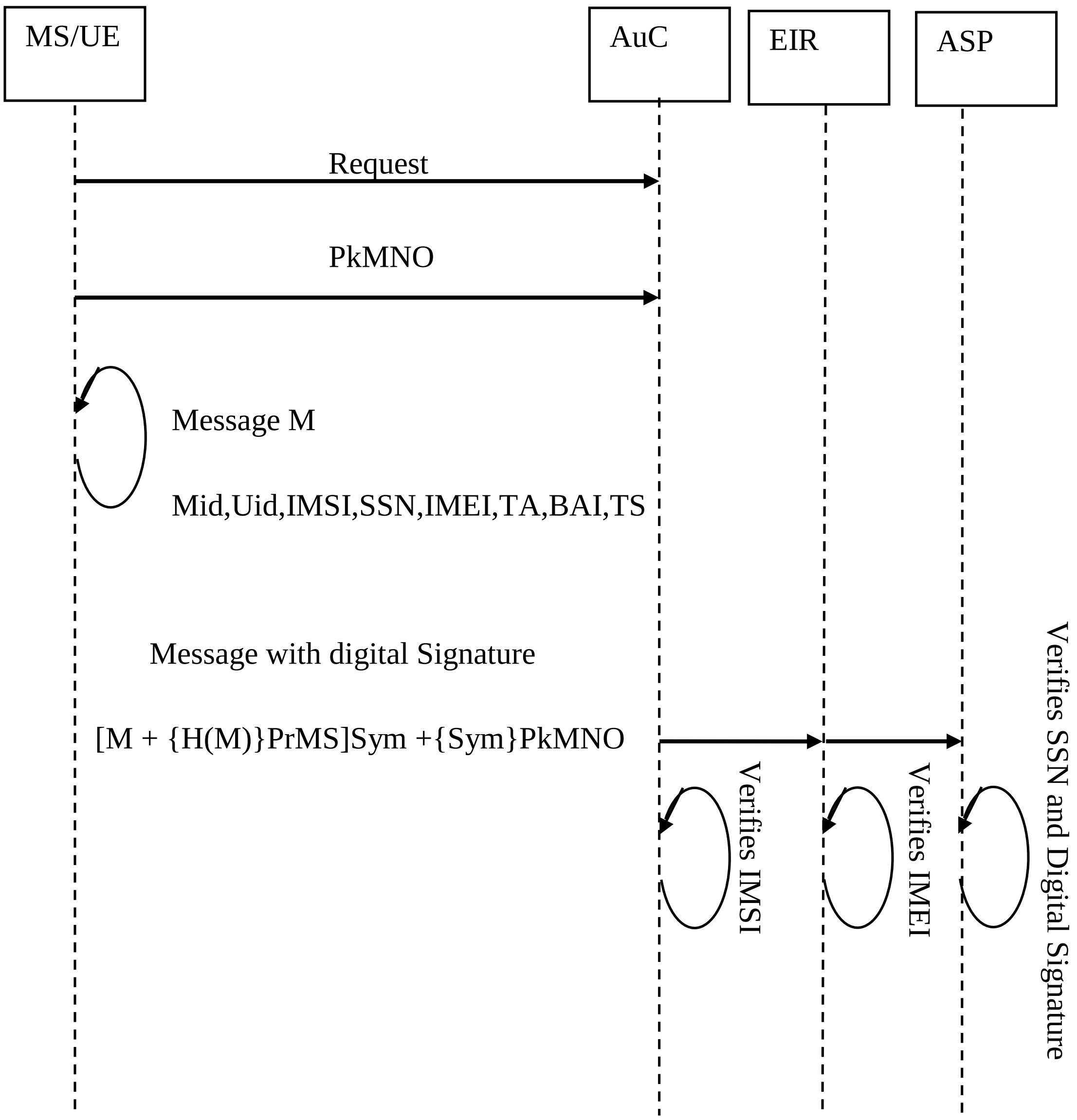

MS/UE
AuC
EIR
ASP
Request
PkMNO
Message M
Mid,Uid,IMSI,SSN,IMEI,TA,BAI,TS
Message with digital Signature
[M + {H(M)}PrMS]Sym +{Sym}PkMNO
Verifies IMSI
Verifies IMEI
Verifies SSN and Digital Signature

Figure 3.3: MS-MNO Security level

Interface between MS and NFC-POS

NFC devices communicate with each other via RF waves and an adversary equipped with radio scanner could eavesdrop. In general communication range of NFC devices is within close proximity or less than 4 inches. But there is not a set distance on how close an attacker needs to be in order to intercept a radio signal [30, 31]. A successful attack requires a good quality signal receiver and decoder, an antenna that changes directions in 3 dimensions, and an environment with less distractions and barriers such as noise, metal and wall. The geometry of the antenna and power level of sender could also influence the success of an attack. Another non-negligible factor is the operating mode of the sender device, in an active mode the sender creates its own RF field and in passive mode it uses the other device's RF field.

An active mode is intended to seek for passive devices within close proximity and therefore in this mode eavesdropping is possible up to a distance of about 10 meters. On the contrary, a device in passive mode waits silently until active device power. Thus, the possible eavesdropping distance is 1 meter. Eavesdropping could be prevented using a secure communication channel.

And we have proposed lattice cryptography to realize this secured channel because of its hardness to break and also faster computational time.

4. RESULTS AND DISCUSSION

4.1 Benchmark

The backbone of our mobile payment system is data encryption using lattice cryptography. To realize lattice cryptography we have implemented NTRU algorithm. NTRU is a patented and open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data and has been made available under the Gnu Public License (GPL) v2 or higher.

To address the research question concerning the performance of NTRU against RSA and ECC we implemented set of benchmarks: key generation, encryption and decryption time to run on both mobile device (android) and PC (windows) for comparison against cryptographic systems.

For both PC and smartphone version the performance was calculated for key generation time, encryption time and decryption time for respective key size and security level as shown below.

Smartphone : Samsung galaxy S5(Qualcomm MSM8974 processor, 4 cores, Clock Speed 300Mhz-2.46Ghz and 2GB RAM)

PC: Lenovo ThinkPad E520 (Intel core i5 2410M processor, 2 cores, Clock Speed 2.3 to 2.9 GHz and 6 GB RAM)

