An End-to-End Authentication Method for NB-IoT Devices over 5G network using Whirlpool Hash Function and Physical Unclonable Function

by

Kazi Anisuzzaman
16341017
Mehreen Khan
16241009

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
BRAC University
January 2021

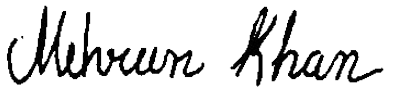
Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at BRAC University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I/We have acknowledged all main sources of help.

Student's Full Name & Signature:

Kazi Anisuzzaman
16341017



Mehreen Khan
16241009

Approval

The thesis/project titled "An End-to-End Authentication Method for NB-IoT Devices over 5G network using Whirlpool Hash Function and Physical Unclonable Function" submitted by

1. Kazi Anisuzzaman (16341017)
2. Mehreen Khan (16241009)

Of Fall, 2020 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January, 2020.

Examining Committee:

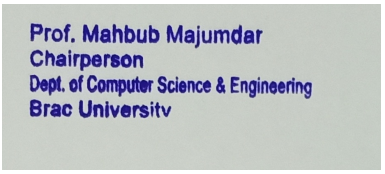
Supervisor:
(Member)

Dr. Md. Motaharul Islam
Professor
Department of Computer Science and Engineering
United International University
&
Associate Editor
International Journal of Computers and Applications
Taylor & Francis, UK.

Thesis Coordinator:
(Member)

Dr. Md. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)



Dr. Mahbub Alam Majumdar
Professor
Department of Computer Science and Engineering
BRAC University

Ethics Statement

We, hereby, declare that this thesis paper is based on the findings of our research. All the materials and resources utilized have been correctly mentioned and appropriately cited in the document.

This paper has not been submitted for any degree or award of any degree. It accurately credits the substantial contributions of the authors and supervisor.

All authors have actually and effectively contributed in significant work driving to the completion paper.

Abstract

The Narrow-band Internet of Things (NB-IoT) is a high throughput and Low Power Consumption Wide Area Network (LPWAN) radio technology, introduced by 3rd Generation Partnership Project (3GPP). The NB-IoT and LTE-M technologies continue to evolve as a part of the 5G specifications with upcoming releases of 3GPP. The assessment of security threats such as attacks on inter-operator security, radio interfaces, signaling and user plane, masquerading, replay, man-in-middle, bidding-down and privacy security issues have been considered for the 5G system. However, there is a scope for improvement in end-to-end security authentication for 5G NB-IoT. The user identity related issues are still a concern as the existing authentication protocols provide poor compatibility with current network architecture. In addition, these protocols demands dual authentication and key agreements. In this paper, we are proposing an application of Whirlpool Hash Function and Physical Unclonable Function (PUF) for an end-to-end authentication method for NB-IoT devices over 5G network.

Keywords: Narrowband Internet of Things; 5G; 3GPP; security authentication method; Physical Unclonable Function; Whirlpool Hash Function

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis has been completed without any crucial disruption.

Secondly, we are very thankful to our supervisor Dr. Md. Motaharul Islam for his kind support, advice and guidance in every step of our work. Under his constant supervision, we have become able to complete our thesis.

Thirdly, we are gladly indebted to our parents because without their throughout support this journey may not have been possible or completed.

Last but not least, we are immensely grateful to BRAC University for providing us with this opportunity and its adequate resources. We are privileged to be a part of this institute.

Table of Contents

Declaration i

Approval ii

Ethics Statement iv

Abstract v

Acknowledgement vi

Table of Contents vii

List of Figures ix

List of Tables x

Nomenclature xiii

1 Introduction 1

1.1 Overview 1

1.2 Motivation 2

1.3 Contribution 2

2 Related Work 4

3 Narrowband Internet of Things 7

3.1 Origin 7

3.2 Characteristics 9

3.3 Operation Modes 10

4 NB-IoT Network Architecture 12

4.1 4G Network Architecture 12

4.2 5G Network Architecture 14

5 Hash Function 17

5.1 Fundamentals 17

5.2 Whirlpool Hash Function 18

5.2.1 Algorithm 18

5.2.2 Advantages of Whirlpool 22

6 End-to-End Authentication **25**

7 Methodology **27**

7.1 Device Used 27

7.2 Development Environment 27

7.3 Implementation 28

7.4 Result and Analysis 29

8 Conclusion and Future Work **33**

References **36**

List of Figures

3.1 In-band Operation Mode 10
3.2 Guard Band Operation Mode 10
3.3 Stand Alone Operation Mode 11

4.1 NB-IoT 4G Network Architecture 13
4.2 NB-IoT 5G Network Architecture 14
4.3 5G Core and NG-RAN 16

5.1 High-level diagram of W block-cipher 18
5.2 Preprocessing and Message Digest Generation 20
5.3 S-box 20
5.4 Constant Matrix 21

7.1 Imported Packages 29
7.2 Unique String Generation 29
7.3 Test Code 29
7.4 Run-time Comparison between SM3 and Whirlpool using 64 bits of Input 31
7.5 Run-time Comparison between SM3 and Whirlpool using 128 bits of Input 31

List of Tables

3.1 Improvements of NB-IoT in 3GPP Release 13 [15] and Realease 14 [16] . 7
3.2 Improvements of NB-IoT in 3GPP Release 15 [17] and Release 16 [18] . . 8
3.3 Features of NB-IoT 9

5.1 List of Parameters 19
5.2 Performance Comparison between SHA-512 and Whirlpool 23
5.3 Comparison Between SHA-256 And Whirlpool Based On Different Works 23

7.1 Input and Output bits of Hash Function 28
7.2 Data set for Run-time Caparison using 64 bits of Input 30
7.3 Data set for Run-time Caparison using 128 bits of Input 30
7.4 Differences between 4G and 5G network 32

