Hardware Implementation of Ultra-lightweight SIMON Algorithm for Data Encryption and Authentication using RSA for VANET Security

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF TECHNOLOGY

in

VLSI DESIGN

Submitted By

Deeksha

601562008

Under Supervision of

Mrs. Manu Bansal

Assistant Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY, PATIALA, PUNJAB

JUNE, 2017

DECLARATION

I, **Deeksha** hereby declare that the work presented in this thesis entitled "**Hardware Implementation of Ultra-lightweight SIMON Algorithm for Data Encryption and Authentication using RSA for VANET Security**" in partial fulfillment of the requirement for the award of degree of Master of Engineering submitted at Electronics and Communication Engineering Department, Thapar University, Patiala is an authentic record of work carried out under supervision of **Mrs. Manu Bansal** (Assistant Professor, ECED, Thapar University, Patiala). The matter presented in this, has not been submitted either in part or full to any other university or institute for the award of any other degree.

Date: 10 August, 2017

Deeksha
DEEKSHA
REG No.601562008

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 10/8/17

Manu Bansal
Mrs. Manu Bansal
Assistant Professor
TU, ECED, Patiala

ACKNOWLEDGEMENT

I take this opportunity to express my profound sense of gratitude and respect to all those who helped me through the duration of this dissertation. I acknowledge with gratitude and humility my indebtedness to **Mrs. Manu Bansal, Assistant Professor,** Electronics and Communication Engineering Department, Thapar University, Patiala, under whose guidance I had the privilege to complete this dissertation. I wish to express my deep gratitude towards her for providing individual guidance and support throughout the dissertation work. I convey my sincere thanks to **Head of the Department, Dr. Alpana Aggarwal, ECED,** entire faculty and staff of Electronics and Communication Engineering Department for their encouragement and cooperation.

My greatest thanks is to all who wished me success especially my family. Above all I render my gratitude to the Almighty who bestowed ability and strength in me to complete this work.

Place: Patiala
Date:

Deeksha
M Tech Final Year,
Thapar University.

ABSTRACT

In modern era, traffic accidents are serious botheration across the world. VANET is a fundamental module of Intelligent Transport Systems (ITS) that has gained a lot of attention from the automotive industry. Approximately 1.3 million people got died during road mishaps as well as additional 20-50 millions are hurt globally. VANETs share information about road safety associated to traffic investigation by giving intimation to driver to abstain 60%of the mishaps. But VANETs also faced some challenges in terms of security and authentication as VANETs is susceptible to many attacks such as DOS attack, Sybil attack, replay attack, routing attack, timing attack, eavesdropping, location trailing, bogus information and brute force attack. To resist the impact of these threats, a survey is done on VANETs attacks and their countermeasures. Also, comparative analysis of VANET security technique is done. Based on survey it is found that for data security and authentication, different cryptography algorithms are used such as AES, blowfish, ECC and RSA *etc*. But these algorithms have very huge consumption of area and memory. These algorithms are not suitable to use in resource-constrained devices.

This thesis work attempts to resolve these resource constrained issues and provides efficient data security and authentication for VANETs. In the proposed work, for providing encryption, optimized ultra-lightweight cryptography algorithm SIMON is used. The performance analysis is done on the basis of slices utilization, throughput and efficiency. The hardware results reflect that the proposed approach consumes 60% less area than existing parallel architecture of SIMON and is 85% more efficient than existing serial architecture of SIMON. Further, for the authentication RSA algorithm is proposed in which multiplication of numbers is done using two multiplication algorithms i.e. Vedic algorithm and Karatsuba algorithm. From the Performance analysis based on LUTs, it is concluded that Vedic consumes less area as compared to Karatsuba.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

MANETs	Mobile Ad-hoc Networks
VANETs	Vehicular Ad-hoc Networks
V2V	Vehicle-to-Vehicle communication
V2I	Vehicle-to-Vehicle communication
RSU	Road Side Units
DSRC	Dedicated Short-Range Communication
DOS	Denial of Service
DDOS	Distributed Denial of Service
TPM	Trusted Platform Module
AES	Advanced Encryption Standard
DES	Data Encryption Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
ARM	Advanced Risk Machines
GPSR	Greedy Perimeter Stateless
NSA	National Security Agency
ECC	Elliptic Curve Cryptography
ARAN	Authenticated Routing for Ad hoc network
SEAD	Secure and Efficient Ad hoc Distance Vector
NIST	National Institute of Standards and Technology
ECDH	Elliptic-Curve Diffie Hellman

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW of WIRELESS NETWORKS

Wireless networks can be usually a network of nodes that manage the environment which enable communication involving persons or computers as well as surrounding environment. The primary professional wireless network was developed at the University of Hawaii under the brand ALOHA net in 1969 and became operational in June 1971. The Advantage of wireless networks is that complexity of infrastructure setup and management has been sorted and joining of networks can be done anytime, anywhere using “on the fly” to enable devices. One decentralized type of wireless networks is MANETs. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research area since mid-1990s. MANETs which are infrastructure less networks are continuously self-configuring and are connected wirelessly. It often changes its links to other devices because of the independency of each device to move freely in any direction. These kinds of networks may need the connection to larger internet or may operate by themselves. The Radio frequencies used for the communication in MANETs is 30 MHz - 5 GHz. There are many applications of MANETs i.e. peer to peer messaging, environment sensors, robots, disaster rescue operations, safety of roads, health, home, vehicular ad- hoc communications, navy defense *etc.*

1.2 OVERVIEW ON VANETs

VANETs are a subgroup of MANETs. In modern era, traffic accidents are serious botheration across the world. Traffic crashes on Road rated as 9th foremost cause of death. Approximately 1.3 million people got died during road mishaps as well as additional 20-50 millions are hurt globally. Some survey shows that if the driver acquires intimation about the accident still before 1/2 a second of mishap then 60% of accidents can be abstained. Vehicular Ad hoc Networks (VANETs) accomplish the purpose via sharing information about road safety which associated to traffic investigation, normal statistics like files, videos etc by means of continuous internet association [1]. In VANETs, vehicles as well as roadside infrastructures are communicating nodes and MANETs featuring wireless communication while moving. At present, there are many applications of VANETs which focus on different facets of transportation organizations like driving aid, security of public, collection of tolls, control of traffic on roads, rising security as well as freeway system’s potency [2]. Due to Large storage capacity, energy sufficiency, high processing power, predictable movement of

nodes, VANET considered being different as of additional ad-hoc wireless networks of the similar category.

1.2.1 Architecture of VANETs

In this, the basic architecture of VANETs has been discussed. Figure 1.1 shows the basic architecture of VANETs that includes V2V, V2I communication, OBUs, Application Units (AU), RSU and Access network.

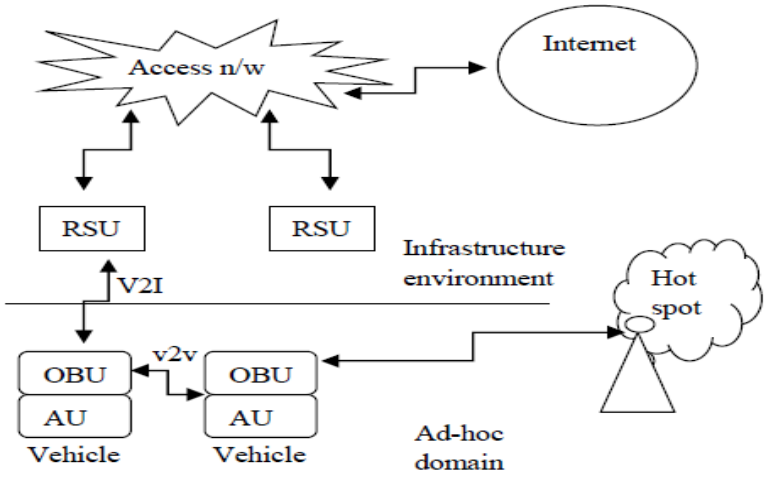

Figure 1.1 Architecture of VANETs [1]

The architecture of VANETs has following mechanism:-

- Ad hoc environment: It dwells intelligent vehicles (nodes) that contain fundamentally components: On Board Unit and Application Unit.
- OBU: GPS module, wireless communication module, Central control module, and human-machine interface module are the four modules of OBU unit. Central control module encloses processing of serial port information, memory, judgment as well as decision making and data transceiver. The OBU unit has communicational capabilities. The connection of vehicle with RSU via DSRC radios is done by this unit where DSRC is at present acknowledged as mainly assuring standard of wireless to connect I2V and V2V. On one side, vehicles got information from GPS module comprising acceleration, location and speed which are broadcast numerous times per second by each OBU-equipped vehicle and they also receive "safety messages" from OBU- appareled neighbors at same time. After receiving these messages, vehicle decides whether there is collision treat or not by figuring out the lane of its neighbor and comparing these with its own trail. If a collision hazard is identified, the caution information will be transmitted to neighbors instantly. On the other hand, when the driver determine hazard, he/she can push the warning buttons on the touch display of the OBU. Then, the warnings will be transmitted to neighbor vehicles by OBU. The OBU will act right away to inform the

driver after determining collision hazard or getting a warning [3]. Figure 1.2 shows the global design diagram of OBU unit.

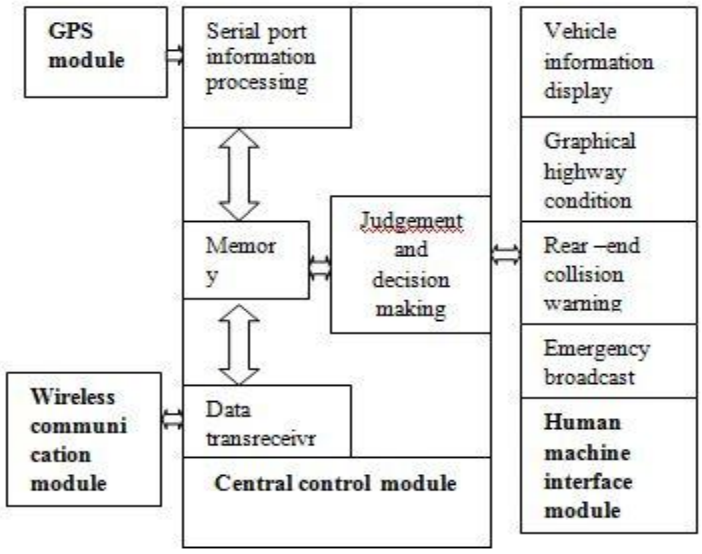

Figure 1.2 Global design diagram of OBU unit

- AU (Application Unit): This unit facilitates OBU to communicate by implementing program. The connection of AU to the OBU can be wired or wireless and AU could endure with the OBU in a particular physical component. By using OBU unit (which gets task for all mobility and networking purposes) only, AU can communicate with the network.

➢ Infrastructure environment: It includes RSU as well as access network.

- RSU (Road Side Units): It is a wave device usually permanent beside the road side or in devoted positions such as at the intersections or close to parking places. The work of RSU is to act as a router among the vehicles on the road as well as provide connections to further network devices. Main functions of RSU are:

  1. Widening the range of communication of the ad-hoc network used to redistribute the data to further OBUs

  2. Convey the data to other RSUs to further forward it to other OBUs [4].

➢ Two categories of communication happen in VANETs:

- V2V (Vehicle-to-Vehicle) Communication: This is a wireless communication among vehicles. This communication pattern is useful where message is been sent to a group of vehicles or a specific vehicle i.e. in a multicast or uni-cast situation. For example -To extend traffic safety, warning message ought to be sent to incoming vehicles after recognition of mishaps [5]. The V2V warning propagation is shown in figure 1.3.

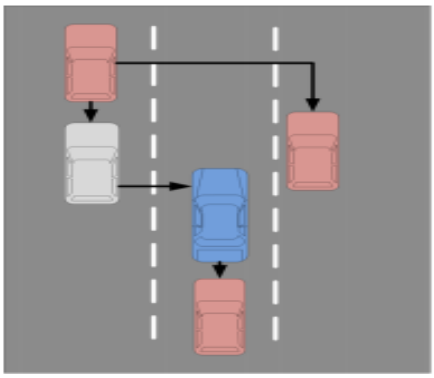

Figure 1.3 V2V warning propagation [5]

- V2I (Vehicle-to-Infrastructure) Communication: In this communication, when a potential danger is detected, sending of messages is done either via infrastructure i.e. through RSUs or a vehicle. For the communication among vehicles as well as RSUs, high bandwidth connection is used. As an example- Approaching to an intersection, a warning could be sent by the V2I when a potential clash could occur. The roadside unit will frequently transmit a message including the limit of speed along with comparison of directional limits or any geographic with vehicle information to conclude if a limit of speed warning relates to any of the vehicles in the surrounding area [4]. The V2I warning propagation is shown in figure 1.4.

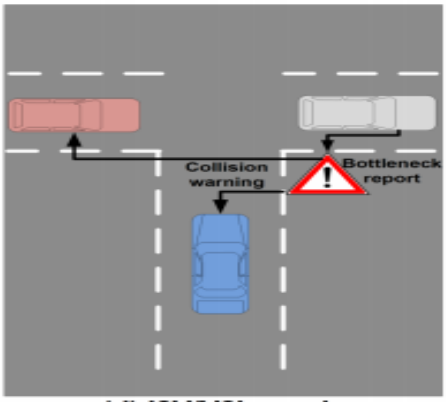

Figure 1.4 V2I Warning Propagation [5]

1.2.2 VANET Security Requirements

In VANETs, there are some security issues i.e. addition of several timeslots to the message which leads to receiving of message to a car in accidental position instead of safe position, convincing the vehicles to take alternate path by creating large number of pseudonymous, getting access of confidential data, tracing the vehicle and getting the confidential information about the driver by illegal trailing of the position or route followed by the vehicle etc. So, security is required as VANET packets holds life critical information and it is essential that these packets must reach to the drivers without any modification or insertion of

data, similarly the responsibility of drivers should also be recognized that they notify the traffic environment appropriately and within time. So, VANETs must satisfy following security requirements:

- Authentication: Authentication provides us a guarantee that data is engendered by an authentic client. It is crucial that the data which propagates in the organism must be accurate and engendered by an authentic client because in VANETs, nodes react according to the data established from the other end.
- Integrity: It ensures that the data at the sender and recipient side are same. Alteration of message is done by authorized users only. Recipient utilizes the same procedure as used at sender side to create a second digest from the message for comparing it with the original message. This procedure ensures the integrity in data. So, protection of all messages against alteration attacks is required for security purpose.
- Non Repudiation: This avoids frauds from refusing their offenses because in this even if the attack occurs, Non Repudiation will expedite the capability to recognize attackers [6].
- Availability: Vehicular networks will need real-time for many purposes so they must be accessible all the time. These applications require quicker reaction from sensor networks or Ad-hoc Network, annihilation of the result can occur or the message can become worthless if there is any holdup in seconds for various applications [6].
- Confidentiality: Privacy of all drivers ought to be confined. This security requirement is to guarantee that data will barely be read by approved users. Requirement of confidentiality is needed in group communications, where barely group members are permitted to read such data [5].
- Reliability: For security purpose, it is essential that data obtain during communication must be precise and truthful. To eradicate the precisely incorrect information, we need to do periodic verification of the system.