Message size: 50 bytes

Programming Platform: Java for PC and android for smartphone

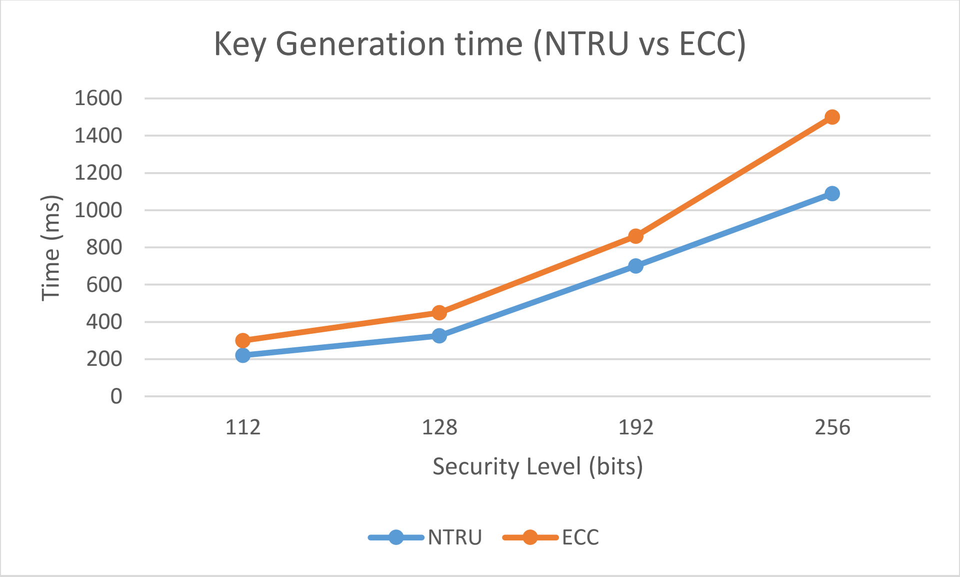


Figure 4.1: Key Generation time (NTRU vs ECC) in smartphone

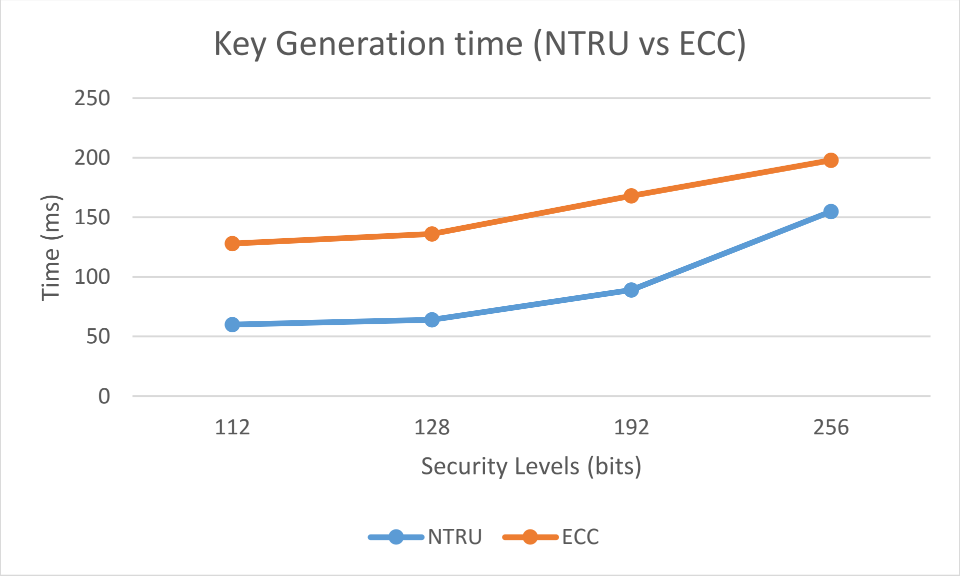


Figure 4.2: Key Generation time (NTRU vs ECC) in PC

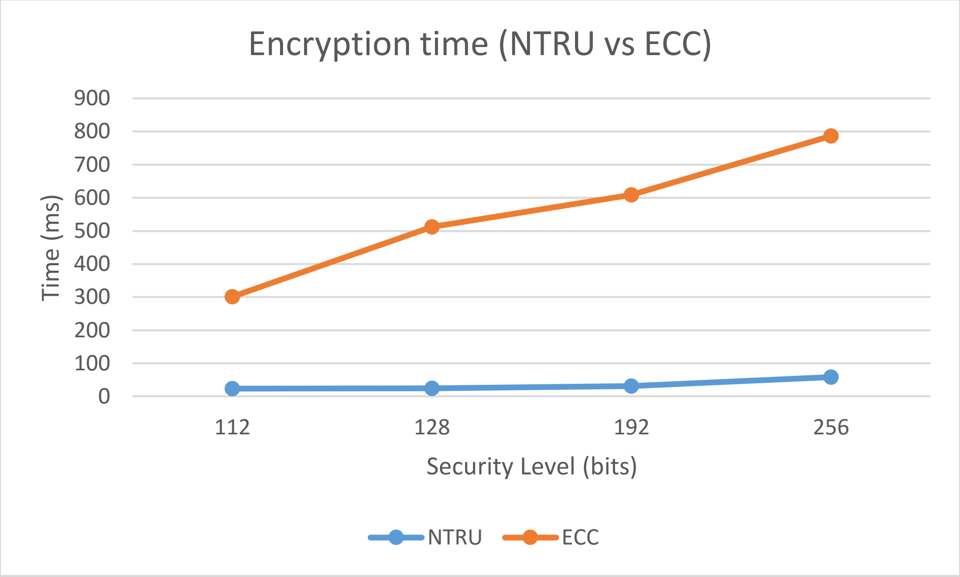


Figure 4.3: Encryption time (NTRU vs ECC) in smartphone

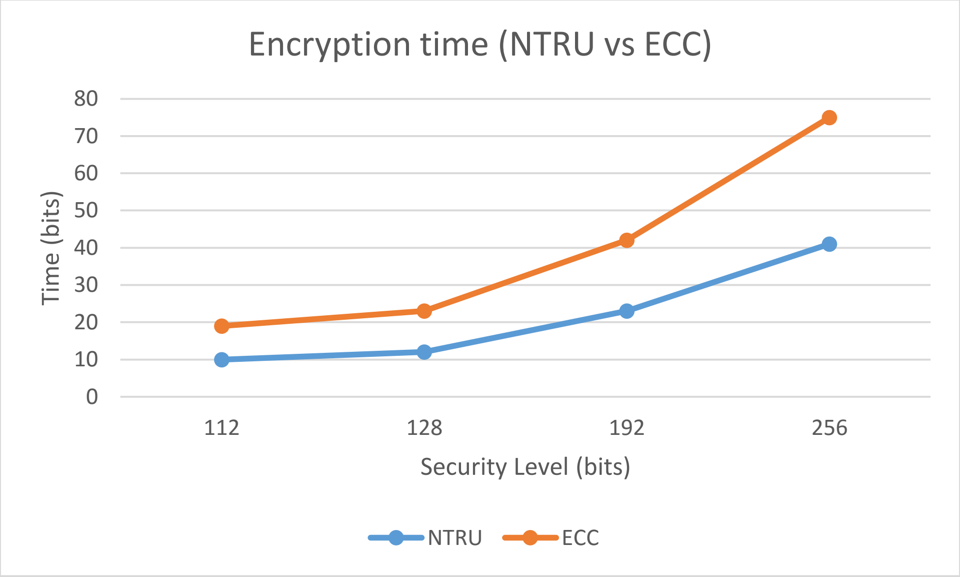


Figure 4.0: Encryption time (NTRU vs ECC) in PC

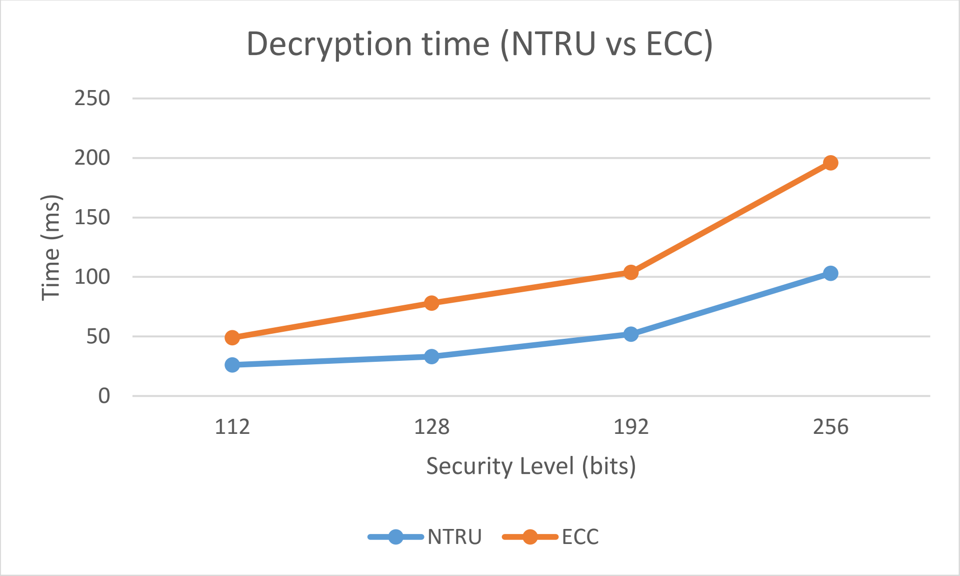


Figure 4.5: Decryption time (NTRU vs ECC) in smartphone

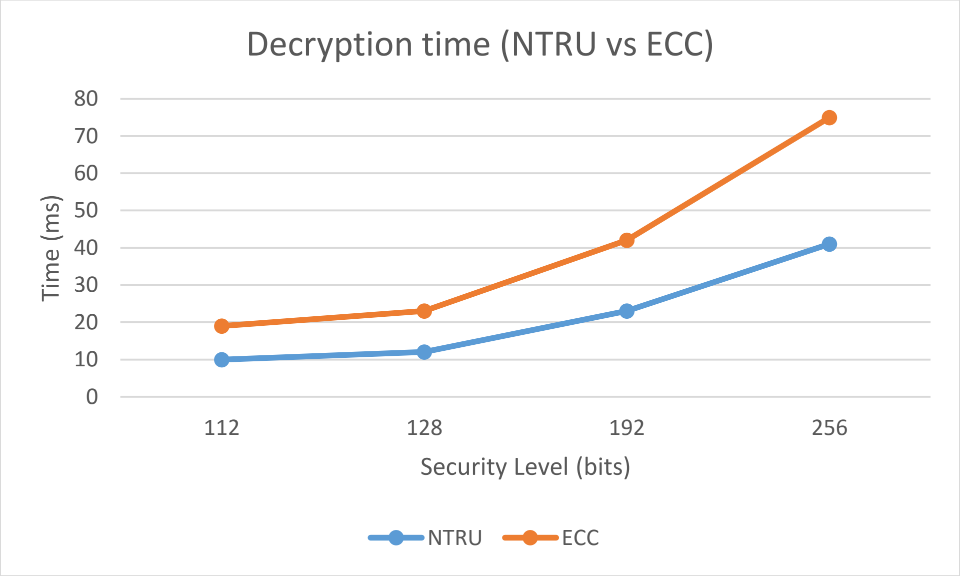


Figure 4.4: Decryption time (NTRU vs ECC) in PC

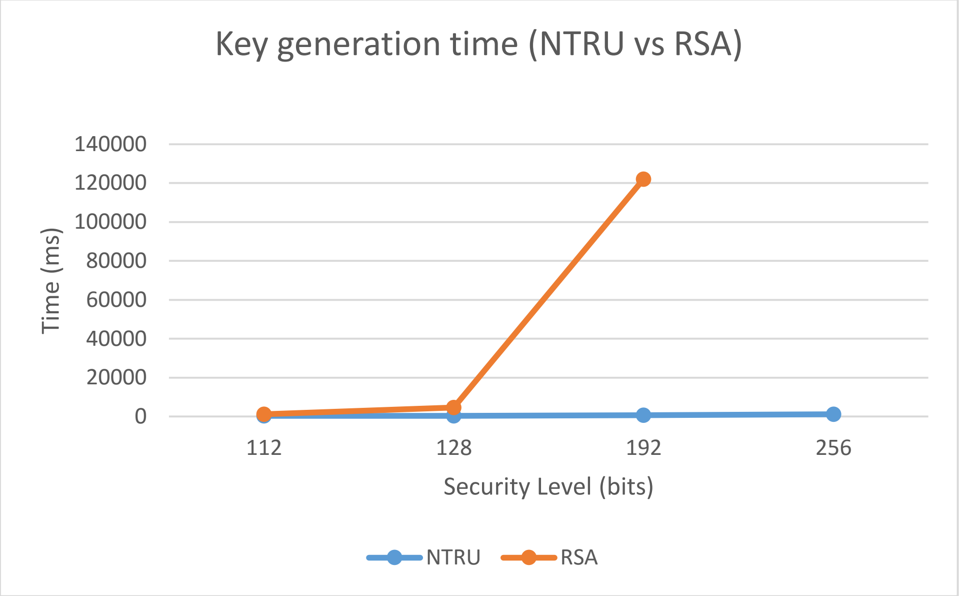


Figure 4.5: Key Generation time (NTRU vs RSA) in smartphone

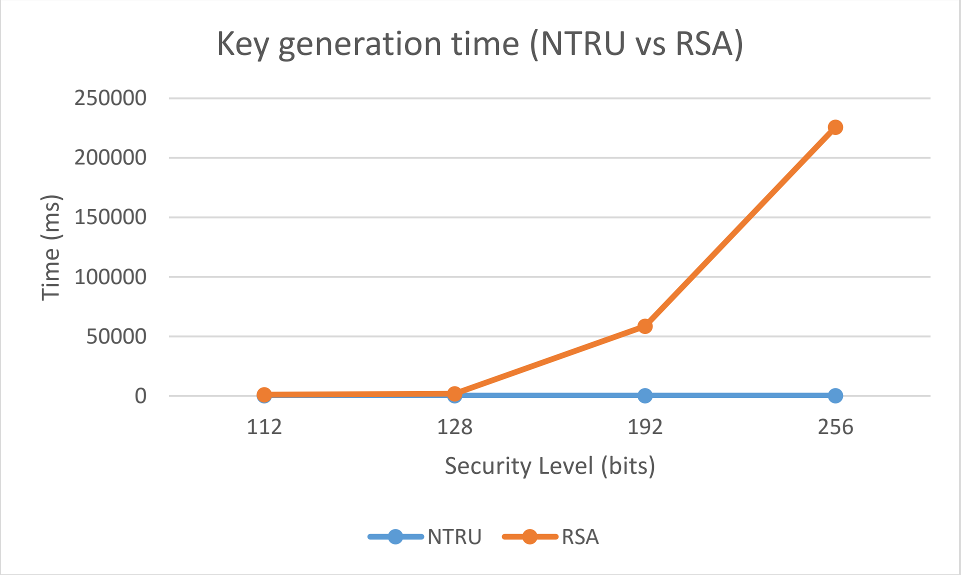


Figure 4.6: Key Generation time (NTRU vs RSA) in PC