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

$3GPP$ Third Generation Partnership Project

$4G$ 4^{th} Generation

$5G$ 5^{th} Generation

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

APN Access Point Name

AS Application Server

$AUSF$ Authentication Server Function

Auth key Authentication key

$BEST$ Battery Efficiency Security for Low Throughput

CK Cipher Key

CLB Configurable Logic Block

$DDoS$ Distributed Denial-of-Service

EAP Extensible Authentication Protocol

EDT Early Data Transmission

$eNodeB$ Evolved Node B

EPC Evolved Packet Core

$FPGA$ Field-Programmable Gate Array

HSS Home Subscriber Server

IK Integrity Key

$IMEI$ International Mobile Equipment Identity

$IMSI$ International Mobile Subscriber Identity

IoT Internet of Things

JVM Java Virtual Machine

LoRa Long-Range

$LPWAN$ Low Power Wide Area Network

LTE Long-Term Evolution

LUT Look-UP-Table

$M-IoT$ Machine Internet of Things

$MITM$ Man-in-the-Middle

MME Mobility Management Plane Entity

NAS Non-Access Stratum

$NB-IoT$ Narrowband Internet of Things

$NG-RAN$ Next Generation Radio Access Technology Network

$NIST$ National Institute of Standards and Technology

$NPRACH$ Narrowband Physical Random Access Channel

$OSCCA$ Office of State Commercial Cryptography Administration

$OTDOA$ Observed Time Difference Of Arrival

$P-GW$ Packet Data Gateway

PCF Policy Control Function

PDN Packet Data Network

PDU Protocol Data Unit

PSM Power Saving Mode

PSM Power Saving Mode

PUF Physical Unclonable Function

QoS Quality of Service

RAN Radio Access Network

RAT Radio Access Technology

RRC Radio Resource Control

$S-GW$ Serving Gateway

SBA Service-Based Architecture

$SCEF$ Service Capability Exposure Function Gateway

$SEAF$ Security Anchor Function

SMS Short Message Service

UDM Unified Data Management

UDP User Datagram Protocol

UE User Equipment

UPF User Plane Function

$UUID$ Universally Unique Identifier

$VLSI$ Very-Large-Scale Integration

E-CID Enchanced Cell ID

Chapter 1

Introduction

1.1 Overview

The terminology of Internet of Things (IoT) and its original concept was devised by Kevin Ashton, in 1999. The central theory behind IoT was to connect a group of devices and appliances using embedded sensors and the internet. At present, Narrow Band Internet of Things (NB-IoT) radio technology, which was standardized by the 3rd Generation Partnership Project (3GPP), is being adapted worldwide increasingly. The limitless popularity and acceptance that NB-IoT is getting across the whole world is highly recommendable.

The foundation of this rapidly growing radio technology was put forth in Release 13 [1] in mid-2016, which discusses the Low Power Wide Area Network (LPWAN) requirements for the future of IoT. Especially in deep coverage, it remarkably enhances the spectrum efficiency, system capacity and power consumption of User Equipment (UE). The NB-IoT devices serve as sensors telemetry units and are controlled by external services, i.e. IoT platforms, through operational control and remote software updates. Its main form of communication would be M2M. The main target of NB-IoT is a low power and low cost connectivity which is mainly designed to connect a large number of end-point devices to a single base station.

With the Release 14 [1], 3GPP has paved the way for NB-IoT, one of the low power wide area technologies, to be a part of the next generation of mobile network technology, 5G. Later in release 15 [1], along with 5G Phase 1 specification 3GPP introduced the feature Battery Efficiency Security for Low Throughput (BEST) where they included symmetric key cryptography for integrity and encryption in the User Plane. The Control Plane (CP) is responsible for signaling traffic and routing. It takes care of system configuration and management authentication connection establishment base station selection. The User Plane (UP) mainly used for sending and receiving user data such voice, webpages and

sensor data.

NB-IoT has been facing with several security issues [2]. It firstly uses User Datagram Protocol (UDP) which means data is visible. So anyone intercepting the transmission can read the message. In NB-IoT, it is easy to orchestrate a Distributed Denial-of-Service (DDoS) attack where an attacker takes control of a large number of NB-IoT devices and makes connection requests to a particular server and demeaning it unusable [3]. In case of an Authentication compromise, attackers can make an injection attack on the main server or manipulate the data stored in the server.

1.2 Motivation

NB-IoT devices do not possess high computational power which brings about a restriction in its security implementation [4]. There is a need to conduct a thorough assessment of the NB-IoT for the industries and the institutes to effectively research and develop new algorithms and services using the NB-IoT technology. In the research [5], an end-to-end security authentication protocol applying Physical Unclonable Function (PUF) and state secret algorithm SM3 was proposed, which can provide bidirectional identity authentication and secure data communication between terminals and NB-IoT devices.

This method can be implemented for the next generation of mobile network technology, i.e. 5G, since the protocol provides light weight, small communication delay, flexible update and good compatibility with the existing network communication platforms. In this paper, we will be enhancing this existing authentication protocol by using Whirlpool secure cryptographic hash function [6] for the 5G NB-IoT which would provide remarkable improvement in performance, in terms of speed and throughput, and more robust hashing algorithm.

1.3 Contribution

We have come across three scopes of improvements- providing better compatibility between authentication protocols and network architecture, bidirectional authentication and key agreements, and dual connectivity to increase the throughput of NB-IoT devices-using

Whirlpool hash function and PUF. We have used the comparison of Whirlpool with SHA-2 to rationalize our choice as SHA-2 is incentive for the formulation of SM3 and SM4. Hence, it is their closest competitor in security, performance and popularity. In order to achieve these targets, we have proposed the following:

- Use of 5G NB-IoT network architecture for significantly better compatibility and more UE support with greater throughput.
- End-to-end authentication using Whirlpool Hash Function.
- Bidirectional authentication and key generation by using an authentication method based Whirlpool Hash Function along with PUF.
- We performed a run-time test for SM3 and Whirlpool Hash Functions and evaluated its results.

In the rest of the paper, we discussed about the past works in Chapter 2. In Chapter 3, we discussed about the evolution, features and deployment of NB-IoT. Chapter 4 explained the transformation of 4G towards 5G network architecture for the NB-IoT. Whirlpool hash function and its advantages have been discussed in Chapter 5. Furthermore, Chapter 6 represented the end-to-end authentication method for NB-IoT over 5G network. In Chapter 7, we showed a run-time benchmark for SM3 and Whirlpool hash functions, analysed its result and we also gave a theoretical analysis for the 5G network. Lastly, we stated our future works and concluded our paper with Chapter 8.

Chapter 2

Related Work

In [1] GSMA provided the detailed setup guide for NB-Iot networks and devices. The paper defines the NB-IoT and addresses its recent releases. It mentioned the added features in release 13, 14 and 15. In release 13, GSMA has introduced Power Saving Mode (PSM) which is designed to help IoT devices consume less battery and therefore obtain a 10-year battery life. Moreover, an evolution for the Radio Access Technology (RAT) has been defined: E-UTRAN NB-IoT. In release 14, a Non-Access Stratum (NAS) security token is incorporated in both the Radio Resource Control (RRC) connection re-establishment requests and messages. This allows authentication for the NB-IoT devices by the MME and authentication of the E-UTRAN Node B (eNodeB) by the UE. Lastly in release 15, GSMA has introduced BEST which supports User Plane integrity and confidentiality.

In [2] the authors categorized a list of vulnerabilities in IoT security. They mentioned inadequate authentication where an intruder might violate integrity. This stated the authentication keys being at risk of getting lost, corrupted or destroyed. They also mentioned improper encryption which may disclose sensitive information or aid in taking over control operations. Open ports in end point devices may give opportunities of easy access to attackers. The authors criticized insufficient access control where manufacturers do not impose users to change the default password. This also lead to unauthorized access of the system where the attacker can again ruin the integrity of the system. They also talked about weak programming, insufficient audit which all inevitably leads to a compromised system.