1.2.3 Various Attacks in VANETS and Their Prevention Measures

There exist several attacks on VANETs that leads to insecure transmission of information. Different types of attacks are possible on VANETs which are classified as follows:-

- Denial of Service (DoS) attack: This attack forbids arrival of critical information by taking authority of resources of vehicles or by jamming the channel utilized by the Vehicular Network. When numerous vehicles attack one particular vehicle, then DDoS poses more hazard than DoS. This attack violates availability property and prevention of this attack can be done using IP information handling technique and symmetric cryptography [1]-[2].

- Sybil attack: In this attack, attacker convinces the vehicles to take alternate path by creating large number of pseudonymous, and tell other vehicles about jam by claiming more than a hundred vehicles ahead [7]. This attack violates authenticity property and the techniques used to prevent this attack are Registration Position, Verification, Radio Resource Testing, digital signature, symmetric cryptography etc.
- Replay Attack: This attack confounds the authorities and prevents vehicles identification in hit and run accident by replaying transmission of previous data to seize benefit of the circumstances of the message at sending time. This attack violates integrity and confidentiality property and prevention of this attack can be done using time-stamping technique [7].
- Routing attack: This attack either disturbs routing process of network or plunges the packets by exploiting the susceptibility of network layer routing protocols. Black hole attack, warm hole attack and gray hole attacks are the most common routing attacks in VANETs. This attack violates availability property and prevention of this attack can be done using cryptography hashing technique.
- Timing attack: Broadcasting of security message to the vehicle at right time is one of the imperative requirements of VANET. Timing attack includes several timeslots to the message which leads to receiving of message via a vehicle in accidental location rather than a safe location. This attack violates authenticity property and the technique used to prevent this attack is Encryption Solution (TPM).
- Eavesdropping: This attack violates the confidentiality property and belongs to attack on network layer. Major target of this attack is to acquire access of private data. Creation of cipher is the best preventive measure of this attack.
- Location Trailing: This attack violates the privacy property. In this, attacker traces the vehicle and gets the confidential information about the driver by illegal trailing of the position or route followed by the car. ID based system is used to prevent this attack [1].
- Bogus Information: In this, Attacker transmits fake data in the network for its own profit and violates confidentiality property. For example a nasty node can transmit fake data of intense traffic due to mishaps over road along with clearing his way. Asymmetric cryptography as well as hashing is used to prevent this attack [1].
- Brute force attack: It is an exhaustive key search technique in which attacker uses all feasible passwords to find the key**.** This attack is time and resource consuming approach as the attacker needs to try all the possible combinations and the vehicle will lose its identity if the attacker found the key.

1.3 OVERVIEW OF CRYPTOGRAPHY FOR VANET SECURITY

The term cryptology derived from “Gree - Kryptós - lógos”, which refers to “hidden word”. Cryptology embraces both Cryptography and Cryptanalysis. Cryptography is the study of using different algorithms, protocols or strategies for encryption and decryption process. Cryptography is the study of protecting data, in which conversion of data into unintelligible form is done to prevent it from unauthorized access and after secure transmission of data again conversion of data into intelligible form is done. Cryptography is the study of securing data whereas cryptanalysis is study to get access to the contents of encrypted messages even if the encrypted key is unknown. Figure 1.5 shows the overview of cryptography.

Modern cryptography involves following terminology:-

- Plaintext: It is the original intelligible message before encryption or after decryption. Message consist characters or binary file format that can easily be read by humans. Plaintext refers to a message or other data that is transferred or stored without cryptographic protection.
- Ciphertext: The transformed message of plaintext is called as ciphertext. We use different algorithms, strategies or protocols to encrypt plaintext into ciphertext and it is unreadable by humans or computer.
- Cipher: It is a strategy for converting an original understandable message to incomprehensible message. The operation of cipher usually depends on Key.
- Key: It is used in cipher and applied to a string or block of data to generate encrypted text, or for the decryption of encrypted text. It is critical information known only to sender or receiver. There are two categories of keys in Cryptography: “public key” and “private key”.
- Encipher (Encryption): It is the procedure of transforming plain data to highly confidential form. The transformed form should be like that only authorized parties can read it.
- Decipher (Decryption): It is the procedure of converting unintelligible message to intelligible again by applying key and cipher. Same or different key can be used for decryption process.
- Cryptanalysis: It is the study methods of converting an unintelligible message back into an intelligible message without any awareness about the key. Differential Cryptanalysis Attack and Linear Cryptanalysis Attack are two major cryptanalysis attacks in cryptography.

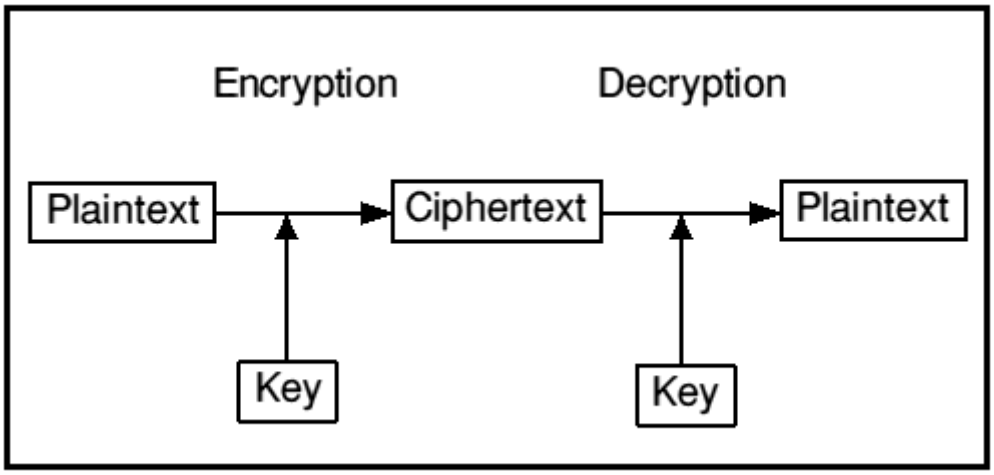

Figure 1.5 Overview of Cryptography

1.3.1 Fundamental Requirements of Cryptography [16]

Cautious examination of the scenarios summarized above reveals following fundamental requirements of secure communications:

- Confidentiality: Encoding is done to obscure the meaning of a message. Cryptographic key is applied to encrypt the intelligible information and by using either same or different cryptographic key, recipient decrypts that message. So, for security it is necessary that information can be understood by approved parties only.
- Integrity: It ensures that the data at the sender and recipient side are same. Alteration of message is done by authorized users only. Recipient utilizes the same procedure as used at sender side to create a second digest from the message for comparing it with the original message. This procedure ensures the integrity in data.
- Non repudiation: It is the method to ensure that data (received or sent) cannot be refuses to acknowledge. By doing non- repudiation, users cannot claim later about sending and receiving the data.
- Authentication: It refers to verification of each other's identity. This goal of cryptography involves two processes: authentication of entity and authentication of origin of data. It ensures that any kind of intruder does not have access to data.

1.3.2 Types of Cryptography

Cryptographic algorithms can be classified into numerous ways. These algorithms can be categorized into two types that depend on the number of keys used for encryption or decryption process. Table 1.1 shows the differences between two cryptography types.

- Symmetric-Key Cryptography (Secret-Key Cryptography): This type of cryptography involves the use of same cryptographic key to encrypt and decrypt the data. This also involves precomputation of keystream. But the major shortcoming of this is that all parties implicated need to exchange key for encryption process before the decryption process. Encryption and decryption algorithm are inverse of each other [17]. Symmetric key cryptography is shown in Figure 1.6.

  Example: block cipher in OFB mode.

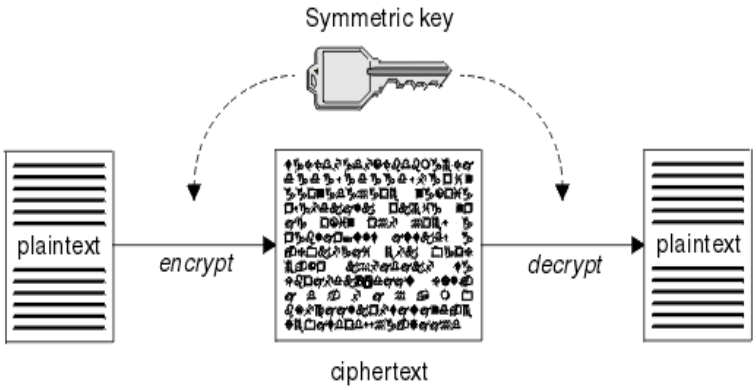

Figure 1.6 Symmetric-Key Cryptography

- Asymmetric-Key Cryptography: This type of cryptography involves the use of public key for the procedure of encryption and private key for the procedure of decryption. Keystream cannot be precomputed in this. In this, the “public key” can be disseminated openly in a public repository, but the related “private key” is known only to the recipients [17]. Asymmetric key cryptography is shown in figure 1.7.

  Example: Block cipher in ciphertext feedback (CFB) mode.

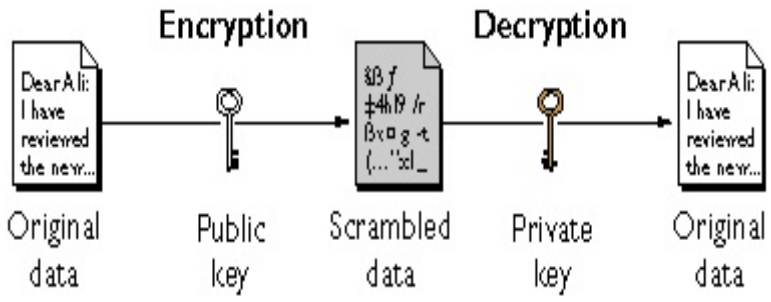

Figure 1.7 Asymmetric-Key Cryptography

Table 1.1 Advantages and Disadvantages of symmetric-key cryptography and asymmetric-key cryptography

Parameters	**Symmetric- Key Cryptography**	**Asymmetric- Key Cryptography**
Key	Shared secret key	Unique, private and public key pair
Strengths	• Fast performance • Easy to understand	• Limited exposure of information • Provides authenticity of the source
Weaknesses	• Exposure of key • Does not provide authenticity of source	• Public key management • Intensive computation
Examples	AES, 3DES	RSA, ECDSA

1.3.3 Cryptography Ciphers

Cipher is an algorithm used for both encryption and decryption process. The procedures of a cipher generally rely upon key. There are two types of ciphers in cryptography.

- Stream ciphers: Stream ciphers encrypts original data digit with corresponding keystream digit to give ciphertext digit. It is used to secure message in applications where the length of original data is either unidentified or unbroken and Because of typically fast processing, compactness and low power consumption in stream ciphers, they are used in resource- constrained devices. We can also call it state cipher because of dependency of each digit of plaintext on the current state of cipher [17-18].

  Stream Ciphers can be classified as:

- Synchronous Ciphers: In this, stream generation of pseudorandom digits is done which is independent of the original and transformed data and followed by combination with the original data or the transformed data is done. It is necessary that before the encryption/decryption process, correspondent and recipient must be precisely in order. In this, alteration of a bit of ciphertext message affects single bit of plaintext only. Synchronous ciphers are vulnerable to active attacks [18]. Synchronous ciphers are shown in Figure 1.8.

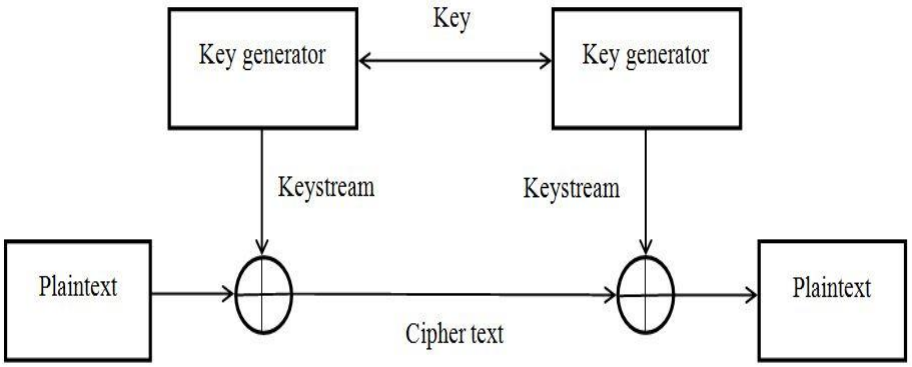

Figure 1.8 Synchronous Ciphers

- Self-Synchronous Ciphers: In this, on the basis of N previous ciphertext bits, updating of the internal state will take place. It is not necessary that before the encryption/decryption process, correspondent and recipient must be precisely in order but in this when N ciphertext bits are received, automatic synchronization of the receiver with the sender occurs. In this, alteration of a bit of ciphertext message affects at most N bits of plaintext bits [18]. Self synchronous ciphers are shown in figure 1.9.

  Examples of stream ciphers: GRAIN, TRIVIUM, SALSA20, MICKEY 2.0

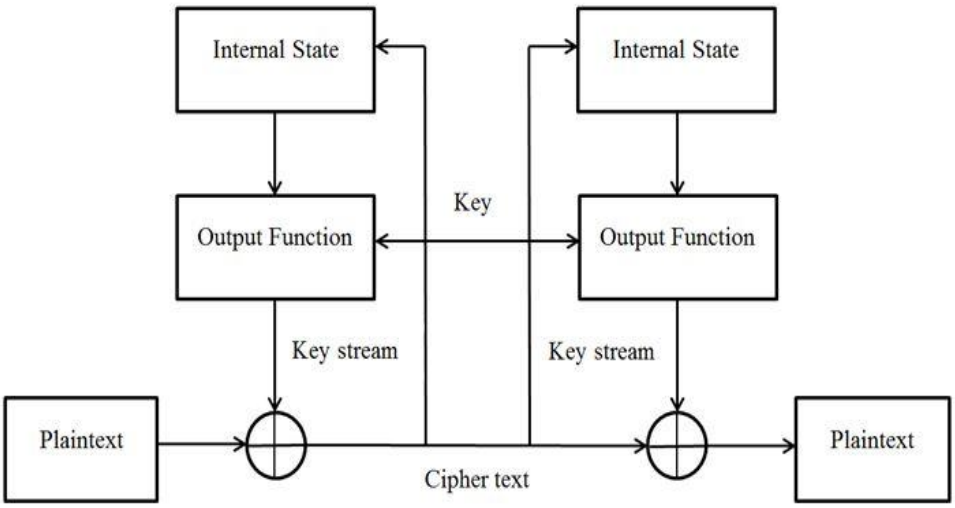

Figure 1.9 Self-Synchronous ciphers

Table 1.2 Advantages and disadvantages of stream ciphers

Advantages of stream ciphers	Disadvantages of stream ciphers
Low memory requirement as Stream ciphers process only one bit at a time.	Stream ciphers do not offer integrity or authentication.
They are not susceptible to noise in transmission because of independency of cipher bytes on other chunks of data.	Time consumption is more as it works on only one bit at a time.