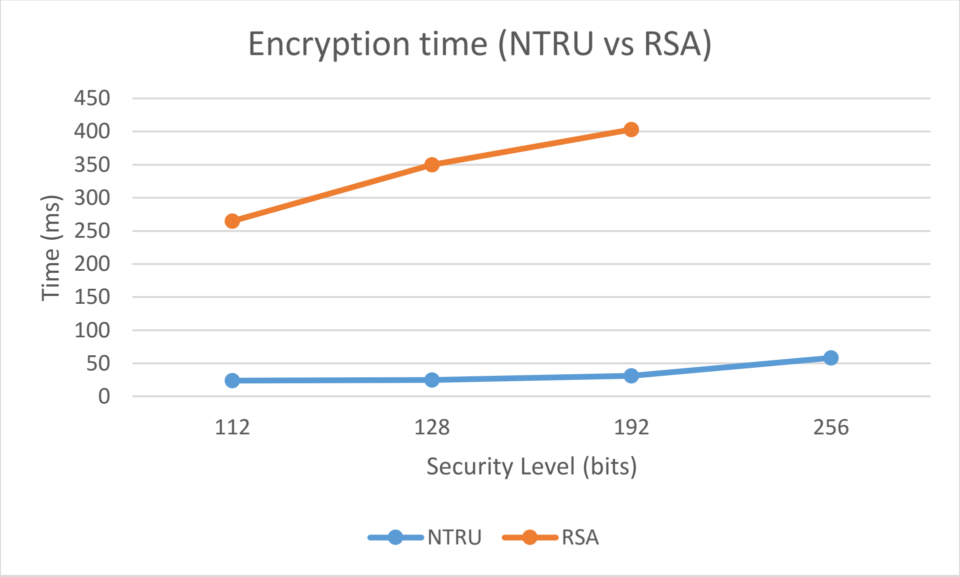


Figure 4.7: Encryption time (NTRU vs RSA) in smartphone

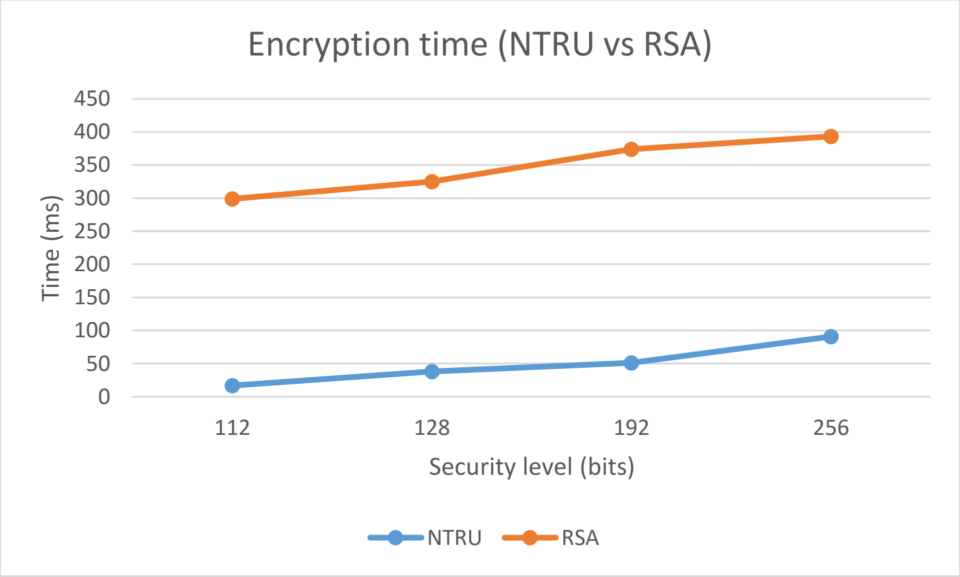


Figure4.8: Encryption time (NTRU vs RSA) in PC

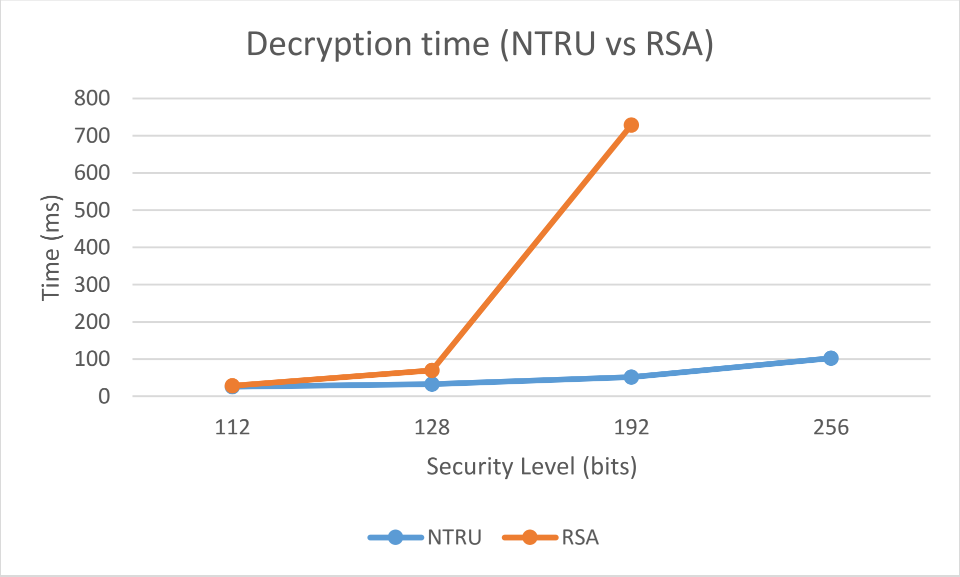


Figure 4.9: Decryption time (NTRU vs RSA) in smartphone

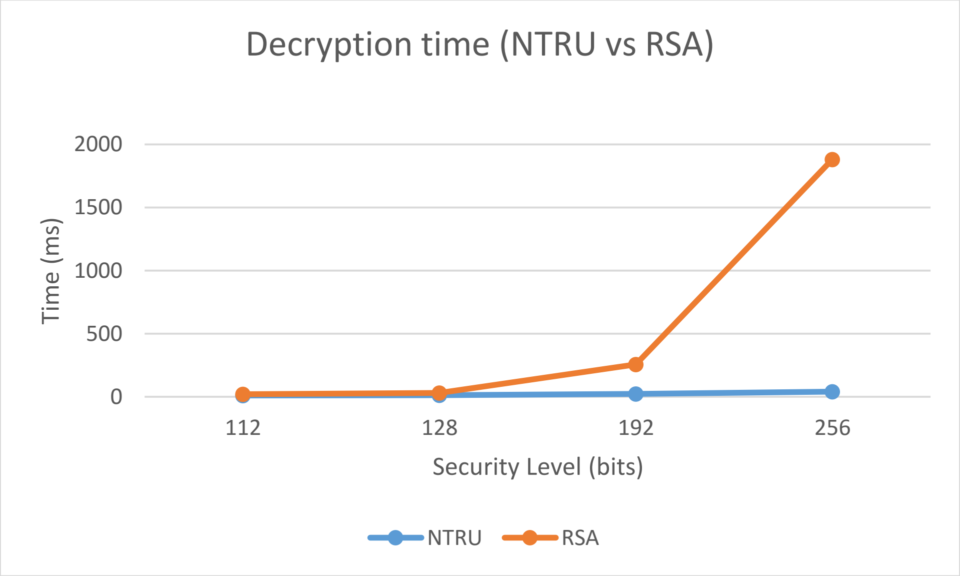


Figure 4.10: Decryption time (NTRU vs RSA) in PC

All the above data comes from the performance tests of our implementations. The encryption time is the time it takes to encrypt one plaintext block. The same applies to decryption. We can see from the above plots that the fastest cryptosystem is NTRU, but this cryptosystem also has the longest private key and the largest message expansion.

NTRU also has longer block size than ECC. The key generation of RSA is very slow compared to other cryptosystems discussed here.