In paper [3], a small section of the security vulnerabilities of the NB-IoT are discussed. The authors mentioned the jamming and security keys. They also addressed scanning using malicious UEs which could impact the integrity of data and also lead to DDoS by battery exhaustion. In paper [4] the authors provided a detailed comparative analysis

of the security issues in a layer-based approach related to NB-IoT devices. They also mentioned the DoS/DDoS as the most common and also the most effective form of attack. DoS/DDoS attack is performed when a malicious user sends mass number of connection request to a server deeming it unusable. The paper discussed Man-in-the-Middle (MITM) attack. In MITM attack, the attacker intercepts the interface between the IoT device and the gateway. This allows the attacker to eavesdrop and also alter the data being sent and receive. Another form of attack is the Sybil attack where the attacker identifies its self as a valid user to compromise the system altogether. They also mentioned about Firmware attack where the attacker install a firmware on the IoT device and take control of it remotely. The authors of [4] identified the principle security issues for three of the layers of IoT architecture. At the Perception layer, there are Sensors tag security issue, Key management security issue and routing protocol security issue. In the Transportation layer, the security issue consists of Network, GPRS and Internet Security Issue. Finally, the Application layer is significant to computing platform security and service support security issues.

In the conference paper [5], the authors worked on the end-to-end security authentication protocol of the NB-IoT system. They stated that the existing protocols require key agreements and dual authentication and are not well suited with current network architecture. They proposed authentication protocol using state secret algorithm SM3 and Physical Unclonable Function (PUF), and also a self-controllable NB-IoT application layer of security architecture.We researched about our chosen Whirlpool hash function from the paper [6]. It is based upon Whirlpool cryptographic hash function. Whirlpool hash function was designed by Vincent Rijmen and Paulo S. L. M. Barreto in 2000. Its design is based upon an iterated block-cipher Advanced Encryption Standard (AES), which is invertible for decryption. The length of the hash code is 512 bits. Its overall structure exhibits resistant to general attacks on hash codes which are based on block-cipher. According to this paper, The National Institute of Standards and Technology (NIST) evaluation of Rijindael resolved that Whirlpool displays favourable execution speed in terms of both software and hardware. Moreover, it is greatly compatible with low-memory conditions

verified by Ruby B. Lee in the paper[7] .

In a survey paper [8], the authors wrote about the Evolved Packet Core (EPC) architecture of NB-IoT. They mentioned the mechanism of EPC and two ways in which the data is transferred between the NB-IoT devices and application server. The two ways are IP based and Non-IP based. They also mentioned the detailed NB-IoT Frame Structure: Downlink and Uplink frame structure, and how they support NB-IoT to maintain its low power and cost consumption in a mass network. China unlike the rest of the world uses their own Cryptographic algorithms for use in their own software and also for foreign products and development services that wish to operate in their country. It is enforced by the Office of State Commercial Cryptography Administration (OSCCA) of china. Their cryptographic algorithms are SM2, SM3 and SM4 which have large similarities with RSA and ECDSA, SHA-256, and AES-128. In [9] the authors performed a theoretical analysis and performance evaluation on the standard cryptographic algorithms and Chinese Cryptographic algorithms. They presented side by side pros and cons of the Chinese and standard cryptographic algorithms. Controlled tests were set up in [9], [10] to answer some critical performance questions which helped us further in our study.

For understanding the 5G system and its network architecture, we read and took the primary idea from [1], [11] and [12]. The suggested Physical Unclonable Function (PUF) was first proposed by Ravikanth Srinivasa Pappu, in 2002 [13]. PUF is a physical unit which generates a physically-defined digital fingerprint output for a given input and conditions. The fingerprint is generated from the unavoidable random differences during the chip production. The output or response serves as a unique identifier. PUFs are often implemented in integrated circuits and used in applications with high-level security requirements, particularly cryptography. Its uniqueness ensures that no two PUFs are to be the same or to be copied [14]. The Use of PUF also ensures that no additional device is needed for authentications where NB-IoT devices are only shrinking quickly. PUF are next to impossible to predict which also provides stability over time and ease for evaluation. We acquired the motivation and knowledge from these papers for our work.

Chapter 3

Narrowband Internet of Things

3.1 Origin

Narrow band Internet of Things (NB-IoT), also known as LTE Cat NB, is LPWAN Technology was developed to allow a wide range of IoT devices to connect to the internet using existing cellular networks. Its specification was standardized by 3GPP in their Release 13[15], in June 2016.

3GPP Release	**Release Date**	**Summary**
Release 13	Q1 2016	• Standardization of NB-IoT • SMS deployment for NB-IoT-only UEs • PSM Standalone Timers • LTE In-band Deployment • LTE Guardband Deployment • Paging
Release 14	Mid 2017	• Positioning: E-CID and OTDOA • E-CID and OTDOA positioning enhancements • New Category LTE Cat NB2 • Relaxed monitoring for cell reselection • Single-cell multicast transmission • Power Class Cell (14dBm) • Paging and random access on nonanchor carrier • Release Assistance Indication • Element on road to 5G

Table 3.1: Improvements of NB-IoT in 3GPP Release 13 [15] and Realease 14 [16]

It is rapidly arising as the one of the best LPWAN technology in the world. It enhances the spectrum efficiency, system capacity and lowers the power consumption for NB-IoT devices in deep coverage area. The concept of NB-IoT is all about less power consumption

and less cost connectivity as it is developed for large number end-to-end connections per single base station.

3GPP Release	**Release Date**	**Summary**
Release 15	End 2018	• Local RRC Management Policy Information storage for UE differentiation • BEST • Mobility enhancements • Early Data Transmission (EDT) • Power consumption and latency reduction • Low power class • NB-IoT small cell support • NB-IoT Test Driven Development (TDD) support • Reduced system acquisition time • Wake-up signals (WUS) • Scheduling request (SR) • NPRACH range enhancement • 5G Phase 1 specification
Release 16	End 2020	• Higher Mobility Enhancement • Positioning • Network Slicing • Better coverage • NB-IoT in-band deployment with 5G New Radio (NR) • 5G Phase 2 specification

Table 3.2: Improvements of NB-IoT in 3GPP Release 15 [17] and Release 16 [18]

Then in 2017, NB-IoT was classified as a 5G technology, standardised by 3GPP [16]. It is rapidly arising as the one of the best LPWAN technology in the world. With the new added and improved features in Release 14, 15 and 16, NB-IoT has become better

in performance with higher spectrum efficiency, system capacity and even lower power consumption.

3.2 Characteristics

NB-IoT provides deep indoor penetration as it is operated at low-frequency bandwidth of 180 kHz for both UL and DL channels [4]. It supports very low-complexity devices offering up to 10 years of battery life. It provides a coverage range of 164dB with the peak data rate of 26 kbps in downlink and 66 kbps in uplink (multi-tone). Its latency is generally around 1 s in normal coverage, but increases up to 10 s in case of extended coverage [4].