- Block Ciphers [18]: Block ciphers involve the encryption of a data block by applying key and algorithm. In this, encryption and decryption takes place on data block as whole data is divided into block of certain bits (generally 64 bits or 128 bits). Block ciphers cannot be modified easily and are appropriate for the encryption of large data size.

  There are two types of Block Ciphers:

- Substitution/Permutation Block Ciphers: In this**,** generation of ciphertext block is done by applying numerous rounds of substitution-boxes and permutation-boxes on a block of plain text and key. S-box includes substitution of small data block by another data block and P-box includes the permutation of all the bits of data block i.e. in this, outputs of Substitution-box of one round are taken and then shuffling of the bits is done followed by the transfer of the Substitution boxes to the next round.

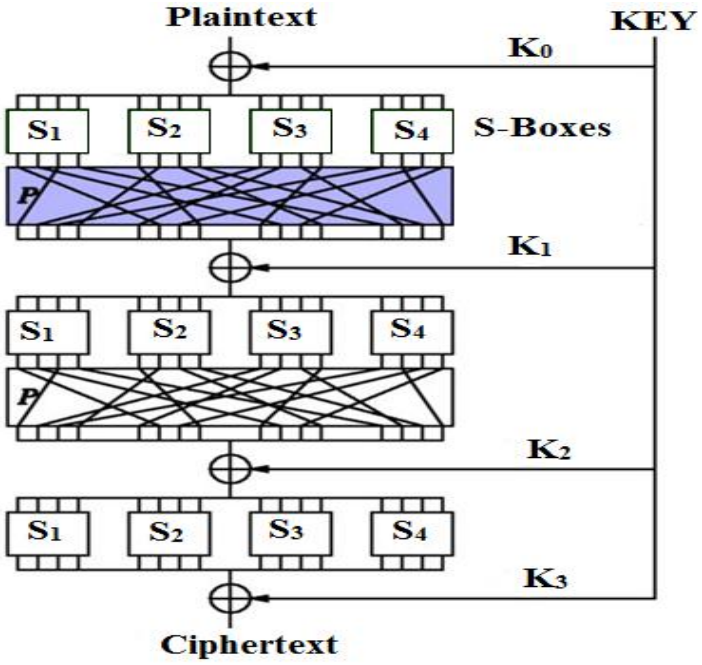

Figure 1.10 Substitution/Permutation Block Ciphers

- Feistel Block Ciphers: In this, original data block is partitioned into two parts, L (Left half) and R (Right half) for each round. In each round, encrypting function 'F' that depends on right half and encryption key is applied on left half while the right half remain unchanged. Then, XORing of output F (K, R) is done with the left half. Then, at the end of each step, permutation step swaps the modified L and unmodified R. So, for the next round R will become L of the current round and vice-versa. These substitution and permutation stages form rounds which are specified by the algorithm design. Huge amount of Confusion and diffusion is created by feistel cipher as it combines components of permutation, key expansion and substitution. The main advantage of feistel cipher is that the encryption and decryption process are similar. Feistel network are shown in figure 1.11.

  Examples of Block Ciphers: PRESENT, SIMON, SPECK, AES, BLOWFISH

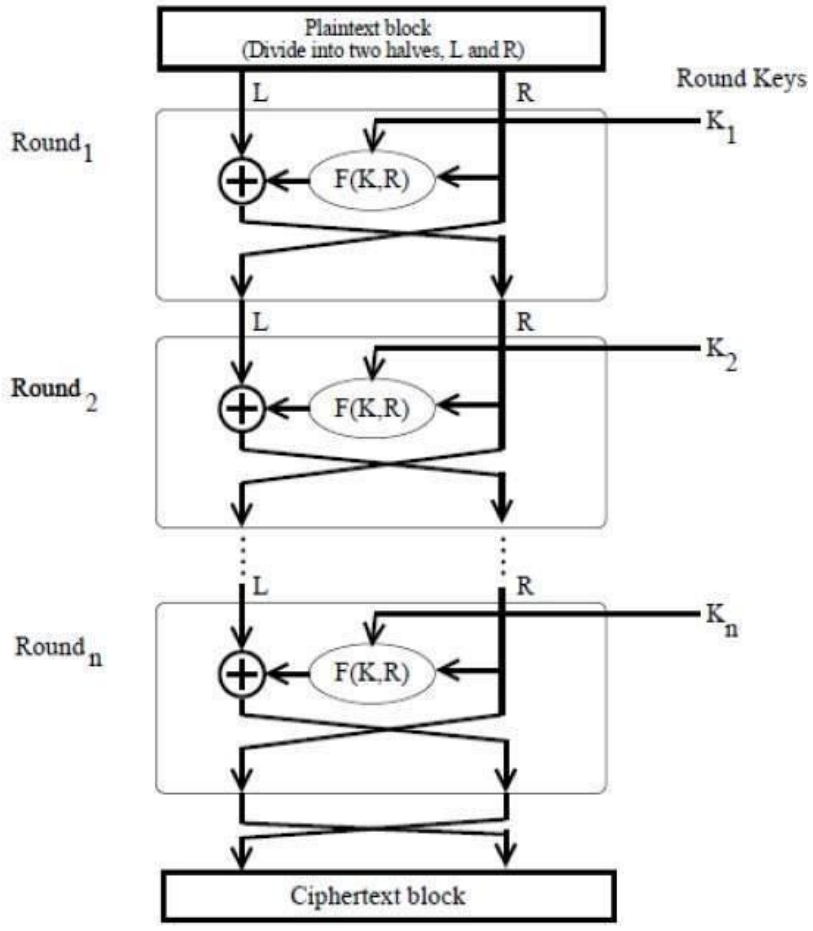

Figure 1.11 Feistel block ciphers

Table 1.3 Advantages and disadvantages of block cipher

Advantages of block ciphers	Disadvantages of block ciphers
Block ciphers provide integrity and confidentiality requirements.	As block ciphers work on data block as a group and can also get "carry over" from the preceding block so more memory is required.
Provide immunity to tampering.	Encryption of whole data block at a time makes it more susceptible to noise in transmission.

In VANETs, Symmetric as well as Asymmetric algorithms are used for both security and authentication purpose as shown in figure 1.12.

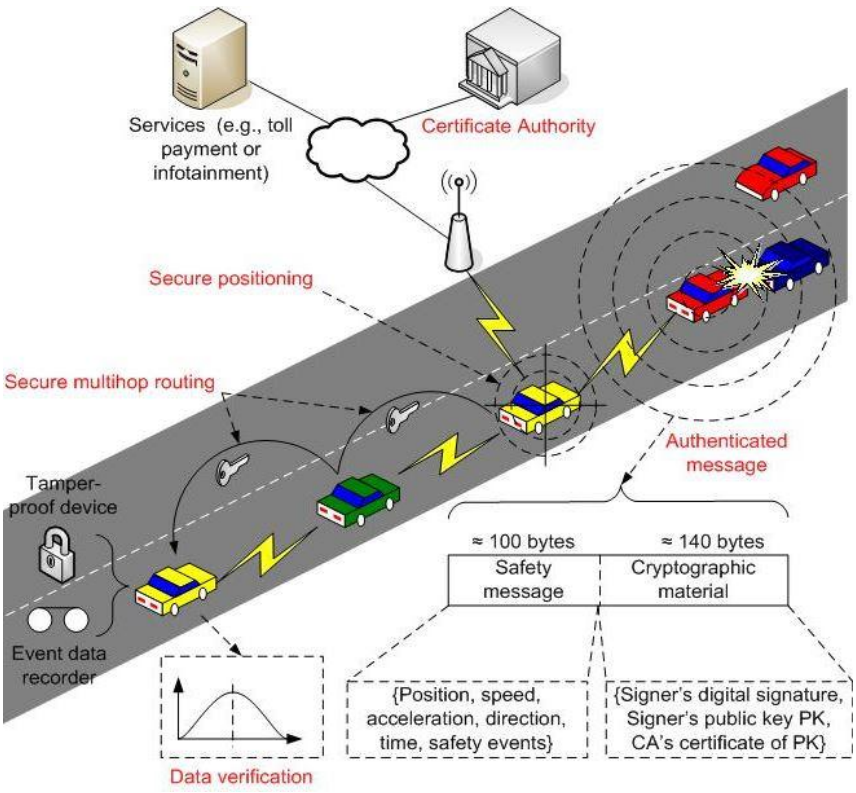

Figure 1.12 VANET architecture for both security and authentication

1.4 ORGANISATION OF DISSERTATION

The main aim of dissertation is to design a hybrid of encryption and authentication algorithms for VANET security. In order to achieve this, dissertation is divided into five chapters.

Chapter 1: Introduction

This chapter starts with the overview of wireless networks. After that overview of VANETs, architecture of VANETs, security requirements in VANETs, attacks in VANETs has been explained. A brief introduction overview of cryptography, cryptography types and cryptography ciphers has also been included in this chapter.

Chapter 2: Literature Survey

Work done by various researchers in the field of cryptographic algorithm has been included in this chapter.

Chapter 3: Problem Formulation and Objectives

This chapter embraces problem formulation from literature survey and from the various observations, objective has been defined.

Chapter 4: Overview of encryption and authentication algorithms for VANETs

This chapter includes overview of encryption and authentication algorithm. After that comparison between original algorithm and proposed approach has been done.

Chapter 5: Hardware Results

Simulation and hardware results have been summarized in this chapter using Vivado 2016.2 tool and BASYS3 board.

Chapter 6: Conclusion and future scope

This chapter sums up the conclusion of the work and suggests some ideas for future endeavours.

CHAPTER 2
LITERATURE SURVEY

Cryptography has been undergone a large amount of research in recent times. Several papers on cryptography, VANET security and their attacks have been studied. They are followed by the study of hardware implementation of cryptographic algorithm. The following section gives a brief review of studied literature.

Akhilesh Singh, *et al.* [1] investigated that VANET, which is an infrastructure less network offers intensification in approaches which relates to safety as well as contentment while driving. Safety and traffic analysis information is shared by vehicles using VANET. Because of the contemporary advances in expertise and growth of smart cities worldwide, scope of VANETs application has increased. According to them, VANET offer a self aware scheme which has considerable impact in augmentation services of traffic as well as in abbreviating road mishaps. Data which is distributed in this scheme is sensitive to time along with desires for tough as well as rapid forming network links. VANET which is a wireless ad-hoc network delivers this function totally but is decumbent to attacks on security.

Qiong Yang *et al.* [3] presented a design along with implementation of the OBU in the VANET for highways, and apprehends V2V communication. OBU includes four parts i.e. GPS module, wireless communication module, Central control module (CCM), and human-machine interface module. In this, ARM11-based embedded development platform, DCMA-86P2 module, and a GPS module are hardware platforms. Embedded Linux operating system is the software platform. After testing, results showed that implemented OBU can send as well as receive data for safety assist driving, along with realization of all the required functions and can work firmly.

VANET networks enhances traffic management and safety because of envision of numerous new applications. In this paper, authors **Arturo Ribagorda *et al.* [5]** proposed that traditional security methods are not acceptable all the time because of various exclusive characteristics of VANETs i.e. high mobility of nodes, geographic extension etc. They described and analyzed the most adumbrative VANET security developments in this paper.

VANETs can increase security and traffic optimization. In this paper, **Indu Bhardwaj *et al.* [6]** stated that VANETs are eminent type of MANETs. In VANET, wireless gadget transmits data to vehicles in close proximity, as well as messages can be send from one to another vehicle. In addition to these advantages, there are some important and prominent issues in

VANETS. Security issue is one of them. This paper proposed a analysis of necessities of security, attacks and confronts in security to execute security procedures in the VANETs.

Ahmed Shoeb Al Hasan, *et al.* [2] proposed a modern kind of MANET known as VANET that permits smart transport scheme to offer security of roads and diminish traffic jam via V2V communication or V2I communication. Nonetheless, major worry for researchers in VANETs is security issues. Dynamic topology and mixed structural design in VANETs make them diverse from other ad-hoc networks. Hence, conniving security methods to validate broadcasted messages and remove pernicious messages are pivotal in VANETs.

Lu Chen *et al.* [8] surveyed a novel kind of Ad hoc i.e. VANET. It is generally employed in ITS, which contain several features as topological structure, fast moving nodes, easily divided networks and frequently changing. Hence, routing protocol design ought to be completely acknowledged these features by means of much node data so as to convey a great dispute to the security of VANET.

Ghassan Samara *et al.* [9] presented that the awareness of these days research efforts is mainly towards security of VANET, while inclusive resolutions to shield the network from opponent and attacks still require to be enhanced, demanding to attain a satisfactory level, for the driver to attain protection of life and advertorial. They addressed many challenges that VANET are facing and also conferred a set of resolutions offered for these threats and troubles.

In this paper authors compared NS-2 and their own simulator. **Jason J. *et al.*[10]** represented that in simulation of VANETs, we use input traces of vehicle movements which are spawned by simulators of traffic that are based on models of traffic theory. They had expanded a novel VANET simulator that has the capability to handle a lot of additional vehicles than NS-2. They demonstrated outcomes of a cross-validation among NS-2 and their simulator and showed that both simulators generate statistically same outcomes. They proposed authentication method that depends on ECDSA signatures to analyze the proposed authentication and compared using TESLA to broadcast authentication. Each authentication scheme showed strength and weakness in terms of resulting reception rates and latency of broadcast packets.

GPS spoofing is a major threat to upcoming VANET technologies. **Asif Ali Wagan, *et al.* [11]** studied that till then, no one paid attention towards attacks on time synchronization. Thus, they did a study of the attack potential on VANET realizations in glance to spoofed time information. Thereby, they showed that this type of attack permits for brutal refusal of service attacks. Furthermore, via offering the feasibility to misuse authentication features, one

can infringe the non-repudiation feature of the security scheme. Moreover, sybil attack can be realized and consistency of the fundamental data sets of time along with position within VANET messages is extremely doubtful by taking into account the outlined attacks.

Qingzi Liu *et al.* [12] represented that nowadays scholars are paying more attention towards VANET security. In VANET, civil life along with property security is certainly shielded barely when both security and transportation are assured. They validated that architecture of security system act as a protective guard against overall hazards by starring the urgency and complicacy in resolving the worry of VANET by the system. The hierarchical framework of VANET Security System Architecture is considerably worried on, as the entire secure surroundings in VANET relies on bilateral synchronization of self-accomplishment in every hierarchy and mutual support for one another. Core technology applicable in every hierarchy for VANET is recognized and prospect breach for applicable research is exposed.