Comparison of NTRU against RSA and ECC

Table 4.1: Comparison between RSA, ECC and NTRU

Method	**RSA**	**ECC**	**NTRU**
Key Generation	Slow	Faster	Fastest
Encryption	Slow	Faster	Fastest
Decryption	Slow	Faster	Fastest
Complexity	O(N^3)	O(N^3)	O(NlogN)

4.1 Prototype

To show the practicality of a mobile payment system, we developed a prototype mobile application that implemented a simple payment system. Our goals with developing this application were to show basic functionality of a mobile payment system which transfers amount from customer's handset to NFC-POS at the merchant side.

As part of the prototype, we built three components:

1. A client console application for merchant side

2. A client Android application for customer's smartphone

This chapter describes this prototype and what choices were technology choices were made to develop it. We need both MS and NFC POS for our payment system. We developed java program for NFC POS which will be connected to PC and an android program to run on our smartphone.

For NFC POS we have used ACR122U NFC Reader in card emulation mode which is a PC-linked contactless smart card reader/writer developed based on 13.56 MHz Contactless (RFID) Technology. ACR122U is compliant with both CCID and PC/SC. Thus, it is a plug-and-play USB device allowing interoperability with different devices and applications. With an access speed of up to 424 kbps and a full USB speed of up to 12 Mbps, ACR122U can also read and write more quickly and efficiently. The proximity operating distance of ACR122U is up to 5 cm, depending on the type of contactless tag in use.

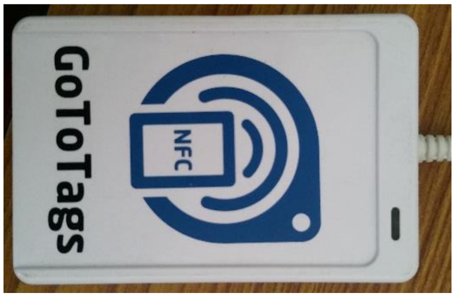


Figure 4.11: ACR122U

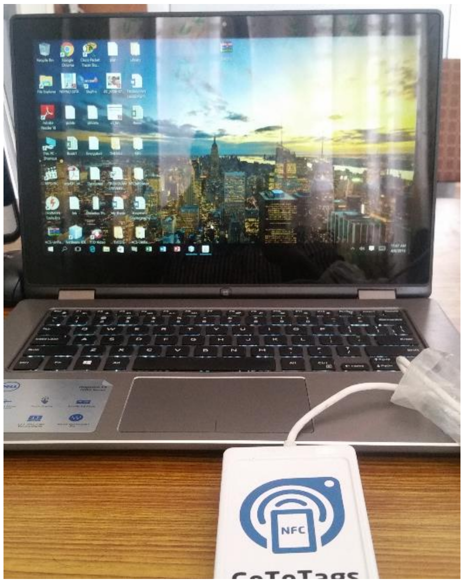
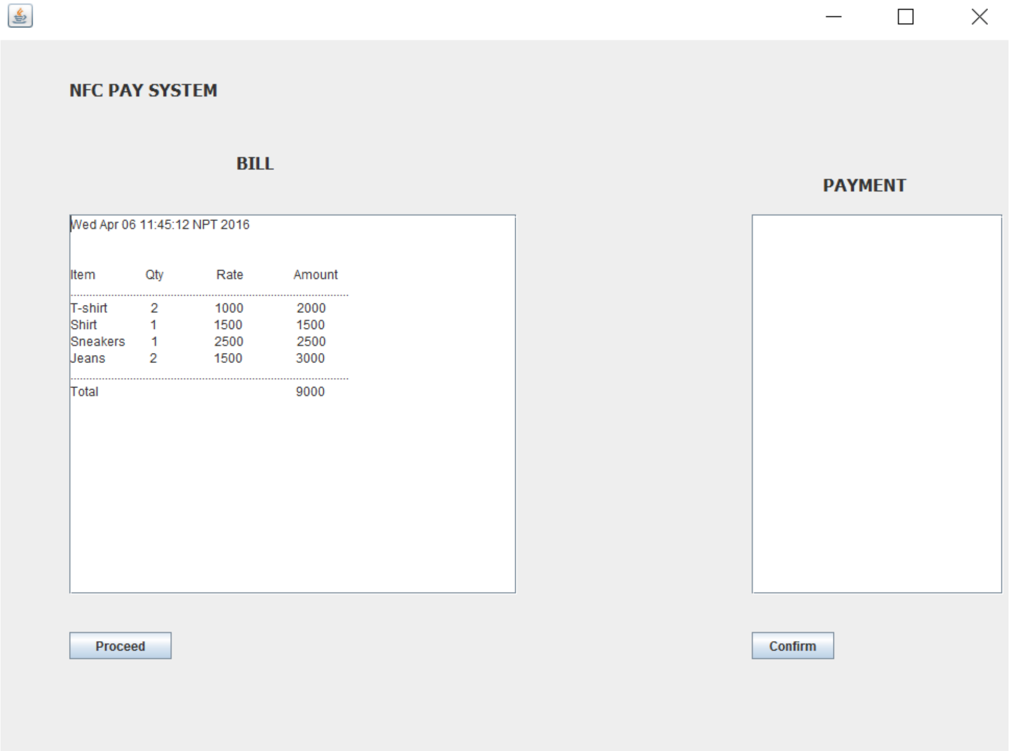