Feature	**NB-IoT**
Bandwidth	180 kHz (200 kHz carrier bandwidth)
Range	10 - 15 km
Coverage	Deep coverage of 164dB
Capacity	Upto 52K devices per cell
Mobility	Nomadic
Battery Lifetime	Upto 10 years with a battery capacity of 5 Wh
Peak Data Rate	26 kbps(downlink) & 66 kbps (uplink)
Latency	<10 s
Cost	Low

Table 3.3: Features of NB-IoT

Unfortunately, there are some some limitation to NB-IoT as it was designed for only data transmission in stationary or nomadic devices. It offers lower data rate (about 250Kbps download and 20Kbps upload) compared to LTE cat-M1. It does not support of a seamless mobility and handover between cells. Also, it does not support application requiring low latency, e.g. voice transmission.

3.3 Operation Modes

NB-IoT can be deployed in three operation modes depending on the accessible spectrum and use cases. The operator selects the most suitable operation mode to fulfill its requirement. The three operation modes are:

1. In-band: In the in-band operation, NB-IoT uses the resources within the bandwidth of 180 kHz of a wideband LTE carrier.[4]

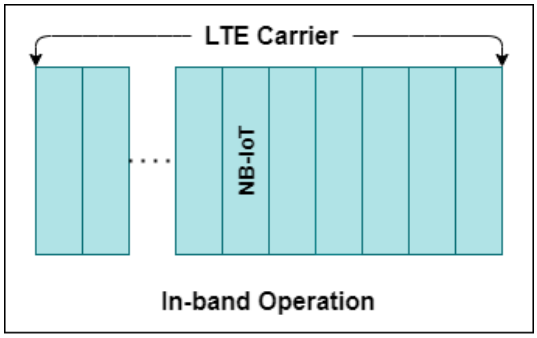


Figure 3.1: In-band Operation Mode

2. Guard-band: In the guard band operation, NB-IoT uses the resource blocks within the edge frequency band of the LTE carrier without requiring new spectrum and with minimal impact to LTE carrier. It utilizes a frequency band of 200 kHz from the guard band.[4]

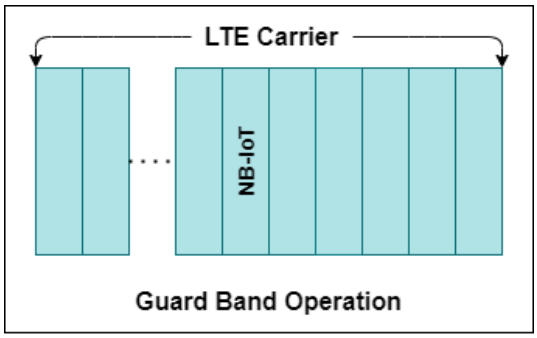


Figure 3.2: Guard Band Operation Mode

3. Standalone: In the guard band operation, NB-IoT uses one or more GSM carriers having a bandwidth of 200 kHz. It does not overlap with the LTE frequency band.[4]

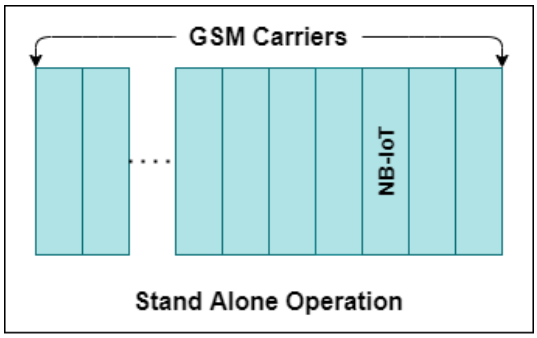


Figure 3.3: Stand Alone Operation Mode

Chapter 4

NB-IoT Network Architecture

4.1 4G Network Architecture

4G NB-IoT has simplified Evolved Packet Core (EPC) architecture [8] to support the small data transmission needed for Machine Internet of Things (M-IoT) application in the form of Control Plane and Use Plane EPC optimization. NB-IoT device exchanges information with NB-IoT device connects with the 4G IoT EPC, Figure 4.1. EPC is comprised of the following entities:

- Mobility Management Plane Entity (MME) – It deals with the Control Plane. It handles the signaling related to mobility and security for E-UTRAN access. It is responsible for the tracking and the paging of NB-IoT devices in idle-mode, authenticating the user, S-GW and P-GW selection. The MME is the termination point of the network for ciphering/integrity protection for NAS signaling and also handles the security key management. Basically, NAS is a protocol that transfers the non-radio signal between the NB-Iot devices and the MME. It also terminates the S6a interface towards the HSS for roaming NB-Iot devices.

- Serving Gateway (S-GW) – It deals with the User Plane. It is the local mobility anchor for inter-eNodeB handover. For idle state UEs, the S-GW terminates the E-UTRAN downlink data path and triggers paging when downlink data arrives for the NB-IoT devices. They transport the IP data traffic between the NB-Iot devices and the external networks. It performs lawful interception. The S-GW is the point of interconnect between the radio-side and the EPC. It is logically connected to the other gateway, the P-GW.

- Packet Data Gateway (P-GW) – It provides connectivity between the EPC and external IP networks by being the point of exit and entry of traffic for the NB-IoT devices. The P-GW performs various functions such as IP address / IP prefix

allocation or policy control, lawful interception and charging. A device may have simultaneous connectivity with more than one P-GW for accessing multiple Packet Data Networks (PDNs).

- Home Subscriber Server (HSS) – It is a central database that contains user-related and subscription-related information. It is the storage of Sub Data (Auth keys, QoS profile, APN profile, etc.). It provides support functions such as mobility management, call and session establishment support, user authentication and access authorization.

In Figure 4.1, Service Capability Exposure Function Gateway (SCEF) provides a secure gateway interface between NB-IoT devices and Application Server (AS) which processes and controls the information. It authenticates AS and UE registration for secure data transmission and delivers the non-IP data over the control plane. It also establishes, control and enforces security policies for UE activity. After the processes involving the entities are performed in EPC, the EPC pass the data to IoT platform which then passes the data to application servers.