Charalampos Manifavas *et al.* [18] emphasized on study of lightweight stream ciphers for the embedded devices. Development and research of Lightweight cryptographic mechanisms is because of the need of lower production costs and bounded resources of embedded devices. Symmetric key cryptosystems mainly include block ciphers which perform well in embedded devices. Nonetheless, stream ciphers are pertinent in ubiquitous computing applications as well. In this paper, standardized stream cipher designs including authenticated encryption schemes has been analyzed. Benchmark analysis of AES-CTR, the Enocoro, Salsa-20, HC, Acorn and WG-8 ciphers on hardware platforms and software platforms that may possibly be found in the framework of ubiquitous computing has also been performed.

Alippi, Cesare *et al.* [19] focused on designs and techniques attempts to provide security property in resource constrained devices and because of this security property, lightweight cryptography is a hastily growing research field nowadays. On the other hand, need of lightweight cryptography also arises from crucial pervading IT applications, where solution complexity is drastically limit by cost and energy constraints, with the repercussion that implementation of traditional cryptography solutions become too costly. There are some recommendations suggested in the paper that to satisfy the hardware constraints, standard security algorithms should be entrenched in small devices and for the dedicated hardware, navel solution should be considered.

Panasayya Yalla *et al.* [20] worked on lightweight implementations of algorithms used in cryptography i.e. HIGHT and PRESNT for Field Programmable gate arrays. In this paper, implementation of HIGHT on FPGA use 117 slices and PRESENT use 91 slices only which are less than half the size of the Advanced Encryption Standard algorithm implementation

(without using block Random Access Memories). Throughput over area ratio of PRESENT is 240 Kbps per slice i.e. similar to that of the AES algorithm and conversely HIGHT smashed them by far with 720 Kbps per slice. In addition, optimization techniques for lightweight implementations have also been introduced in this paper.

Oussama Mohamed Reda *et al.* [21] proposed a resolution to secure the protocol used for routing i.e. GPSR for VANETs. Addition of digital signature (generated by using the symmetric cryptography algorithm AES and MD5 hash function) on the GPSR routing packet is done to provide protection against intrusions. In VANETs, intrusion detection system (IDS) can also be implemented to detect any infringement in security property.

Message Prioritization and data broadcasting plays a chief role in VANETs. **M. Selvi *et al.* [22]** proposed signcryption technique which is based on blowfish algorithm to secure the transmission of information in VANETs. Transmission of information in VANETs includes traffic jam, methods of emergency brake, condition of roads, warnings for accidents, and conditions of bad weather. Misbehaviors and false thwarting are serious issues in VANETs. False thwarting can be identified through Message Prioritization technique and secure transmission of messages can be done under Sybil and Denial of Service attacks by proposed technique.

Kalkundri Ravi *et al.* [23] worked on ECDSA to offer an efficient message authentication proposal. To provide road safety, traffic management and commercial broadcasting for drivers as well as passengers, a network scenario by VANETs is offered. Appropriate security and privacy techniques are required for vehicle-to-vehicle communication and vehicle-to-roadside communication. For the integrity of messages, authentication is required as the messages security is crucial in VANETs. Hybrid of P2P, VANET and ECDSA is more efficient and execute well in message delivery process.

Ray Beaulieu *et al.* [24] outlined the objectives in cryptographic design and how these objectives were balanced in the SIMON and the SPECK designs. Simplicity, security and flexibility are ceaseless yet contradictory goals in cryptographic design**.** To provide security in resource constrained devices and to provide simplicity of design**,** the Simon and the Speck families of the block ciphers were proposed. Nonetheless, the premeditated used cases are miscellaneous and require flexibility in implementation.

Ray Beaulieu *et al.* [25] summarized the cryptographic algorithms**,** their design rationale, along with current cryptanalysis and implementation. The Simon and the Speck families of block ciphers were developed in U.S. by NSA to provide security in constrained environments. In addition to simplicity in implementation of design of these algorithms on

FPGA, ASIC, microcontroller, and microprocessor, they also provide flexibility. Simplicity enables relatively cheap side-channel mitigations, and makes the algorithms attractive for unanticipated uses. Different block and key sizes in these algorithms allow the cryptography to be specifically tuned to an especial application.

Aydin Aysu *et al.* [26] discussed a low-cost alternative of the AES on reconfigurable platforms. On the basis of results, the SIMON is 86% compact than the AES, 70% compact than the PRESENT and having equivalent security. This paper dissipates a new architecture of SIMON known as bit-serialized architecture which is even more compact than the stream ciphers and extensively reduces the cost. As a result, the SIMON is a vigorous substitute to AES for the low cost Field programmable gate array based applications.

Soheil Feizi *et al.* [27] emphasized on hardware implementation of SIMON algorithm. Authentication, confidentiality, security and privacy are the major requirements during information exchange. The American NSA introduced a new block cipher family known as the SIMON in June 2013 which provide flexibility and security properties and perform extraordinarily well in lightweight applications. Selection of size of data and key lengths for various applications and environments can be done due to flexibility property. In this paper SIMON32/64 algorithm based on FPGA hardware has been described. Successful implementation of the Simon32/64 block cipher using the Xilinx ISE development tools on the Field-programmable gate array model Virtex-5 XC5VFX200T yields utilization of 177 LUTs which make it appropriate for different applications in lightweight cryptography and also in embedded systems.

Ege Gulcan *et al.* [28] proposed architecture of the SIMON block cipher which provides flexibility and compactness**.** The SIMON is a substitute of AES for the resource constrained platforms but the implementation results of proposed architecture showed that the SIMON is even more compact than the other block ciphers. All ten configurations of SIMON can be implemented by this architecture. Successful implementation of this architecture on Spartan-3 FPGAs yields 90 slices and on Spartan-6 FPGAs yields 32 slices and in comparison to other block ciphers these area results are smaller with same security level. But the drawback of this proposed algorithm is that it cannot be used in an adaptive security protocol.

Yasmin Alkady *et al.* [43] proposed a hybrid of symmetric as well as asymmetric key which offer high security and having reduce maintenance of key. Security levels are offered by symmetric and asymmetric encryption methods but they have many drawbacks. Symmetric encryption procedures faced problem in maintenance of key and asymmetric encryption methods faced problem at security level but in these maintenance of key is easy. So, the hybrid

of symmetric as well as asymmetric algorithms offer three fundamental requirements of cryptography i.e. confidentiality, authentication and integrity. Combination of ECC and AES offers encryption of nodes. RSA algorithm offers authentication and MD5 offers integrity. Their hybrid outcome offers better performance in terms of ciphertext size and computation time.

The comparative analysis is done on the basis of security algorithms used for VANET security as shown in table 2.1. The comparative analysis is done on the basis of technique used, which attacks covered and limitation of their techniques.

Table 2.1 Comparative Analysis of Security Algorithms for VANETs

Authors	Title	Techniques /technology used	Attacks Covered/ Security dimensions	Limitations of used technology
Akhilesh Singh, *et al.*[1] (2016)	VANET security: Issues, challenges and solutions	Symmetric cryptography, digital signature, hash function, elliptical curve parameter and ID registration technique	Replay attack, DOS, Routing attack, , fake information attacks	-----
Arturo Ribagorda, *et al.*[5] (2010)	Overview of security issues in vehicular ad-hoc networks	Vehicular public key infrastructure, certificate validation, attribute- based encryption, plausibility check mechanisms	Eavesdropping, Identity revealing, Location tracking, DOS attack	These techniques hadn't addressed the issues on privacy problems due to radio frequency fingerprinting.

Shiang-Feng Tzeng, *et al.* [29] (2015)	Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET	System initialization, anonymous identity generation, message signing, and message verification.	Forgery attack	Effective solution for forgery attacks only. No solution for other attacks.
Lu Chen, *et al.*[8] (2013)	Analysis of VANET security based on routing protocol information	Elliptic curve algorithm, digital signature technology, Intrusion Detection	Integrity, reliability and confidentiality	------
Asif Ali Wagan, *et al.*[11] (2015)	Emerging attacks on VANET security based on GPS Time Spoofing	Prevention of Time Stamp Jumps, short lived pseudonym certificates and retrospective attack detection via logging.	Denial of service attacks, sybil attack	No solution for other attacks.
Ahmed Shoeb Al Hasan, *et al.*[2] (2016)	Security threats in vehicular ad hoc networks	Public Key, Symmetric and Hybrid, Certificate Revocation , ID-based Cryptography	Privacy and security	Good privacy schemes with reduced overhead but no solution for attacks.
Ghassan Samara, *et al.*[7] (2010)	Security Analysis of	Vehicular Public Key	DOS attack, Fabrication	

	Vehicular Ad-Hoc Network (VANETs)	Infrastructure, group signature, Certificate Authority, ECC,	attack, alteration attack, replay attack, message	-------
Ram Shringar Raw, *et al.*[13] (2013)	Security challenges, issues and their solutions on VANETs	ARAN, SEAD, SMT (Secure Message Transmission), NDM (Non-Disclosure Method), ARIADNE	Replay Attack, Impersonation, False Warning, information disclosure, DOS, routing attack, resource consumption, location tracking effect	Efficient solution for privacy and authentication requirements but no solution for confidentiality.

Basis on the survey, comparative analysis of lightweight cryptography algorithms is done in table 2.2 on the basis of key size, block size, number of rounds, gate equivalents, and throughput.

Table 2.2 Comparative analysis of lightweight cryptography algorithms

Cipher	Key size	Block size	Number of Rounds	Gate equivalents	Throughput (kbps)
AES [30]	128	128	10	3100	72
	192		12	----	----
	256		14	----	----
PRESENT	80	64	32	1570	200
	128			1884	
CLEFIA [30]	128	128	18	4950	356
	192		22	----	----
	256		26	----	----

SIMON [25]	64	32	32	----	----
	72/96	48	36	----/739	----/5.0
	96/128	64	42/44	809/ 958	4.4/ 4.2
	96/144	96	52/54	955/ ----	3.7/----
	128/192/256	128	68/69/72	1234/ ----/ ----	2.9/----/ ----
SPECK [25]	64	32	22	----	----
	72/96	48	22/23	----/794	----/ 4.0
	96/128	64	26/27	860/ 996	3.6/3.6
	96/144	96	28/29	1012/ ----	3.4/----
	128/192/256	128	32/33/34	1280/ ----/ ----	3.0/----/----
HIGHT	128	64	32	3048	188.20
DES	56	64	16	2309	44.40
BLOWFISH [31]	At most 448	64	16	13000	----

CHAPTER 3

PROBLEM FORMULATION AND OBJECTIVES

3.1 PROBLEM FORMULATION

From the literature survey the authors **Oussama Mohamed Reda *et al.* [21]** and **M. Selvi *et al.* [22]** worked on conventional algorithms "AES and the Blowfish" symmetric algorithms which are used for data security but due to huge consumption of gate equivalents in AES and blowfish as shown in table 2.2, these algorithms are not suitable to use in highly constrained devices. So, instead of these algorithms lightweight algorithms "PRESENT and CLEFIA" can be preferred but still there is a huge consumption of gate equivalents in these algorithms as shown in table 2.2. Therefore, these algorithms are also not suitable to use in highly constrained devices. According to NIST report, the SIMON family of ultra-lightweight block cipher acts as an aid for securing applications in very constrained environments. So, for data security SIMON can be used in place of other algorithms.

The Authors **Kalkundri Ravi *et al.* [23] and Yasmin Alkady et al. [43]** also worked on the ECC and RSA asymmetric algorithms which are used for data authentication. In these algorithms, power consumption and memory requirements are high because these algorithms operation includes multiplication of large numbers. So, our one research direction is how to multiply two numbers such that area utilization becomes minimized and fast execution.

So, to provide security and authentication in VANETs, a hybrid of encryption and authentication algorithms is implemented.

3.2 OBJECTIVES

- Study of existing VANET architecture, attacks and cryptography algorithms.
- Study of ultra-lightweight SIMON algorithm and their different architecture and selection of round based architecture for VANET architecture.
- Design and Implementation of SIMON on Xilinx Vivado 2016.2 tool and on FPGA board BASYS3.
- Implementation of different multiplication approaches for multiply two numbers.
- Design of Optimized RSA algorithm for authentication purposes in VANET.
- Performance analysis of hybrid encryption and authentication algorithms based on LUT, Power, Throughput, Efficiency.

3.3 DESIGN METHODOLOGY

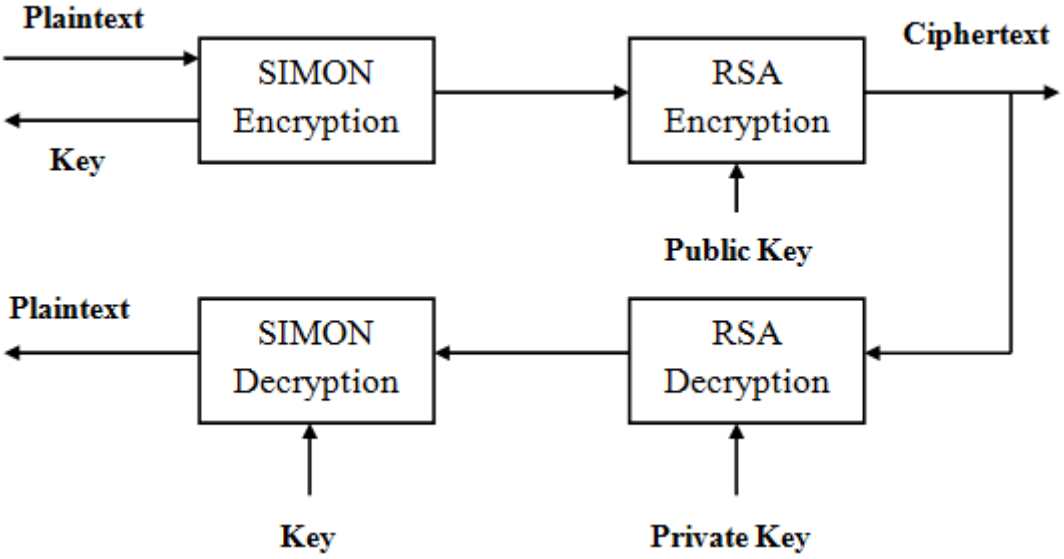

Figure 3.1 Design Methodology

CHAPTER 4
OVERVIEW OF ENCRYPTION AND AUTHENTICATION ALGORITHM FOR VANETS

The following section covers details of SIMON and RSA algorithm. First of all, operations of existing algorithm have been illustrated. Then various proposed revisions have been done to optimize or alter some of the operations to realize optimized hardware design. The proposed architecture is implemented in VHDL by using Vivado 2016.2 tool and the VHDL RTL codes are synthesized on BASYS3 FPGA board with a speed grade of -1.