Figure 4.12: NFC payment physical setup



```
Wed Apr 06 11:45:12 NPT 2016


Item        Qty        Rate        Amount
.................................................
T-shirt      2         1000         2000
Shirt        1         1500         1500
Sneakers     1         2500         2500
Jeans        2         1500         3000
.................................................
Total                               9000
```

Figure 4.13: NFC payment Application PC side

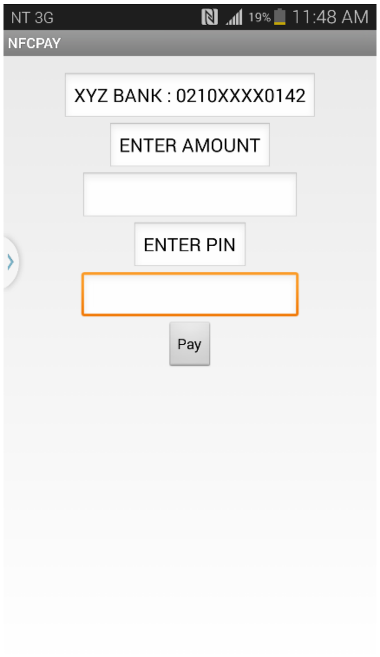


Figure 4.14: NFC payment Application smartphone side

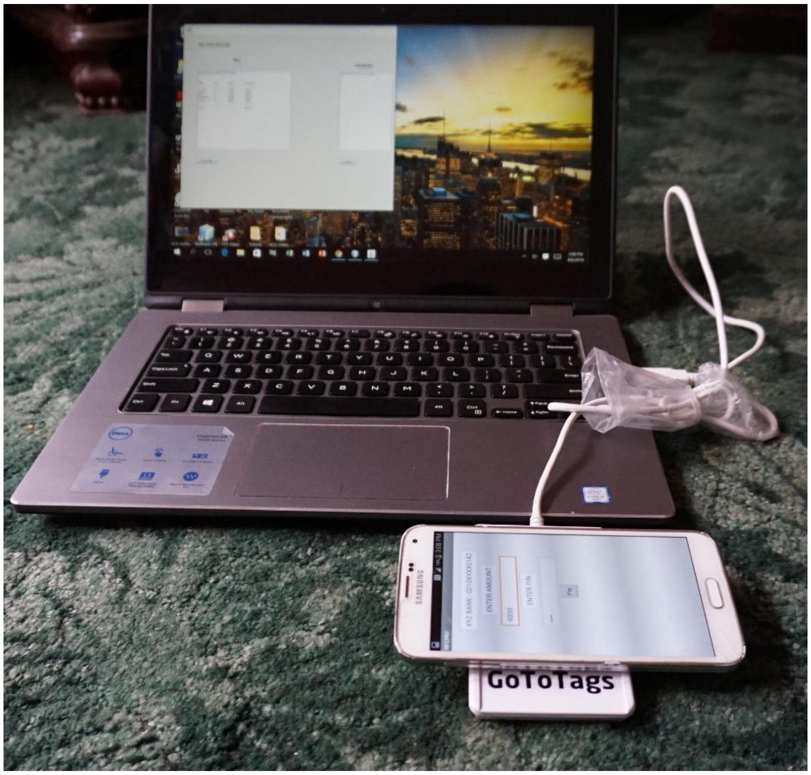
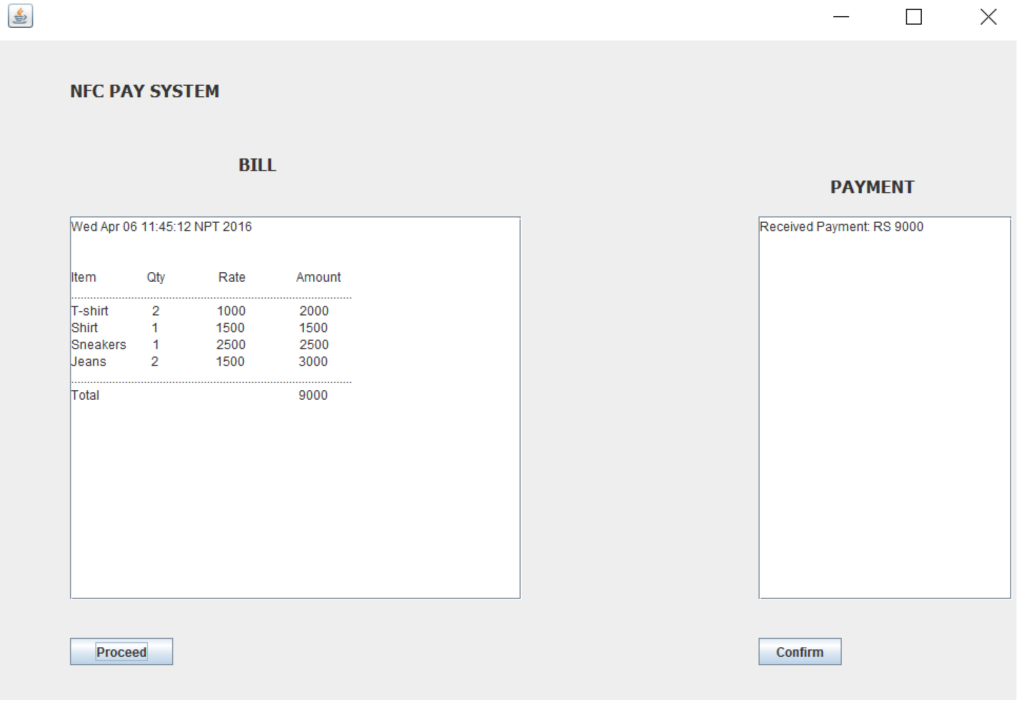


Figure 4.15: NFC Payment in process



NFC PAY SYSTEM

BILL

```
Wed Apr 06 11:45:12 NPT 2016


Item        Qty         Rate        Amount
-------------------------------------------
T-shirt      2          1000         2000
Shirt        1          1500         1500
Sneakers     1          2500         2500
Jeans        2          1500         3000
-------------------------------------------
Total                                9000
```