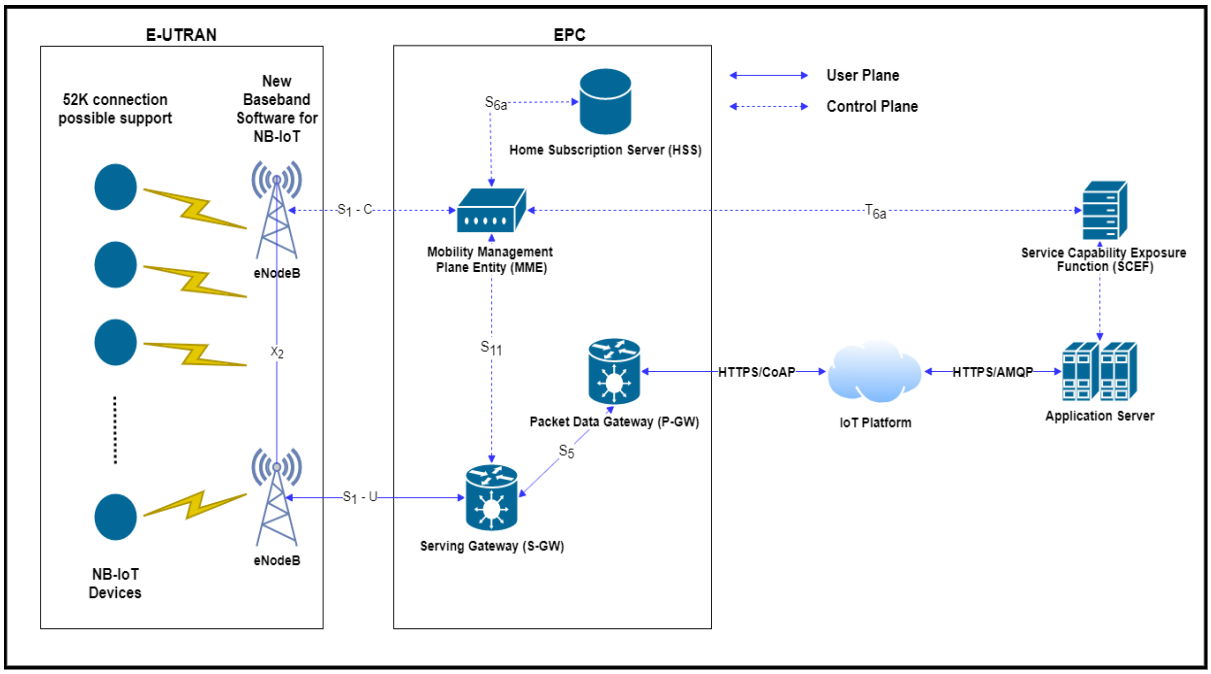


Figure 4.1: NB-IoT 4G Network Architecture

4.2 5G Network Architecture

The 5G NB-IoT network architecture, in Figure 4.2, supports the 2G, 3G and 4G systems. It is much more service based and secure than previous generation architectures [1]. 5G is a unified platform that is more capable than 4G as it uses better spectrum and have lower latency. Thus, it is faster than 4G. The 5G Core assembles data traffic from end devices, just like 4G EPC. It also authenticates devices and users, enforces personalized policies and manages the mobility of the devices before routing the traffic towards the application services or Internet. Although the NB-IoT EPC and 5G Core have some common characteristics, the 5G Core still have few crucial features. The 5G Core is divided into a number of Service-Based Architecture (SBA) entities and is designed for complete control and user plane separation [11].

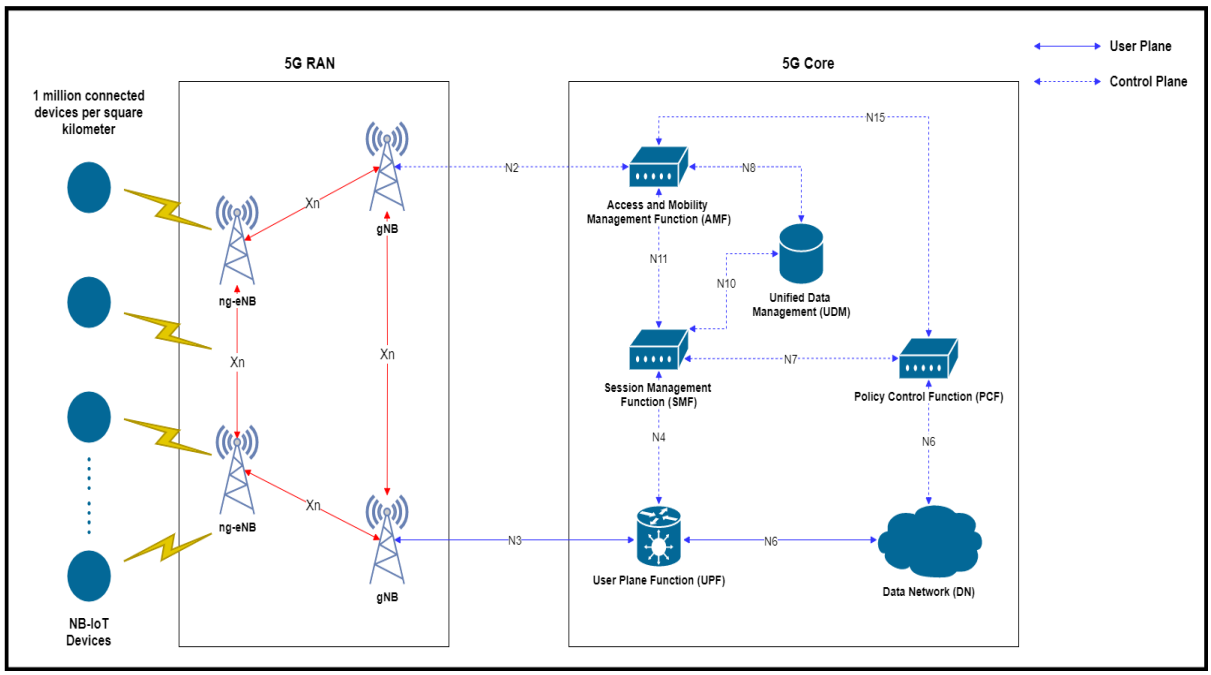


Figure 4.2: NB-IoT 5G Network Architecture

The New 5G Core Network consists of the following network functions [12]:

- Access and Mobility Management Function (AMF) – In the new architecture, MME is divided into two network functions, the AMF and SMF. AMF handles subscriber mobility, registration and security. It receives all the session and connection information from UEs or the Radio Access Network (RAN). It also provides a UE with

temporary identity whenever it signals the network, which is also used for paging.

- User Plane Function (UPF) – It represents the enhancement of the data plane function of P-GW and S-GW. UPF is the anchor point of 5G RAN mobility, so it enforces the Quality of Service (QoS) flow and implements the policy enforcements.

- Policy Control Function (PCF) – It governs the Control plane functions using the defined policy rules and User plane functions using the policy enforcement. It handles the dynamic policy decisions with given conditions. It shifts both the mobility and session related services.

- Session Management Function (SMF) – It is a rudimentary part of the SBA, it manages the establishment, modification and the tear down of the Protocol Data Unit (PDU) sessions. It also handles the PCF interactions for data network profile, UPF selection and IP address allocation.

- Authentication Server Function (AUSF) – It performs the authentication function of 4G HSS. It also applies the Extensible Authentication Protocol (EAP) authentication server and provides encryption keys.