4.1 SIMON ALGORITHM

A group of researchers from US National Security Agency (NSA) designed a family of the SIMON and the SPECK block ciphers in June 2013 which provide flexibility and security properties and perform extraordinarily well in lightweight applications. SIMON is a feistel network and was designed to address security issues in resources constrained devices. To provide flexible level of security, SIMON has ten compositions for different block sizes and key sizes. Table 4.1 shows the different compositions of SIMON in which p represents the bit length of each word and known as word size, 2p represents block size, k represents key words and T represents rounds in feistel network

Table 4.1 Different Configurations of SIMON [33]

Block Size (2p)	Key _Size (kp)	Word_Size (p)	Key _Words (k)	Constant_ Sequence	Rounds (T)
32	64	16	4	P_0	32
48	72	24	3	P_0	36
	96		4	P_1	36
64	96	32	3	P_2	42
	128		4	P_3	44
96	96	48	2	P_2	52
	144		3	P_3	54

128	128	64	2	P_2	68
	192		3	P_3	69
	256		4	P_4	72

SIMON algorithm involves two steps: Round Function and Key Scheduling

- Round Function: Figure 4.1 demonstrates the round function for ten configurations of algorithm SIMON. Round function of algorithm SIMON is feistel network. A_{upper} stands for upper words (most significant words) of the block and A_{lower} stands for lower words (least significant words) of block and each are of p-bits. The round function utilizes bit-wise AND, bit-wise XOR, and circular shift by left operations. For each round, circular left shift and bit-wise AND operations are carried out on the most significant words and then the XORing of the result is done with the least significant words and then with the round_key. Then the resultant value on the lower words is transferred to upper words and the upper words are transferred to lower words and this process will run continually until the completion of specified number of rounds is done [28].

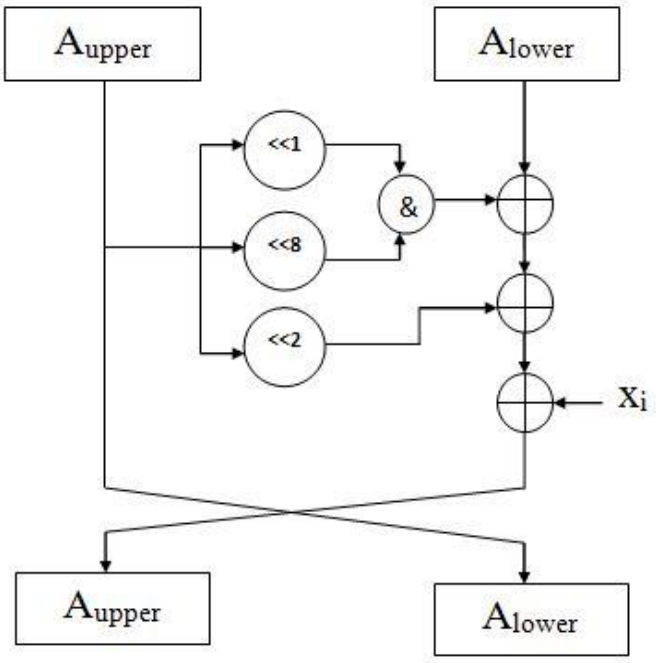

Figure 4.1 Round Function of SIMON

We can represent round function (used for encryption) as a two stage feistel map as:

$$R(L_1, R_1, x) = (F(L_1) \oplus R_1 \oplus x, L_1) \qquad \text{Equation}(4.1)$$

Where $F(L_1) = \left(S^1(L_1)\&S^8(L_1)\right)\oplus S^2(L_1)$, put this value in equation (4.1).

$$R(L_1, R_1, x) = \left(\left(S^1(L_1)\&S^8(L_1)\right)\oplus S^2(L_1)\oplus R_1\oplus x, L_1\right)$$

And its inverse (used for decryption) can be expressed as:

$$R^{-1}(L_1, R_1, x) = (R_1, F(R_1)\oplus L_1\oplus x) \qquad \text{Equation}(4.2)$$

Where $F(R_1) = \left(S^1(R_1)\&S^8(R_1)\right)\oplus S^2(R_1)$, put this value in equation (4.2).

$$R^{-1}(L_1, R_1, x) = \left(R_1, \left(S^1(R_1)\&S^8(R_1)\right)\oplus S^2(R_1)\oplus L_1\oplus x\right)$$

Where L_1 is leftmost word of given block, R_1 is the rightmost word of given block and x is round _key [33].

- Key Scheduling: Key scheduling function generates unique round keys for each round as the SIMON algorithm require exclusive round_keys for every round. In conflict to SIMON's round function, three different compositions of the key scheduling are present in this algorithm which depends on value of the k (key words) which can be 2, 3 and 4. Figure 4.2, 4.3, 4.4 represents the key scheduling for 3 distinctive key-lengths, corresponding to k=2, 3 or 4 respectively. X_m is the round key for the m^{th} round. For k = 2 and k = 3, the XOR and circular shift operations of the key scheduling are alike. For these, right circular shift by 3 and 4 is done on the most significant word, and then the XORing of the result is done on the least significant word and then with round constant p_i. For m = 4, right circular shift by 3 is done on the most significant word (x_{m+3}), then the XORing of result is done with x_{m+1}, then the right circular shift by 1 is done on result and XORing is done with the lower word and round_constant p_i. At the end of each key scheduling, upper word is replaced by new round_key, and right shifting by one word is done on all the words. As x_m is the key utilized in the existing round only so it will no longer be desirable and is overwritten. A sequence of 1 bit round_constants is also utilized in key scheduling to eliminate slide-properties and circular-shift symmetries. To make difference between ten configurations of SIMON, five different round constant sequences are used [28].

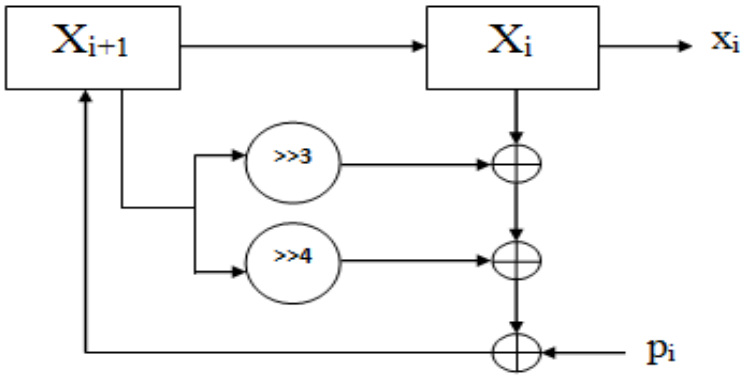

Figure 4.2 SIMON Key Scheduling for k=2

.

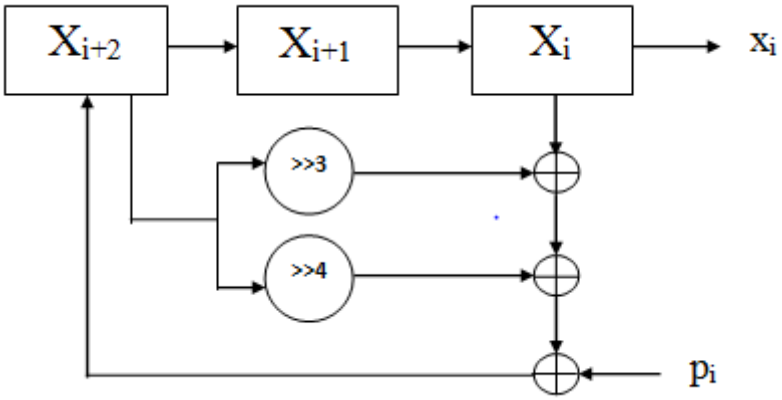

Figure 4.3 SIMON Key Scheduling for k=3

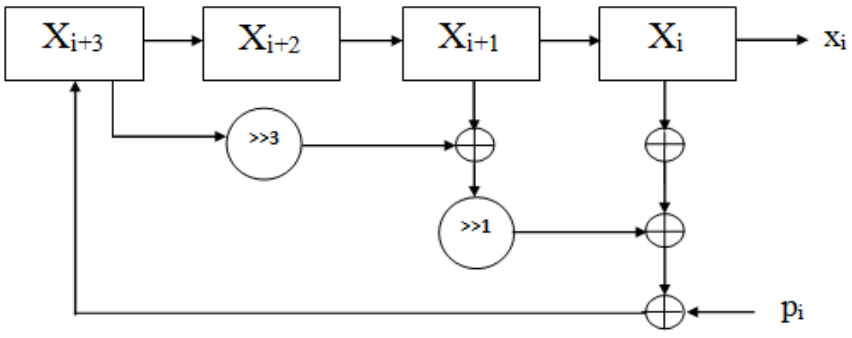

Figure 4.4 SIMON Key Scheduling for k=4

$$\text{LET } c = = 2^p - 4 \; = \; (2^p - 1) \oplus 3 = 0 \times \text{ff} \ldots \ldots . \text{fc}$$

For SIMON2p with k key words, T rounds and round sequence $p_{i,}$ round keys are generated by [27]:

For $0 < m < T- k$.

$$X_{i+k} = \begin{cases} c \oplus (p_i)_m \oplus x_m \oplus (I \oplus \phi^{-1})\, \phi^{-3} x_{m+1} & \text{if } k= 2, \\ c \oplus (p_i)_m \oplus x_m \oplus (I \oplus \phi^{-1})\, \phi^{-3} x_{m+2} & \text{if } k= 3, \\ c \oplus (p_i)_m \oplus x_m \oplus (I \oplus \phi^{-1})\, (\phi^{-3} x_{m+3} \oplus x_{m+1}) & \text{if } k=4, \end{cases}$$

Where ϕ^{-1} represents right circular shift by 1and ϕ^{-3} represents right circular shift by 3.

4.2 OVERVIEW of AUTHENTICATION ALGORITHMS

ECC and RSA algorithms can be used for authentication purpose. But these algorithms involve multiplication of two prime numbers which consume more power and memory. So, different approaches can be used for multiplication of two prime numbers:

4.2.1 RSA Algorithm

This algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1976 at MIT. It is an asymmetric algorithm and is based on number theory. Security of this algorithm depends on the complexity of the factorization of large prime numbers. This algorithm uses two different keys - public key and private key. Public key is used for encryption process and private key is used for decryption process. So, the advantage of RSA algorithm is to provide security by encrypting the data in such a way that only the authorized party can access the data.

Following parameters are used in RSA algorithm [36]:

1. prime numbers - a_1 and b_1 - Private
2. $s_1 = a_1 * b_1$ -Public
3. $\phi(c_1) = (a_1 - 1)(b_1 - 1)$ - Private
4. d_1 – Encryption key - Public
5. d_2 – Decryption key - Private
6. P- plaintext - Private
7. C – ciphertext- Public

➢ Steps Involved in RSA Algorithm:

Following three steps are involved in RSA algorithm:

- Key Generation: Following methods need to be followed to generate a key pair for encryption.

1. Opt any two random prime numbers, a_1 and b_1.

2. Compute $s_1 = a_1 * b_1$. Care must be taken that a_1 should not be equal to b_1. Because if p and q both are equal then $s_1 = a_1^2$ and then a_1 can be attained from square root of s_1.
3. Determine $\phi(s_1) = (a_1 - 1)(b_1 - 1)$.
4. Determine public key, d_1 which is comparatively prime with $\phi(s_1)$.
5. Generation of private key using equation d_1. $d_2 = 1 + h\phi(s_1)$. So, d_1 can be determine using this equation: $d_1 = 1 + h\phi(s_1) / d_2$, where h is an integer

- Encryption: Following methods need to be followed for encryption process.

1. Plaintext is structured into block p_1, p_2, ... such that value of each block must be in range from 0 to s_1-1.
2. Encryption of each block of plaintext p_i to block c_i is done with this equation:

$$c_i = p_i^{d_2} \bmod s_1 \qquad \text{Equation (4.3)}$$

- Decryption: Following methods need to be followed for decryption process.

1. Decryption of each block of ciphertext c_i to block p_i is done with this equation:

$$p_i = c_i^{d_1} \bmod s_1 \qquad \text{Equation(4.4)}$$

For $c_i = p_i^{d_2} \bmod s_1$

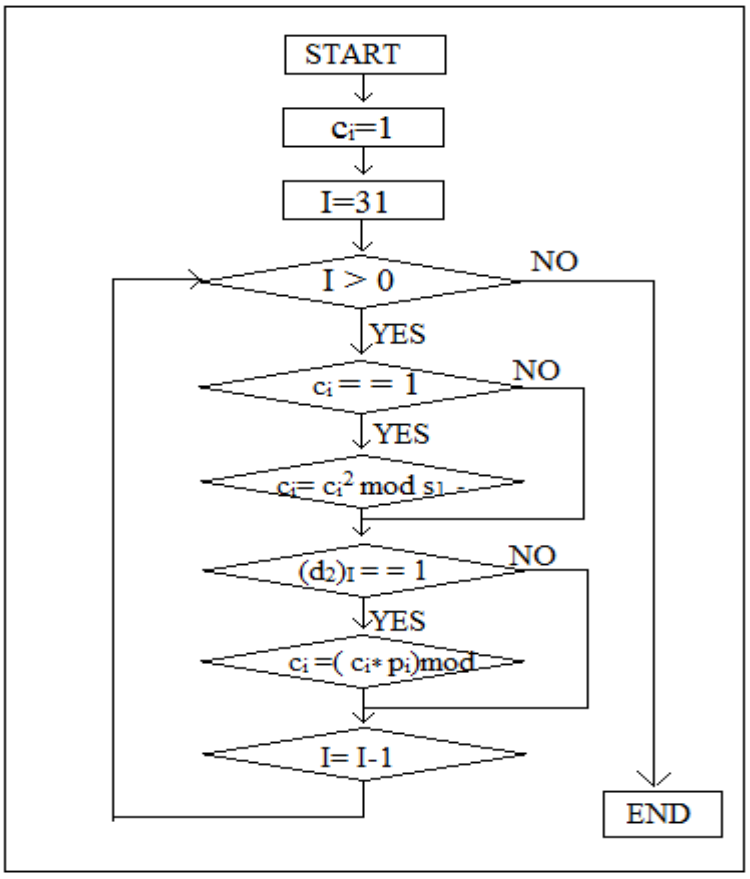

Figure 4.5Flow Chart for Encryption and Decryption of RSA [37]

4.2.2 ECC Algorithm

ECC was realized in 1985 by Neal Koblitz and Victor Miller. ECC take any cryptographic algorithm which is described over a random group and then group of rational points which are on elliptic curve are used over a finite field. Both ECC proposals and RSA proposals are public-key mechanisms and offer similar functionality. Multiplication, addition, inversion and subtraction operations of each point depend upon the finite field and chosen coordinate system. Generalized Weierstrass Equation of elliptic curves is [38]:

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

Computation of Elliptic curves can be compute over three fields:

- First one is over real numbers which are infinite as well as less accurate.
- Second is over prime field $GF(p)$ which is appropriate for implementations on software.
- Third is over binary field $GF(2^m)$ which is appropriate for implementations on hardware.