PAYMENT

```
Received Payment: RS 9000
```

Figure 4.16: Payment Completion

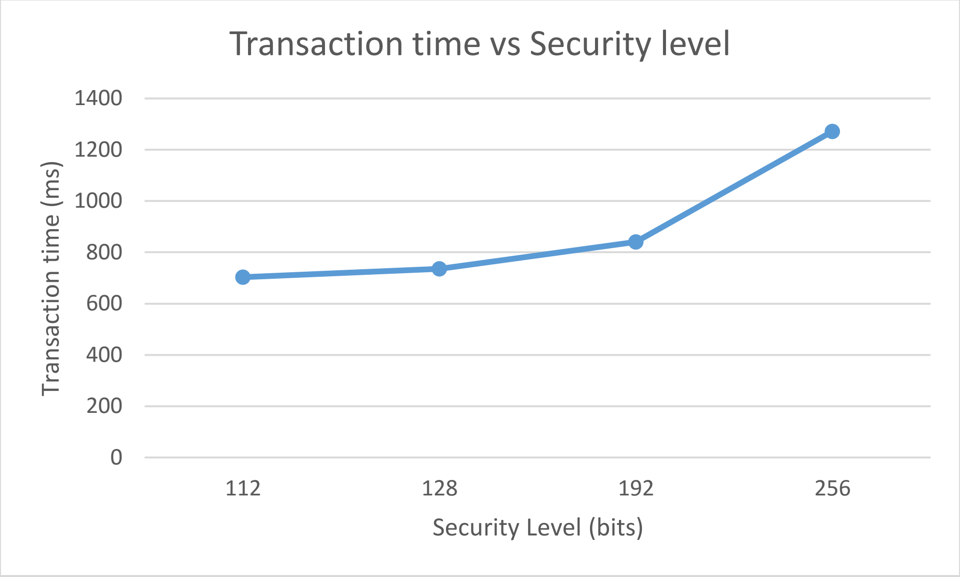


Figure 4.17: Total Transaction time for different security levels

4.3 System Security Issues

As with any technology MP is vulnerable to attacks and sufficient security is required for a successful implementation [32]. All communications between a phone and other components of the system are via an OTA interface, and thus MP is exposed to all wireless network attacks, such as eavesdropping, Man-In-The-Middle attacks, and virus or worm infection. MP is still in its novice stage and has not been scrutinized for years. It requires more standardization and interoperability in heterogeneous computing networks. To provide sufficient security, a system should fulfill vital requirements such as authentication, authorization, non-repudiation, data integrity, confidentiality.

4.3.1 Dimensions of Security

Authentication

This is the process of proving the identity of the entity to the verifying entity. Authentication could be in any form as long it uniquely identifies. Examples include a password to log into a system, PIN has been used as a password to enter the mobile payment application. Using USIM/SIM PIN, RFID key fob to gain access to a building, a smart card, or fingerprints on driver's license. In our payment system, the first factor is owning a cell phone and the second factor is that USIM/SIM the user is authenticated against the USIM/SIM, the USIM/SIM is then authenticated against the cellular mobile network before the subscriber is allowed to use the UMTS/GSM services. In addition to USIM/SIM PIN, user needs to enter PIN just like in ATM cards. The application calculates the hash of the entered PIN, when this hash value is known to the bank server, the server checks for the sameness. The payment happens only when user inputs his own PIN.

Authorization

After successful authentication, a system checks if a user is permitted the requested access; in this payment model, the MNO verifies if user is indeed subscribed to MP services and if so a payment transaction continues. The payment application in the Smartphone fetches the information about SSN, IMEI and IMSI, and all these three parameters are uniquely bind to the particular SIM.

Non-Repudiation

Sometimes one of the entities involved in communication later on denies its participation; a sender might repudiate having sent message, or a recipient might deny receiving a message. Non-repudiation protects against the denial of an entity. In this payment model, a user might deny sending a purchase request or an MNO might refuse to acknowledge a transaction confirmation sent earlier. In either case, with signed confirmation of a purchase from a third party which is merchant, non-repudiation is achieved. MS send financial information along with digital signature which will be later used later to verify message integrity.

Data Integrity

During communication between entities it is important that the message or data has not been tampered with. Data integrity guarantees that message still in its original form and has not been modified during transmit. In this payment model, the data integrity can be guaranteed by signing the financial transaction information. A digital signature is an electronic signature derived using mathematical operations and used to prove a sender's identity.

Data Confidentiality

Ensuring that data has not been tampered is vital for security, and equally important is data confidentiality. This property states that data will never be accessed by an unauthorized entity. This payment model provides data confidentiality by using message encryption between an MS and a communicating MNO or NFC POS.

4.3.2 NFC threats and Solutions

Even though the range of operation of NFC is within about 4 inches, there are still threats to NFC applications. NFC security has not been scrutinized as much as other wireless technology, but some studies show that it is possible to intercept communication between entities and modify data.

Eavesdropping

NFC devices communicate with each other via RF waves and an adversary equipped with radio scanner could eavesdrop. In general communication range of NFC devices is within close proximity or less than 4 inches. But there is not a set distance on how close an attacker needs to be in order to intercept a radio signal. A successful attack requires a good quality signal receiver and decoder, an antenna that changes directions in 3 dimensions, and an environment with less distractions and barriers such as noise, metal and wall. The geometry of the antenna and power level of sender could also influence the success of an attack. Another non-negligible factor is the operating mode of the sender device, in an active mode the sender creates its own RF field and in passive mode it uses the other device's RF field. An active mode is intended to seek for passive devices within close proximity and therefore in this mode eavesdropping is possible up to a distance of about 10 meters. On the contrary, a device in passive mode waits silently until active device power. Thus, the possible eavesdropping distance is 1 meter. Eavesdropping could be prevented using a secure communication channel.

NFC by itself cannot protect against eavesdropping. The only real solution to eavesdropping is to establish a secure channel as has been done in our system by implementing encryption mechanism.

Data Modification

This attack differs from data corruption in that it sends valid but modified data. The data modification depends on the applied strength of the amplitude modulation. The possibility for such attack has been prevented by implementing secure communication channels.

Data Insertion

An attacker replies with its own message to a sender before a valid receiver replies back. If this attack occurs at the same time as when a receiver replies back, the data will be overlapped and corrupted. The success of this attack is to insert data before an answering device sends its reply.

Prevention of this attack has been done by using secured communication channel.

Man-in-the-Middle

The advantage of NFC's close proximity prevents a Man-in-the-Middle attack; an RF field of an attacker is easily detected due to its active disturbance. During active to passive communication, an RF field created by the attacker overlaps with the RF field of active device. A passive device will not be able to understand an overlapped message. Also, an active device could detect that some activity is going on during transmission. A Man-in-the-Middle attack also is not possible during active to active communication. We will explain it by an example. An active device Alice sends a message (M) to an active device Bob and turns off its RF field. An attacker Eve creates its own RF field to disturb Bob receiving M. Alice is listening now and detects the disturbance created by Eve and stops communication. Alice could also detect Eve's activity earlier when it sent M to Bob because Eve creates disturbance so Bob will get it before Alice's M.

Therefore a Man-in-the-Middle attack is not possible with NFC. The recommendation is to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties. Additionally, we have a secure channel between two NFC devices.