- Unified Data Management (UDM) – It is a central repository of subscriber information which is directly involved with access authorization. UDM, which is the alternative for HSS, is cloud-native. It is involved in registration and mobility management because it will be tracking allocation of AMF to the subscriber. It stores the data network profiles and encryption keys.

Moreover, AMF hosts Security Anchor Function (SEAF) which generates a unified anchor key K_{SEAF} used between the UE and 5G network to protect the end-to-end communication.

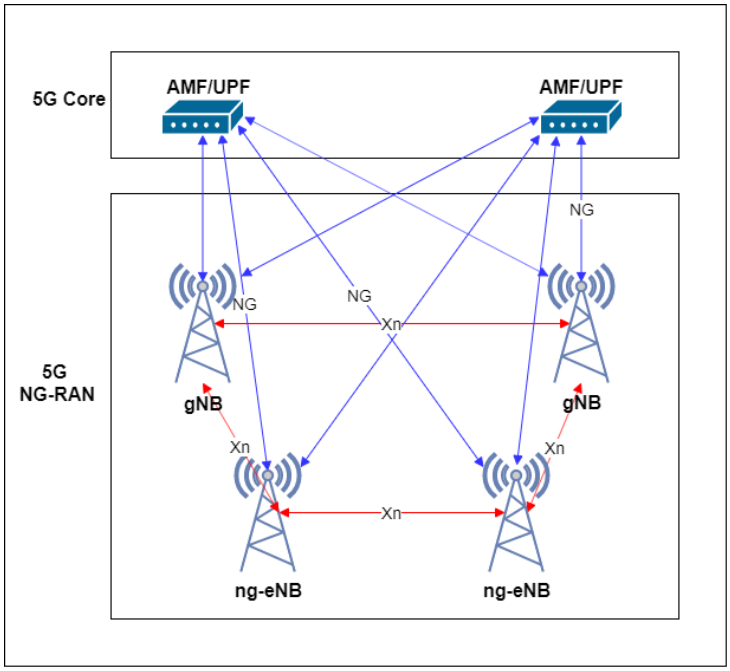


Figure 4.3: 5G Core and NG-RAN

The 5G Next Generation Radio Access Technology Network (NG-RAN) has gNB and ng-eNB as nodes (Base Station). The gNB is next generation NodeB and the ng-eNB is a next generation evolved 4G eNodeB. In Fig. 3, using the NG interface, gNB and ng-eNB connects to the 5G Core network. However, they use other radio interfaces to establish communication with the UEs. The ng-eNB also uses the existing 4G NB-IoT air interface to interact with 5G UE. The ng-eNB is the primary node which controls the radio signals with the UE, whereas the gNB is the secondary node. Through the Xn interface, the gNB and ng-eNB are interconnected. Thus, we can deliver high throughput for the UEs using this architecture, while providing dual-connectivity without putting additional pressure on the 5G Core network architecture.

Chapter 5

Hash Function

5.1 Fundamentals

A cryptographic hashing function of n-bit is a mathematical operation that is used to generate a unique n-bit hash value message from an arbitrary length of input message. Simply put, it takes maximum input data as per the algorithm and condenses it to a fixed length alphanumeric output. The output produced should be computationally infeasible to be inverted to the original input. It is sometimes dubbed as a one-way-encryption function. The main function of cryptographic hash function is data integrity. However, it can also be applied to construct stream and block-ciphers, pseudo-random code and generate authentication code using digital signature. This also ensures non- repudiation.

There are primarily three criteria to a proficient design of an efficient and safe hash function:

1. It has to have high throughput to be useful in its environment. That is the time taken to re-compute the input from the output should be comparatively immeasurable.

2. The hash function should have a high avalanche effect. A marginal alteration in the input message will create a sizable incomprehensible alteration in the output message.

3. A high collision resistance is of utmost necessity for a hashing function. This means it would have a tremendously low chance of having the same output message for two separate input messages.

Some popular functions used are non-resource constrained devices are SHA-2, SHA-3, GOST, BLAKE and RIPEMD.

5.2 Whirlpool Hash Function

In the year 2000, Whirlpool hash function was certified by the New European Schemes for Signatures, Integrity and Encryption [6]. It is a 512-bit hash function adopted by ISO and IEC as international standards. It is essentially a block-cipher algorithm derived from Advanced Encryption Standard (AES). This has significant improvements from its predecessor Whirlpool-0 to Whirlpool-T.

The compression function of Whirlpool operates on 512-bit message blocks and 8×8 byte matrix which holds the final hash value as well as the intermediate value between the steps. It has 10 rounds of compression and output hash value size is 512-bit. Whirlpool has a pre-image attack resistance and collision attack of $< 2^n$ & $< 2^{\frac{n}{2}}$ respectively.

5.2.1 Algorithm

Whirlpool is an iterative, one-way hash function that takes any input M to produce a 512-bit message digest. The steps of the algorithm are as follows:

1. Append padding bits to the input message.
2. Append length to the input message.
3. Initialize the 8x8 byte hash matrix
4. Process the message in blocks of 512-bits (W block-cipher).

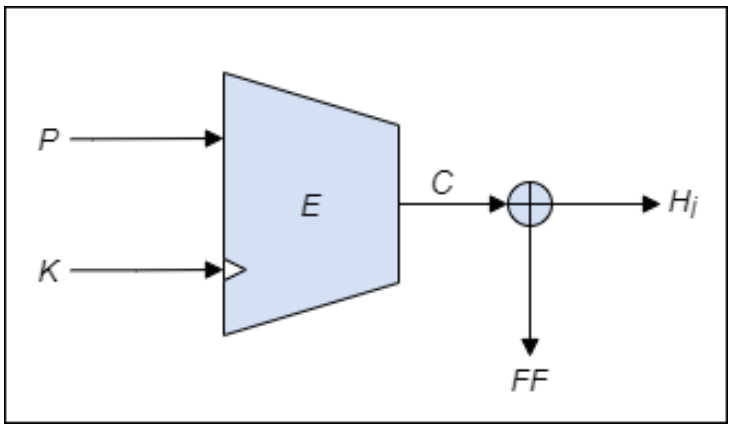


Figure 5.1: High-level diagram of W block-cipher

Parameters: The parameters used in the block-cipher of Whirlpool hash algorithm specifications are as follows:

Parameter	Description
$H^{(i)}$	The i^{th} hash value. Between initial hash value $H^{(0)}$ and the final hash value $H^{(N)}$.
P	The input as plain text.
K	The encryption key is added to W block-cipher in every iteration, which is equal to the intermediate hash value from the preceding iteration.
C	The output cipher text of every iteration.
FF	The feed forward value for the next iteration. That is the bit wise XOR of the current message block and intermediate hash value from the preceding iteration.
$M^{(i)}$	Message block i of 512-bit.
N	Number of 512-bits message block.
A	Input matrix in each round of $0 \leq t \leq 9$.
B	Output matrix in each round of $0 \leq t \leq 9$.
CM	Constant matrix used in Mix Row operation.