Example: Alice and Bob public keys are given by:

$$P_a = nAG$$

$$P_b = nBG$$

If Alice want to send message P_m to Bob, Alice uses Bob's public key to encrypt message the ciphertext is given by:

$$P_c = \{ kG, P_m + kP_b \}$$

Bob decrypts message by subtracting the coordinate of 'kG' multiplied by nB from '$P_m + k P_b$' and is given by:

$$P_m = \{P_m + k P_b - nBkG\}$$

4.2.3 Different Approaches of Multiplication

In cryptographic proposals, multiplication of large integer is an important module and one of the hindrances for many applications. RSA algorithm as well as ECC algorithm needs multiplication in many public key cryptosystems. So, for the secure online transmission, a hybrid of these algorithms is done with symmetric cryptosystems. So, following approaches can be used for multiplication:

- Shift and Add multiplication: In this algorithm, digits of multiplier are taken one at a time from right to left followed by multiplication of only one number of multiplier with the multiplicand. After then placement of intermediary product is done in the correct position to left of previous results. Large computation time is needed in this multiplication. As an example, consider the multiplication of two numbers 89 and 97, convert them into binary and then the normal multiplication of both numbers involves following steps:

89= 100010001 and 97=10010111

```
      10001001
    * 10010111
    ----------
      10001001
     10001001*
    10001001**
   00000000***
  10001001****
 00000000*****
00000000******
10001001*******
---------------
10100001 1001111
```

- VEDIC Multiplication

Vedic math is an antique approach of multiplying numbers that invented in India. It was applied to do mathematical computations more rapidly than usual [40].

Let assume 2 values: 89 and 97. As the value taken are of double digit so, subtract each value from 100.

For 89, the value become 100-89 i.e. 11

For 97, the value become 100-97 i.e. 3

Then place result of each value to right of original numbers

89	11
97	3

Multiply 11 and 3=11*3= 33, these are the last two digit of multiplication

Now, to get the first digits, subtraction along either of the diagonals is done. Any of the diagonal can be picked as both will give the same result.

i.e. 89-3= 86 or 97-11=86

then concatenate both values, which will become final result.

89 ↘	11	
97	3	So, final result= 8633
86	33	

- Karatsuba Multiplication

It was one of the foremost multiplication procedures that improve the multiplication method of different algorithms. This algorithm contains a series of additions along with shifts. Division of every integer multiplicand to 2 minor integers is done by this technique. Though, numerous intermediary values ought to be stored so additional storage of hardware is required in this algorithm [41].

Assume a and b be represented as n-digit strings in some base 'M'. p should be less than n, two given numbers can be written as:

a= 89, b=97, M=10, p=1

$$a = a_1 * M^P + a_0 \quad \text{Eq. (4.3)}$$

after putting value of a, M and p in equation 4.3, we get,

$$89 = 8 * 10^1 + 9 \quad \text{Eq. (4.4)}$$

$$b = b_1 * M^P + b_0 \quad \text{Eq. (4.5)}$$

after putting value of b, M and p in equation 4.5 , we get,

$$97 = 9 * 10^1 + 7 \quad \text{Eq. (4.6)}$$

Smaller integers are exploited to calculate 3 intermediate results:

$$x_2 = x_1 * y_1,\ x_1 = (x_1 + x_0) * (y_0 + y_1) - x_2 - x_0,\ x_0 = x_0 * y_0$$

So, $x_2 = 8 * 9 = 72$

$x_0 = 9 * 7 = 63$

$x_1 = (8 + 9) * (9 + 7) - x_2 - x_0 = 137$

Then the result of this multiplication is done by adding these 3 intermediate results and shifting is done accordingly.

$$\text{result} = x_2 * M^{2p} + x_1 * M^p + x_0 \quad \text{Eq. (4.8)}$$

After putting the value in equation (4.8), we get

$$\text{result} = 72 * 10^2 + 137 * 10^1 + 63 = 8633$$

CHAPTER 5
HARWARE IMPLEMENTATION RESULTS

This chapter mostly covers the details of FPGA implementation including tools and methodologies used. Various parameters of FPGA implementation like device utilization summary, simulation results and RTL diagrams have been included in the chapter.

5.1 IMPLEMENTATION PROCEDURE of SIMON ALGORITHM

- After through design of top level system architecture, which has been explained in chapter 4, design is needed to be converted in synthesizable code in any HDL (Verilog or VHDL). VHDL has been used for present design.
- Round–based Architecture of the SIMON algorithm has been implemented using on-the –fly key generation technique.
- Then different multiplication techniques are used to reduce the area utilization in ECC and RSA algorithms.
- Then the hybrid of the SIMON and RSA algorithm is done to provide both security and authentication in VANETs.
- All the results have been summarized and comparatively analyzed with the original results.

5.2 IMPLEMENTATION RESULTS of SIMON

Present design of SIMON has been developed using Vivado tool's version 2016.2. Target FPGA board utilized for the implementation is BASYS3. All of stages for Field-Programmable-Gate-Array implementation like synthesis, mapping, placement & routing and burning have been accomplished through Vivado tools with suitable constraints. Summary of the implementation has been given below:

5.2.1 Simulation Results for the Encryption Process of SIMON Algorithm

Key : ff ee dd cc bb aa 99 88 77 66 55 44 33 22 11 00
Block_input: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Block _output: c5 22 7f 3b c7 bf a8 1e 6f 23 ae b4 bd 12 38 34

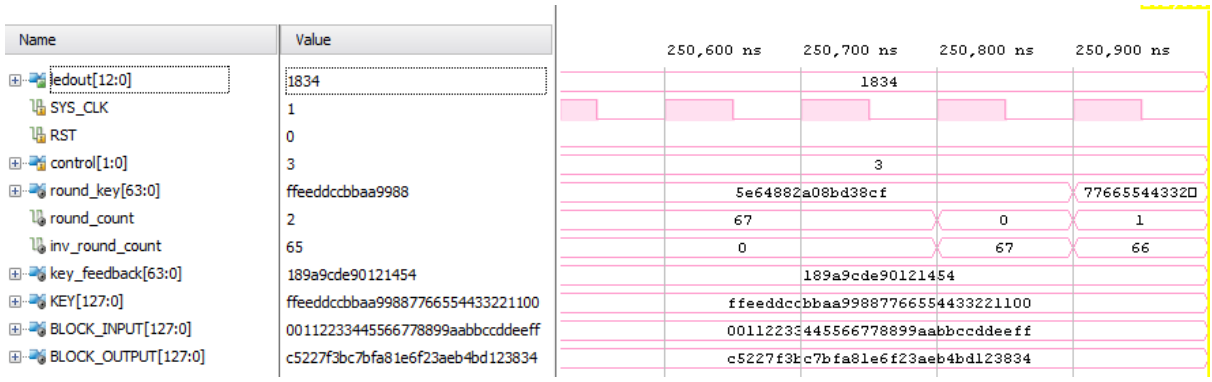

Figure 5.1 Simulation results for the encryption process of SIMON

5.2.2 Simulation Results for the Decryption process of SIMON Algorithm

Key : ff ee dd cc bb aa 99 88 77 66 55 44 33 22 11 00

Block_input: c5 22 7f 3b c7 bf a8 1e 6f 23 ae b4 bd 12 38 34

Block_output: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

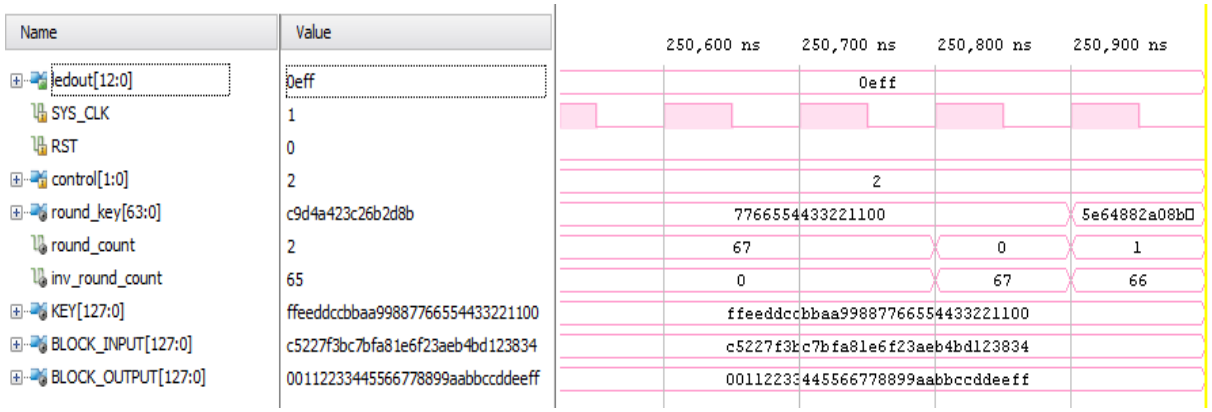

Figure 5.2 Simulation results for the decryption process of SIMON

5.2.3 RTL Diagram of SIMON Algorithm

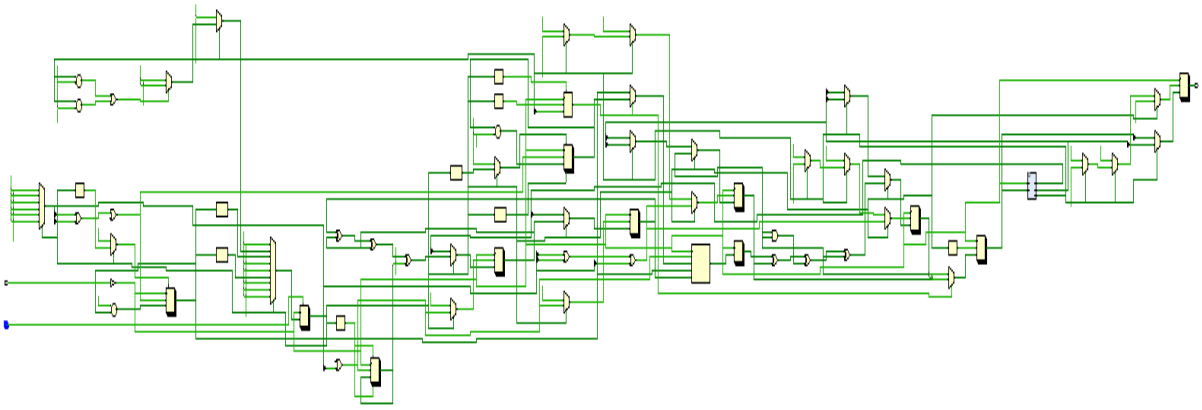

Figure 5.3 RTL diagram of SIMON

5.2.4 Hardware Results of SIMON

In this, two switches are used as CONTROL inputs which define whether encryption or decryption process will occur and one switch is used for RST. The output has been shown on the 13LED outputs of board.

- For Encryption:

Block_output: c5 22 7f 3b c7 bf a8 1e 6f 23 ae b4 bd 12 38 34

Led_output: 0010110000011(LSB to MSB of block_output)

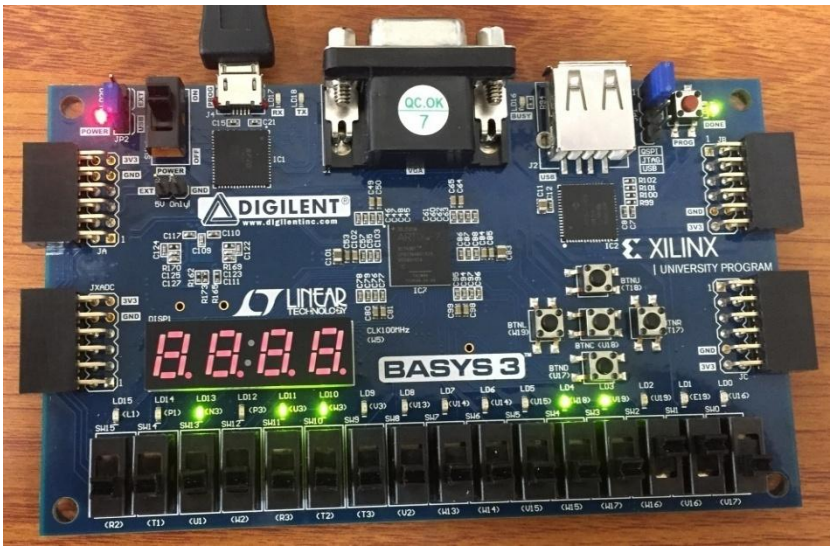

Figure 5.4 Hardware result for the encryption process of SIMON

- For Decryption:

Block_Output: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Led_output: 1111111101110 (LSB to MSB of block_output)

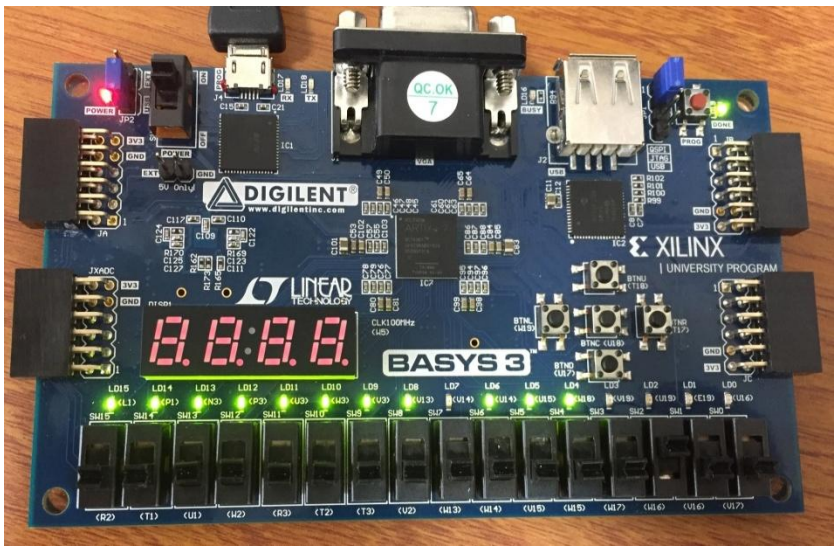

Figure 5.5 Hardware result for the decryption process of SIMON

5.2.5 Performance Parameters

- Throughput: Rate of generation of new outputs per unit time is called as throughput. Throughput can be measured by using formula [34].

$$\text{Throughput} = \frac{\text{Block size} * \text{frequency}}{\text{Clock cycles}}$$

- Efficiency: Ratio of throughput to area calculated at a determined clock frequency. It calculates the cost consumption occur for processing single ciphertext in terms of area and time [34].

$$\text{Efficiency} = \frac{\text{Throughput}}{\text{area}}$$

- Avalanche Effect: It means that for even a slight change in input i.e. even if one bit is flipped, there must be 50% change in output bits. Block cipher considered to have a poor randomization if a block cipher demonstrates less avalanche effect, thus a cryptanalyst can create calculations about the input, by knowing output only [35].

$$\text{Avalanche effect} = \frac{\text{Number of bits changed in ciphertext}}{\text{Total number of bits in ciphertext}}$$

- Correlation Factor: It is the measurement of relation between input and output values. Correlation factor basically describe the degree to which output data is associated with input data. For cryptography correlation factor must be less.