4.4 Concluding Remarks

We have presented a payment protocol that is a reasonably close to what was envisioned. The choice of Lattice cryptography over RSA and ECC is justified by its faster key generation time, encryption time and decryption time. The performance of the payment system presents features of being fast and practically feasible throughout the range of security level (112 bits, 128 bits, 192 bits and 256 bits). In the meantime the model also addresses different facets of security: Authorization, Authentication, Non-repudiation, Data Integrity and Data Confidentiality, and the model also address the threats such as eavesdropping, data modification, data insertion and man in the middle attack.

It is not without its caveats- especially performance is a concern- but we have no problems in recommending further developments in this area.

5. RECOMMENDATIONS

As is clear from the conclusion, the work in Lattice cryptography based payment system has been by no means finished. The following areas of research can be remarked as further improvements to the current state of payment model. Improvements can be made both in implementation work as well as new academic directions.

This thesis was mainly focused on the details of the involved cryptography and their implementation details. Several unrelated questions often cropped up during our implementation and during the interpretation of our results. These questions dealt with what factors constrain the practicality of mobile payment system. The practicality of a payment system is not just constrained by its security features or its speed; it is also constrained with how usable these features are. But what makes a usable payment system? What would a mobile payment application look like? What transaction speeds constitute a payment system that is pleasant to use? These questions are unaddressed in this thesis, but of incredible importance to complete the picture of a truly practical payment system.

5.1 Implementation improvements

We have successfully developed and tested the performance of the payment model. However another part of the model which is the transfer of encrypted financial transaction between MS and MNO server via OTA needs to be tested. One future direction would be to test and compare the results between transfer of NTRU encrypted financial transaction between MS and MNO server and transfer of ECC encrypted financial transaction between MS and MNO server. Since ECC has smaller key size and OTA size is also small, this provides solid glimpse into the trade-offs between the key size and speed.

5.2 Divisible payment system

Lattice systems have been used to enable fully homomorphic cryptosystems, which has potential as a basis for fundamentally different and divisible payment systems. Lastly, and most importantly within the context of this work, signature systems based on lattices allow for very fast verification [33, 34]. The reason verification of lattice-based signatures is so fast is that only very simple algorithms on matrices of small numbers are needed to perform a verification.

Lattice cryptosystem can be a basis of highly secured, offline, anonymous, and scalable divisible payment system.

REFERENCES

[1] Royal Bank of Scotland, "World Payments Report 2015", 2015.

[2] Federal Reserve Bank of Kansas City, "Complex Landscapes: Mobile Payments in Japan, South Korea, and the United States", 2007.

[3] Raina, Vibha Kaw, U. S. Pandey, and Munish Makkad, "Use of mobile transactions payment model in customer oriented payment system using NFC technology." *International Journal of Mathematical and Computer Sciences*11.2 (2011): 49-57.

[4] GSMA, “The Mobile Economy 2015”, 2015.

[5] Aziza, H, "NFC technology in mobile phone next-generation services,” *Near Field Communication (NFC), 2010 Second International Workshop on*. IEEE, 2010.

[6] Pasquet, Marc, Joan Reynaud, and Christophe Rosenberger, "Secure payment with NFC mobile phone in the Smart Touch project." *Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on*. IEEE, 2008.

[7] Linck, Kathrin, Key Pousttchi, and Dietmar Georg Wiedemann, "Security issues in mobile payment from the customer viewpoint." (2006): 1-11.

[8] Minihold, Roland, "Near Field Communication (NFC) Technology and Measurements." White Paper 6 (2011).

[9] Woo, Jungha, "Verification of receipts from M-commerce transactions on NFC cellular phones." *E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2008 10th IEEE Conference on*. IEEE, 2008.

[10] Alliance Smart Card, "Proximity mobile payments: Leveraging NFC and the contactless financial payments infrastructure." *Smart Card Alliance* (2007).

[11] Madlmayr, Gerald, Josef Langer, and Josef Scharinger,"Managing an nfc ecosystem." *Mobile Business, 2008. ICMB'08. 7th International Conference on*. IEEE, 2008.

[12] *International Organization for Standardization*, Near Field Communication – Interface and Protocol (NFCIP-1).ISO/IEC 14443, 2009.

[13] Roland, Michael, Josef Langer, and Josef Scharinger, "Security vulnerabilities of the NDEF signature record type." *Near field communication (NFC), 2011 3rd International Workshop on*. IEEE, 2011.

[14] NFC Forum, *NFC Forum Technical Specifications* [Online] Available: http://members.nfc-forum.org/specs/spec_list/.

[15] Siira, Erkki, Tuomo Tuikka, and Vili Törmänen, "Location-based mobile Wiki using NFC tag infrastructure." *Near Field Communication, 2009. NFC'09. First International Workshop on*. IEEE, 2009.

[16] Coutinho and Severino Collier, *The mathematics of ciphers: number theory and RSA cryptography*. Universities Press, 2003.

[17] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[18] Certicom, *ECC Tutorial* [Online] Available: https://www.certicom.com/ecc-tutorial

[19] Regev Oded, "Lattice-based cryptography," in *Advances in Cryptology-CRYPTO 2006,* Springer Berlin Heidelberg, 2006. 131-141.

[20] Lenstra, Arjen Klaas, Hendrik Willem Lenstra, and László Lovász. "Factoring polynomials with rational coefficients," in *Mathematische Annalen* 261.4 (1982): 515-534.

[21] Gentry Craig, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009.

[22] Trappe Wade, "Lattice Methods," in *Introduction to cryptography with coding theory*, The Mathematical Intelligencer 29.3 (2007): 66-69.

[23] Tech-FAQ, *History of Cell Phones* [Online] Available: http://www.tech-faq.com/who-invented-the-cell-phone.html

[24] Ali I. Gardezi, Security in wireless cellular networks [Online] Available: http://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security/

[25] Garg Vijay, *Wireless communications & networking*, Morgan Kaufmann, 2010.

[26] He, Sheng, and Ing Christof Paar, "SIM card security," Bochum: Ruhr-University (2007).

[27] Kataria, Jyoti, and Abhay Bansal, "Exploration of GSM and UMTS Security Architecture with Aka Protocol," *International Journal of Scientific and Research Publications* 3.5 (2013).

[28] Lukeman C, "Securing Cellular Access Networks against Fraud" (2009).

[29] Kaaranen Heikki, and Miikka Poikselkä, "UMTS Core Network," *UMTS Networks: Architecture, Mobility and Services, Second Edition* (2005): 143-194.

[30] Platform, Global, "GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging," *White Paper, April* (2009).

[31] Haselsteiner Ernst, and Klemens Breitfub, "Security in near field communication (NFC)," *Workshop on RFID Security RFIDSec*. 2006.

[32] Francis Lishoy, "A security framework model with communication protocol translator interface for enhancing NFC transactions," *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*. IEEE, 2010.

[33] Hoffstein Jeffrey, Jill Pipher, and Joseph H. Silverman, "NSS: An NTRU lattice-based signature scheme," *Advances in Cryptology—Eurocrypt 2001*. Springer Berlin Heidelberg, 2001. 211-228.

[34] Güneysu Tim, "Software speed records for lattice-based signatures," *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2013. 67-82.