Table 5.1: List of Parameters

Preprocessing: Preprocessing requires padding the message, then dissecting that padded message into 512-bits block and finally initializing the values, which would be used in the hash computation. It consists of three steps:

1. Padding the message: This is done to make the input M an odd multiple of 256-bits. Irrespective of its length padding is always be done.

2. Appending the length: A 256-bits block containing the length of the unpadded message is added to the input message.

3. Setting the initial hash matrix: For holding the intermediate and the final hash value. An 8x8 byte matrix is initialized holding a value of 64 bytes which is equal to the block size of 512 bits.

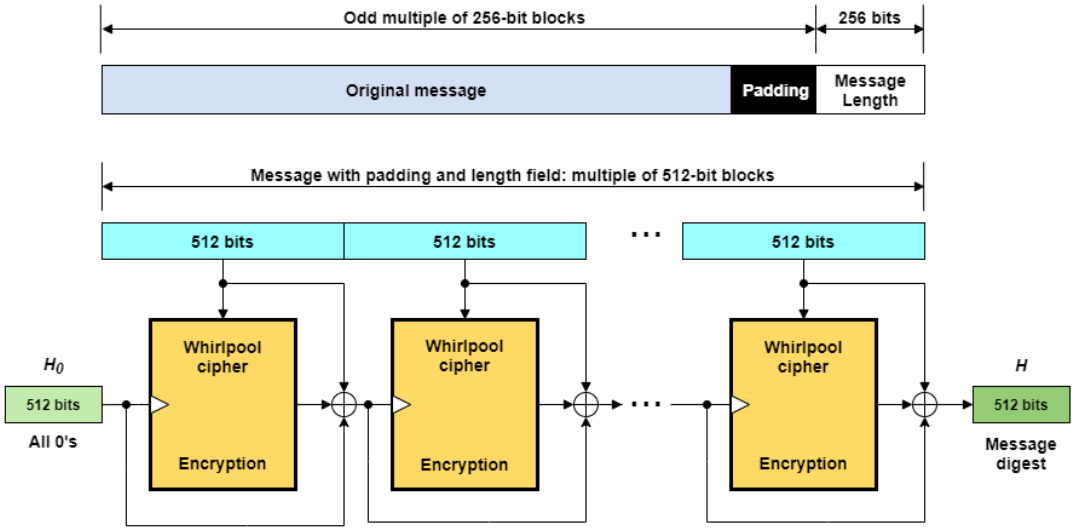


Figure 5.2: Preprocessing and Message Digest Generation

Hash Computation: The message blocks $M^{(1)}$, $M^{(2)}$, $\cdots$, $M^{(N)}$ are computed in sequence based on the following steps:

1. Substitute Byte (SB): Substitute byte transformation operation provides nonlinear mapping through a 16×16 lookup table called S-box. All byte of the current state block is mapped into a new state. Non-linearity ensures that a small change in input leads to a large change in output.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

Figure 5.3: S-box

2. Shift Column (SC): Also known as the permutation layer is a circular downward shifting of each of the columns with respect to its column index. Thus, the n^{th} column has n-bits circular downward shifting, e.g. 1st column has 1-byte circular downward shifting, 2^{nd} column has 2-byte circular downward shifting, etc.

3. Mix Row (MR): Consists of an 8×8 constant matrix where each row of the current state block performs product operation on the columns of the constant matrix. This layer is also known as the diffusion layer. A new value, which is a function of all the eight bytes in each row, forms each byte of the new rows.

$$\begin{bmatrix} 01 & 01 & 04 & 01 & 08 & 05 & 02 & 09 \\ 09 & 01 & 01 & 04 & 01 & 08 & 05 & 02 \\ 02 & 09 & 01 & 01 & 04 & 01 & 08 & 05 \\ 05 & 02 & 09 & 01 & 01 & 04 & 01 & 08 \\ 08 & 05 & 02 & 09 & 01 & 01 & 04 & 01 \\ 01 & 08 & 05 & 02 & 09 & 01 & 01 & 04 \\ 04 & 01 & 08 & 05 & 02 & 09 & 01 & 01 \\ 01 & 04 & 01 & 08 & 05 & 02 & 09 & 01 \end{bmatrix}$$

Figure 5.4: Constant Matrix

4. Add Key (AK): In this layer, exclusive-OR (XOR) operation takes bit wise place between the 512-bit state block and the 512-bit key. This key is also generated using the same Whirlpool round function. The round key function initial matrix is also initialized with the S-box with the first rows being non-zeros.

$$b_{(0,0)} = a_{(0,0)} \oplus (9 \cdot a_{(0,1)}) \oplus (2 \cdot a_{(0,2)}) \oplus (5 \cdot a_{(0,3)}) \oplus (8 \cdot a_{(0,4)}) \oplus a_{(0,5)} \oplus (4 \cdot a_{(0,6)}) \oplus a_{(0,7)}$$

Result: After processing $M^{(N)}$ times, the final 512-bit message digest of the message M, is the resulting state block of the final round.

Algorithm 1 : Whirlpool Algorithm

Input: A
Output: $H^{(N)}$

1: **for** $i = 1$ *to* N **do**
2: **for** $j = 0$ *to* 9 **do**

3: $B = SB(A) \leftrightarrow b_{(i,j)} = S[a_{(i,j)}]$; ▷ $0 \leq i, j \leq 7$

4: $B = SC(A) \leftrightarrow b_{(i,j)} = a_{((i-j) \ mod \ 8, \ j)}$;

5: $B = A \cdot CM$;

6: $B = AK[K_j](A) \leftrightarrow b_{(i,j)} = a_{(i,j)} \oplus k_{(i,j)}$;

7: **end for**

8: **end for**

9: $H^{(N)} = B$;

5.2.2 Advantages of Whirlpool

The complex structure of the hash function is developed in a way that resists usual attacks on block-cipher-based hash codes. Since, SM3 and SM4 hash functions are the Chinese alternatives for the SHA-256 and SHA-512 respectively, we collected data set for SHA-2. On the basis of the collected data shown in Table 5.2 and Table 5.3, we observed that Whirlpool is comparatively better than SHA-2. Whirlpool can be applied easily in both hardware and software as the existing versions are written in C and in Java. It is available in the public domain as well. Major advantages of Whirlpool are as follows:

- It works relatively faster than other hash functions for low power devices (NB-IoT, FPGA devices, etc.).
- Its implementation requires fewer area slices per Mbps of throughput than that of SHA-512.
- Whirlpool has a collision resistance of 2^{256} compared to SM3 which have an output bit size of 256 and collision resistance of 2^{128}.
- All Whirlpool implementations require between 4000 and 8000 Configurable Logic Block (CLB) slices to implement and operate at a frequency range between 105 MHz and 140 MHz.
- It takes approximately 3 minutes to brute force a hashed short-length password, whereas SHA-512 takes 37 seconds to do the same, according to the article in [19].