Table 5.1 Comparison of Implemented results of SIMON to existing results

Parameters	Existing Results of Serial architecture [26]	Existing results of Parallel architecture [42]	Implemented Results
Slices	36	799	315
Frequency(MHz)	136	135	135
Throughput(mbps)	3.6	392.4	216.8
Efficiency	0.1	0.49	0.68

The implemented design utilize less slices as compared to existing design because round based architecture using on-the-fly key generation (in which keys generated in parallel to data processing) technique has been used.

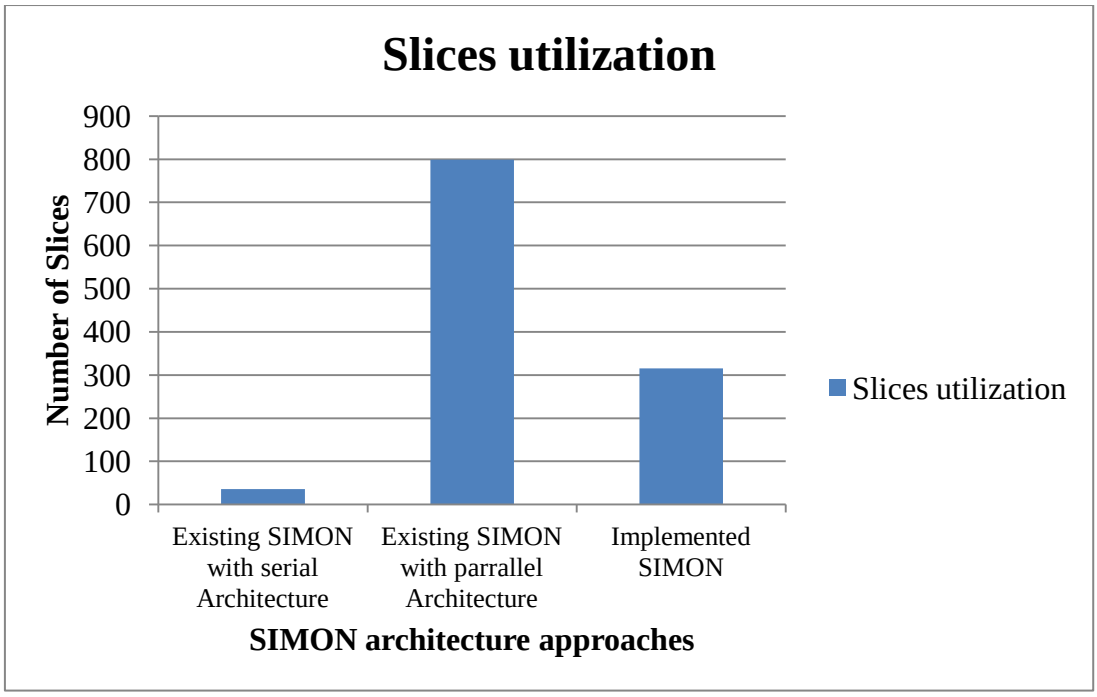

Figure 5.6 Number of Slices for various architecture approaches of SIMON

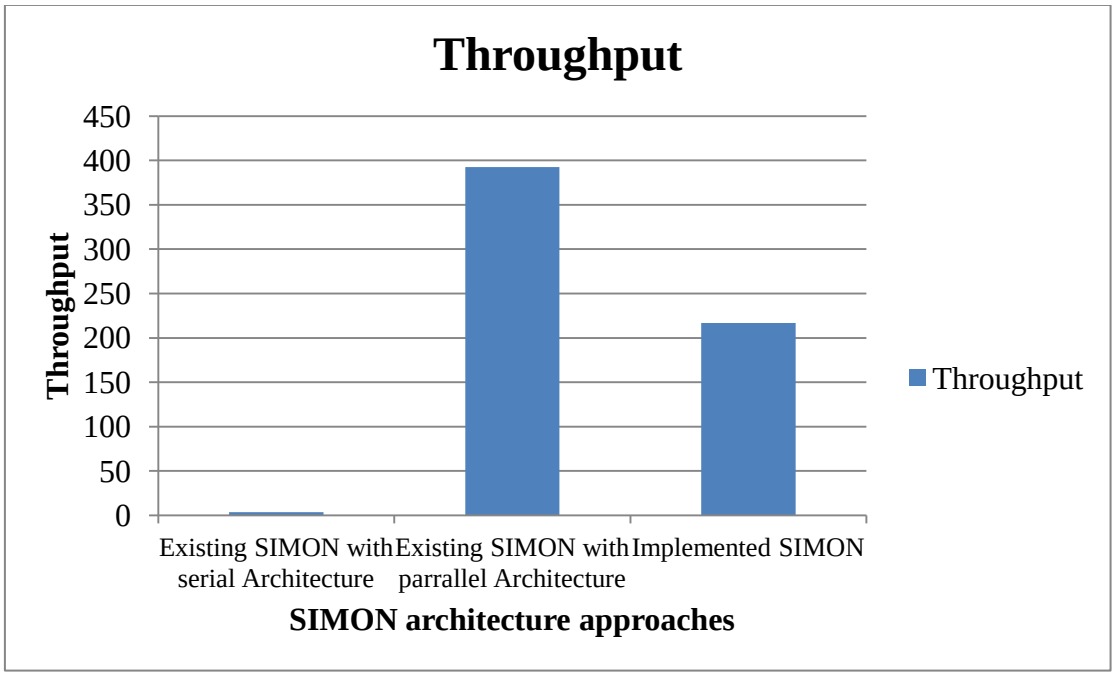

Figure 5.7 Throughput for various architecture approaches of SIMON

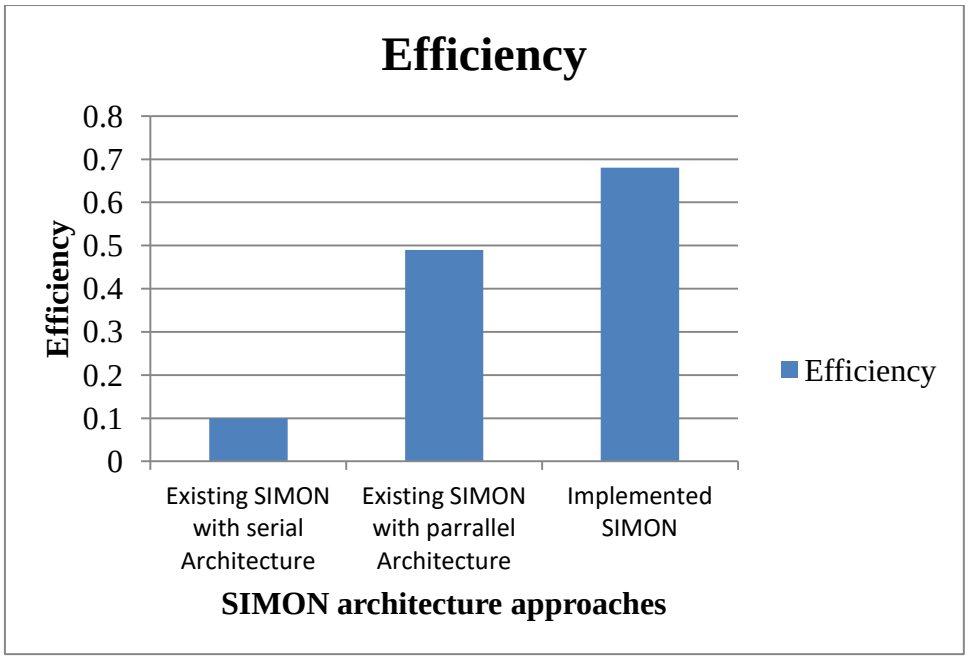

Figure 5.8 Efficiency of various architecture approaches of SIMON

The figure 5.6 shows the area consumption in terms of slices on FPGA BASYS3 board and shows that implemented design consumes 60% less area than existing parallel architecture of SIMON. Figure 5.7 shows the Throughput for various approaches of SIMON. Figure 5.8 shows the implemented design is 85% more efficient than existing serial architecture of SIMON.

5.3 IMPLEMENTATION RESULTS of DIFFERENT MULTIPLICATION TECHNIQUES USED in RSA ALGORITHM

Different multiplication techniques have been used to multiply two large integer numbers. Designs have been developed using Vivado tool's version 2016.2. Summary of the implementation has been given below:

5.3.1 Simulation Results of VEDIC Algorithm

a= 95 = 5f and b=97 = 61

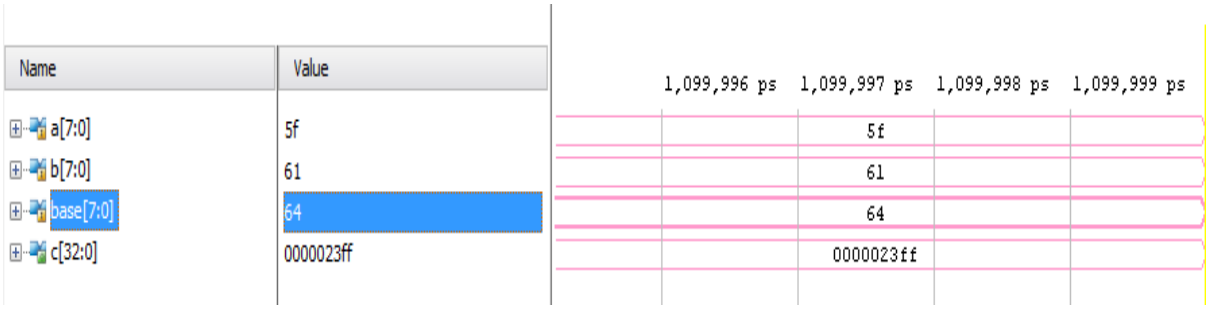

Figure 5.9 Simulation results of Vedic Algorithm

5.3.2 Simulation Results of Karatsuba Algorithm

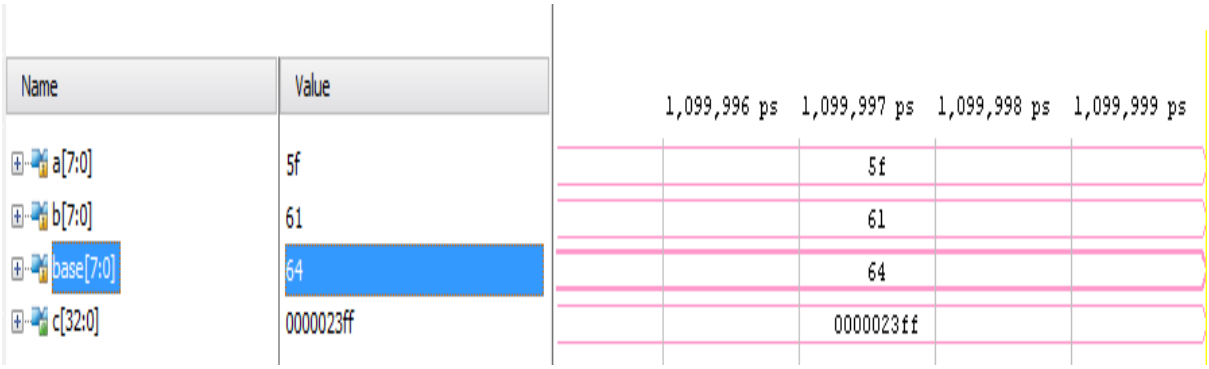

Figure 5.10 Simulation results of Karatsuba Algorithm

Table 5.2 Comparison of Look up tables for VEDIC algorithm and Karatsuba Algorithm

	Vedic Algorithm	Karatsuba Algorithm
LUTs	320	382

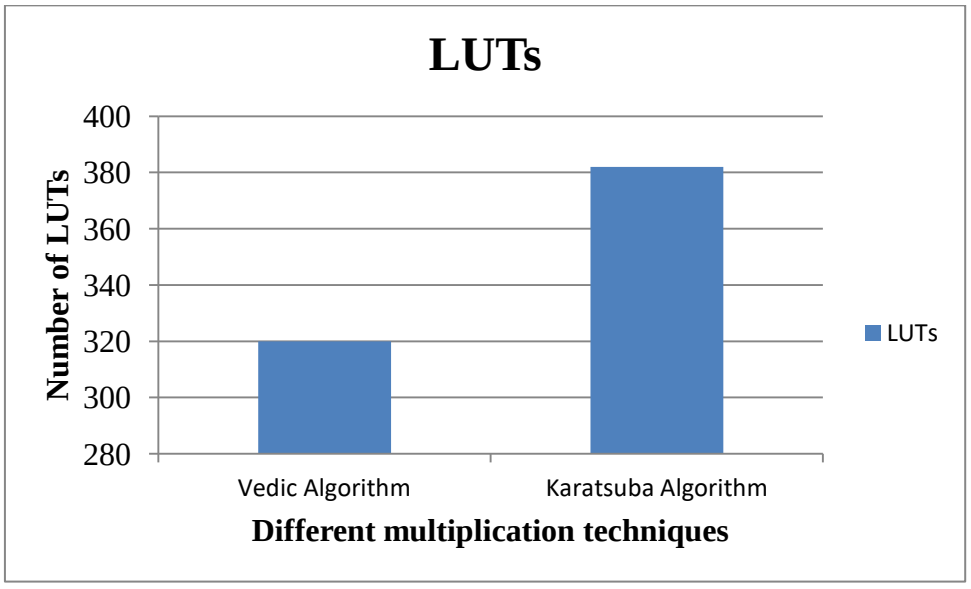

Figure 5.11 Number of LUTs used for different multiplication techniques

Figure 5.11 shows that Vedic algorithm consumes less area as compared to Karatsuba algorithm.

5.4 IMPLEMENTATION RESULTS of SIMON+RSA ALGORITHM

In VANETs, both security as well as authentication is required as shown in figure 1.12 above. So for security purpose SIMON has been chosen because of its ultra-lightweight property and for authentication purpose RSA has been chosen. Designs have been developed using Vivado tool's version 2016.2. Summary of the implementation has been given below:

Table 5.3 Comparison of Look up tables for SIMON+RSA Algorithm using Vedic algorithm and Karatsuba Algorithm

	SIMON+RSA algorithm using Vedic algorithm	SIMON+RSA algorithm using Karatsuba algorithm
LUTs	7810	8390

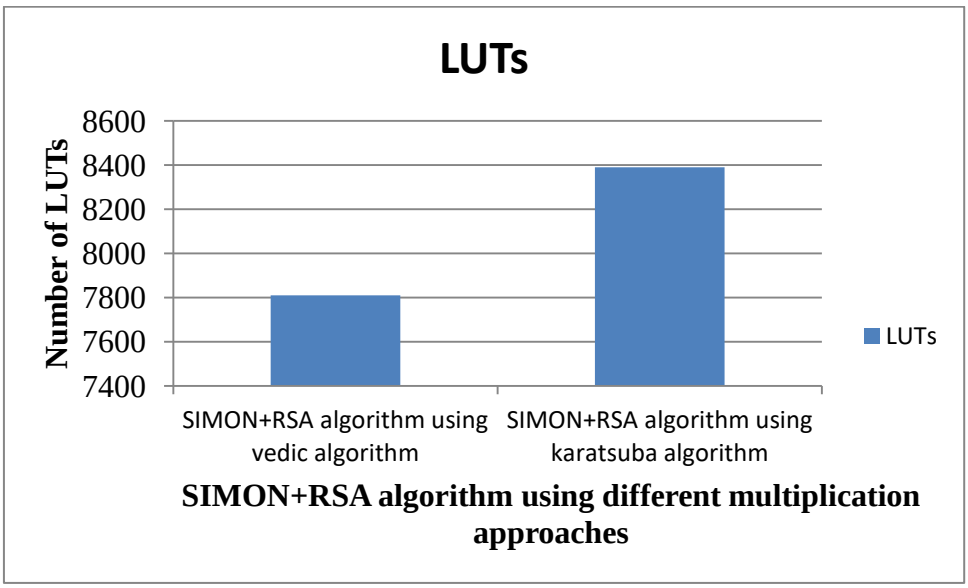

Figure 5.12 Number of LUTs used for SIMON+RSA algorithm using different multiplication techniques

Figure 5.12 shows that the SIMON+RSA algorithm using Vedic multiplier consume less area as compared to SIMON+RSA algorithm using Karatsuba algorithm.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

Wireless networks are usually a network of nodes that manage the environment which enable communication involving persons or computers as well as surrounding environment. One decentralized type of wireless networks is VANETs. VANETs are subgroups of MANETs which share information about road safety associated to traffic investigation, normal statistics like files, videos *etc* by means of continuous internet association to give intimation to driver to abstain 60%of the mishaps. But VANETs also faced some challenges in terms of security and authentication as VANETs is susceptible to many attacks such as DOS attack, Sybil attack, replay attack, routing attack, timing attack, eavesdropping *etc.* A survey on VANET's security and authentication attacks is done. From the survey, it has been concluded that cryptographic algorithms are used for data security and authentication process such as AES, Blowfish, ECC, RSA *etc*. But due to huge amount of consumption of memory, these algorithms are not suitable to use in resource-constrained devices. So, lightweight algorithms are used in resource constrained devices.

In this work, for data security NIST recommended ultra-lightweight cipher SIMON is studied and optimized at hardware level. Hardware implementation of SIMON algorithm is done using Xilinx Vivado 2016.2 tool on FPGA board of BASYS3. The performance analysis is done on the basis of slices utilization, throughput and efficiency. Optimized SIMON using on-the-fly key generation uses 60% less area than existing parallel architecture of SIMON and is 85% more efficient than existing serial architecture of SIMON. For data authentication, ECC and RSA algorithms require multiplication of large numbers. So, we have worked on different multiplication algorithms i.e. Vedic algorithm and Karatsuba algorithm to multiply numbers. From the Performance analysis based on LUTs, it is concluded that Vedic consumes less area as compared to Karatsuba. Then, a hybrid of security and authentication algorithm is implemented.

6.2 FUTURE WORK

Although VANETs cover a vast area of applications yet there are some issues. So some future directions are discussed to resolve these issues as follows:

- Till date, no mechanism which can alleviate the entire attacks or mainly eminent attacks on VANETs with only 1 solution. So, our research work is to eminent most of the eminent attacks with single approach.
- More multiplication techniques will be explored.

REFERENCES

[1] R. Mishra, A. Singh and R. Kumar, "VANET security: Issues, challenges and solutions", *International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 1050-1055, 2016.

[2] A.S. Al Hasan, Md. Shohrab Hossain, and M. Atiquzzaman, "Security threats in vehicular ad hoc networks." *Conference on Advances in Computing, Communications and Informatic*, pp. 21-24, Sept.2016.

[3] Yang, Qiong, Lin Wang, Weiwei Xia, Yi Wu, and Lianfeng Shen, "Development of on-board unit in vehicular ad-hoc network for highways", *International Conference on Connected Vehicles and Exp*, pp. 457-462, 2014.

[4] R. Barskar and M. Chawla , "Vehicular Ad hoc Networks and its Applications in Diversified Fields", *International Journal of Computer Applications*, vol.123, Jan. 2015.

[5] J. M. de Fuentes, A. I. Gonzalez-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks", *Handbook of Reseach on Mobility and Computing, IGI Global*, 2010.

[6] I. Bhardwaj and S. Khara, "An Analytic Study of Security Solutions for VANET", *International Journal of Computer Applications*, vol. 132 , no.10, Dec.2015.

[7] G. Samara , Al-Salihy, W. A. and R. Sures, "Security analysis of vehicular ad hoc networks (VANET)", *Second International Conference on Network Applications Protocols and Services* , pp. 55-60 , Sep. 2010

[8] L. Che , H. Tang, & J.Wang, "Analysis of VANET security based on routing protocol information", *Fourth International Conference on Intelligent Control and Information Processing*, pp. 134-138, June 2013.

[9] G. Samara, Al-Salihy, W. A. and S. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)", *4th International Conference on Trends in Information Science and Service Science*, pp. 393-398, May 2010.

[10] J. J Haas, Hu, Y. C. and K. P. Laberteaux, "Real-world VANET security protocol performance",*Conference on Global Telecommunications*, pp. 1-7, Nov. 2009.

[11] S. Bittl, A. A. Gonzalez, M. Myrtu, H. Beckmann, S. Sailer, and B. Eissfeller, "Emerging attacks on VANET security based on GPS Time Spoofing", *IEEE Conference on Communications and Network Security*, pp. 344-352, 2015.

[12] Q. Liu, Q.Wu, and L. Yong, "A hierarchical security architecture of VANET", *International Conference on Cyberspace Technology* ,pp. 6-10, Nov.2013.

[13] R.S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET", *International Journal of Network Security & Its Applications*, 2013.

[14] H. Jin and P. Papadimitratos, "Scaling VANET security through cooperative message verification", *IEEE conference on Vehicular* , pp. 275-278 , Dec. 2015.

[15] G. Yan, B. B. Bista, D. B Rawat and E. F Shaner ,"General active position detectors protect VANET security", *International Conference on Broadband and Wireless Computing, Communication and Applications* , pp. 11-17, Oct. 2011.

[16] Menezes, J. Alfred, and A. V. Scott," *Handbook of applied cryptography*", CRC press, 1996.

17] Tripathi, Ritu, and Sanjay Agrawal. "Comparative study of symmetric and asymmetric cryptography techniques." *International Journal of Advance Foundation and Research in Computer (IJAFRC)* vol.1 no.6, pp. 68-76, 2014.

[18] Manifavas and Charalampos, "A survey of lightweight stream ciphers for embedded systems." *Security and Communication Networks,* vol.9, no.10, pp.1226-1246, 2016.

[19] Alippi, Cesare, Andrey Bogdanov, and Francesco Regazzoni. "Lightweight cryptography for constrained devices.", *IEEE International Symposium on Integrated Circuits* , pp. 144-147, 2014.

[20] P. Yalla and J. P Kaps ,"Lightweight cryptography for FPGAs. In Reconfigurable Computing and FPGAs", International Conference on IEEE, pp. 225-230, 2009.

[21] Erritali, Mohammed, O. M. Reda, and B. E. Ouahidi. "A Contribution to Secure the Routing Protocol Greedy Perimeter Stateless Routing Using a Symmetric Signature-Based AES and MD5 Hash.",*arXiv preprint arXiv* ,pp. 1110.1579 ,2011.

[22] M. Selvi, and B. Ramakrishnan. "Prioritized and secured data dissemination technique in VANET based on optimal blowfish algorithm and signcryption method." ,*International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 4 pp. 165-172 ,2015.

[23] Ravi, Kalkundri, and S. A. Kulkarni. "A secure message authentication scheme for VANET using ECDSA." *Computing, Communications and Networking Technologies (ICCCNT) Fourth International Conference on. IEEE*, pp. 1-6, 2013.

[24] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, & L. Wingers, "The SIMON and SPECK lightweight block ciphers.", *In Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE* ,pp. 1-6 ,2015.

[25] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, & L. Wingers ,"SIMON and SPECK: Block Ciphers for the Internet of Things", *IACR Cryptology ePrint Archive*, pp. 585,2015.

[26] Aysu, Aydin, Ege Gulcan, and Patrick Schaumont. "SIMON says: Break area records of block ciphers on FPGAs.", *IEEE Embedded Systems Letters* vol. 6, no.2, pp.37-40, 2014.

[27] Feizi, Soheil, Arash Ahmadi, and Ali Nemati. "A hardware implementation of simon cryptography algorithm" *Computer and Knowledge Engineering (ICCKE), 2014 4th International eConference on. IEEE*, pp. 245-250, 2014.

[28] Gulcan, Ege, Aydin Aysu, and Patrick Schaumont,"A flexible and compact hardware architecture for the SIMON block cipher", *International Workshop on Lightweight Cryptography for Security and Privacy. Springer, Cham*, pp. 34-50, 2014.

[29] S. Horng, S. Tzeng and P. Huang "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET*," IEEE Transactions on Vehicular Technology,* 2015.

[30] Akishita, Toru, and Harunaga Hiwatari , "Very compact hardware implementations of the blockcipher CLEFIA",*International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg*, pp. 278-292, 2011.

[31] Lai, Yeong-Kang, and Yu-Chuan Shu. "VLSI architecture design and implementation for BLOWFISH block cipher with secure modes of operation." *Circuits and Systems, 2001. ISCAS 2001. The 2001 IEEE International Symposium on*. vol. 4, pp. 57-60, 2001.

[32] L. Nino, C. Andres, M. M.Sandoval, and A. D .Perez. "Novel FPGA-based low-cost hardware architecture for the PRESENT block cipher", *Digital System Design (DSD), 2016 Euromicro*

Conference on. IEEE, pp. 646-650, 2016.

[33] Wetzels, Jos, and Wouter Bokslag,"Simple SIMON: FPGA implementations of the SIMON 64/128 Block Cipher", arXiv preprint arXiv:1507.06368 (2015).

[34] Mohd, J. Bassam , Thaier Hayajneh, and V.V Athanasios,"A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues" ,*Journal of Network and Computer Applications* vol. 58, pp.73-93, 2015.

[35] Nejad, Farshid Hossein, S. Sabah, and A. J. Jam,"Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys" *Computational Science and Technology (ICCST), 2014 International Conference on. IEEE*, pp. 1-5, 2014.

[36] Iswari, Ni Made Satvika,"Key generation algorithm design combination of RSA and ElGamal algorithm",*Information Technology and Electrical Engineering (ICITEE), 2016 8th International Conference on. IEEE*, 2016.

[37] Mahajan, Prerna, and A. Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." *Global Journal of Computer Science and Technology* 2013.

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

[39] Imran, Malik, M. Kashif, and M. Rashid. "Hardware design and implementation of scalar multiplication in elliptic curve cryptography (ECC) over GF (2163) on FPGA." *Information and Communication Technologies (ICICT), 2015 International Conference on. IEEE,* pp. 1-4, 2015.

[40] Mehta, Parth, and D. Gawali, "Conventional versus Vedic mathematical method for Hardware implementation of a multiplier." *Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT'09. International Conference on. IEEE*, pp. 640-642, 2009.

[41] Rafferty, Ciara, Maire O'Neill, and N. Hanley. "Evaluation of Large Integer Multiplication Methods on Hardware", *IEEE Transactions on Computers*, 2017.

[42] C. Shylaja and T.Shreekanth,"Optimization of Block Cipher with SIMON", International Journal of Computer Applications", *National Conference on Power Systems & Industrial Automation (NCPSIA),* 2015.

[43] Y. Alkady, M. I. Habib and R. Y. Rizk, "A new security protocol using hybrid cryptography algorithms," *9th International Computer Engineering Conference*, pp. 109-115,2013

PUBLICATIONS

- Deeksha, Ajay Kumar and Manu Bansal, "A Review on VANET Security Attacks and Their Countermeasure," 4th International Conference on Signal Processing, Computing and Control (ISPCC-2017), sponsored by IEEE. **(Accepted)**

601562008_Deeksha

ORIGINALITY REPORT

%6	%2	%5	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	"A Flexible and Compact Hardware Architecture for the SIMON Block Cipher", Lecture Notes in Computer Science, 2015. Publication	%1
2	Yang, Qiong, Lin Wang, Weiwei Xia, Yi Wu, and Lianfeng Shen. "Development of on-board unit in vehicular ad-hoc network for highways", 2014 International Conference on Connected Vehicles and Expo (ICCVE), 2014. Publication	%1
3	Li Yong, , Qiwu Wu, and Qingzi Liu. "A hierarchical security architecture of VANET", International Conference on Cyberspace Technology (CCT 2013), 2013. Publication	<%1
4	publica.fraunhofer.de Internet Source	<%1
5	itservices.usc.edu Internet Source	<%1
	Unknown, . "The SIMON and SPECK	

6	lightweight block ciphers", Proceedings of the 52nd Annual Design Automation Conference on - DAC 15, 2015. Publication	<%1
7	Warjri, Janailin, and E. George Dharma Prakash Raj. "KED - A Symmetric Key Algorithm for Secured Information Exchange Using Modulo 69", International Journal of Computer Network and Information Security, 2013. Publication	<%1
8	Ni Made Satvika Iswari. "Key generation algorithm design combination of RSA and ElGamal algorithm", 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 2016 Publication	<%1
9	Kartha, Geethu Krishna, and E.A. Neeba. "Trust Establishment in Mobile Ad Hoc Networks", 2014 3rd International Conference on Eco-friendly Computing and Communication Systems, 2014. Publication	<%1
10	www.ijcaonline.org Internet Source	<%1
11	Panasayya Yalla. "Lightweight Cryptography for FPGAs", 2009 International Conference on	<%1