In paper [20] the author ran a performance analysis of SHA-2 family and Whirlpool alongside other hash function with an efficient architecture and VLSI implementation. Some of the results obtained from the paper [20] are represented in table 5.2.

Hash Function	CLB Slices	Frequency (MHz)	Throughput (Mbps)
SHA-512	2237	75	480
Whirlpool Boolean	5713	72	3686
Whirlpool Look-Up-Table	3751	93	2380

Table 5.2: Performance Comparison between SHA-512 and Whirlpool

From the table we can deduce that Boolean based Whirlpool performs significantly better than SHA-512 with a lower clock frequency. These results aided us to choose Whirlpool over other popular hash functions.

Hash Function	Works	Devices	Area Slices/Block-RAM	Speed (Mbps)
SHA-512 Iterative	McLoone et al[21]	Virtex-4 X4VLX100	2734/2	854
SHA-512 Optimized	Grembowsi et al[22]	Virtex XCV1000	3441/2	676
SHA-512 Unroll x 4	Crowe et al[23]	Virtex-E XCV2000E	3506/0	533
SHA-512 Unroll x 5	Lien et al[24]	Virtex	-/0	1034
Whirlpool Iterative	McLoone et al[21]	Virtex-4 X4VLX100	4956/68	4790
Whirlpool Iterative	Kitsos et al [20], [25]	Virtex-E XCV1000E	5585/0	4480
Whirlpool Unroll x 2	McLoone et al[21]	Virtex-4 X4VLX100	13210	4896

Table 5.3: Comparison Between SHA-256 And Whirlpool Based On Different Works

In [21] the authors did performance evaluation on Whirlpool and SHA-512 Xilinx Virtex-4 FPGA devices.The performance evaluation was done using the Look-UP-Table (LUT) method using different CLB slices as shown in Table 5.3. Form the Table 5.3 it is comprehensible that Whirlpool hash function outperforms SHA-512 with slight more Area Slices. This backs up Rajendal's claim of Whirlpool hash function high throughput with memory constrained devices.

Chapter 6

End-to-End Authentication

Here, we will generate challenge response pair based on PUF and use them for authentication of the NB-IoT devices of the 5G network. Key generation will take place according to the EAP-AKA' protocol of 5G, which is designed for challenge-response authentication. The ID of each NB-IoT devices is generated by hashing its IMEI and IMSI number of the devices using Whirlpool and is stored in UDM. The Authentication occurs in the following six steps:

Algorithm 2 : Authentication and Key Generation

Input: $Chln, IMEI, IMSI$
Output: CK, IK

1: Create challenge-response pairs.

$PUF\ (Chln)$ ▷ $0 \leq Chln \leq 2^{64} - 1$

2: Generate ID using Whirlpool hash.

$ID = Hash(IMEI \| IMSI)$

3: Calculate Response to Challenges for each ID and store it in the AUF.

$Rspon = PUF(ID \| Chln)$;

$UDM = Rspon$;

4: AUSF randomly selects a challenge from UDM for the NB-IoT device for I authentication and validates its response. Here, i is randomly selected from excess repository of PUF responses from UDM.

$Chnl' = RandChnl(Chnl \| i))$; ▷ $0 \leq Chln \leq 2^{64} - 1$

$Rspon' = PUF(Chnl')$;

$ID' = eNB(HASH(IMEI \| IMSI))$;

$Rspon'' = PUF(ID' \| Chnl')$;

5: **if** $(Rspon' \approx (Rspon''))$ **then**

6: $Valid\ Authentication$;

7: **else**

8: *Invalid Authentication*;

9: END;

10: **end if**

11: If authentication is valid in step 4, AUSF proceed to generate Cipher Key (CK) and Integrity Key (IK) as per 5G network protocol. Then, save them in UDM.

$K_i \rightarrow CK + IK \rightarrow CK' + IK' \rightarrow EMSK \rightarrow K_{SEAF} \rightarrow K_{AMF}$

AUSF generates an Extended Master Session Key (EMSK) using the keying informations received from UDM and then uses the first 256 bits of the EMSK as the K_{AUSF}. SEAF derives the K_{SEAF} from K_{AUSF}. AMF takes the K_{SEAF} and derives K_{AMF} from it. It then generates all the keys necessary for the all inter-interfaces communication to ensure end-to-end security.

12: END

Chapter 7

Methodology

For the evaluation of Whirlpool Hash function, an elementary run-time benchmark with Chinese state secret hashing m algorithm SM3 was conducted. We chose SM3 for comparison with Whirlpool as it was implemented in the paper [5] from which with we took an inspiration and are proposing an improvement upon. We used a java based cryptographic library and analyzed the results. We also provided a side by side comparison of 4G and 5G network to justify our choice for selecting 5G Network.

7.1 Device Used

The system is implemented in a 64 bit Windows 10 Home OS system .The CPU used in this system is a 4^{th} generation intel® CoreTM i7 processor with family model number 4510U. It's a quad core processor with 2.0 GHz base clock speed and 4MB cache. It is a dual core four thread mobile processor. To know how the algorithms performs in artificially constrained environment, the CPU max performance was set to 75% in advanced battery and power options.

7.2 Development Environment

For setting up the development environment to execute the run-time benchmark the following applications/software were installed in our local machine:

- Java Development Kit (JDK) 8 update 181 for 64bit Windows Operating system was used to operate the java based cryptographic library and for its well-known compatibility and overall popularity.
- NetBeans Integrated Development Environment (IDE) version 8.2 was installed for java software development and to integrate the cryptographic library with JDK 8.
- BouncyCastle Application Programming Interface (API) in java JDK 1.5-168 a trustworthy Australian based cryptographic library was installed to obtain the

source code of respective hashing function.

7.3 Implementation

We used different input values and parameters for the testing purpose. Whirlpool and SM3 tests were both conducted twice, first with 64 bits input string and second with 128 bits input string. The input string was unique for each message digest performed in both scenarios. The following table gives an idea of the types of test conducted.

Hash Function	**Input Bit**	**Output Bit (Message Digest)**
Whirlpool	64	512
	128	512
SM3	64	256
	128	256

Table 7.1: Input and Output bits of Hash Function

For performing the hashing algorithm,these following packages were used:

- java's built-in security package java.security.Security
- java.security.MessageDigest
- BouncyCastle's package org.bouncycastle.jce.provider.BouncyCastleProvider

These packages were imported into our main BCtest class file as show in Figure: 7.1. The first package centralizes common security methods of JDK8. The second one provides the application a message digest algorithm functionality. Finally, the last one is used to import the main BouncyCastle cryptographic library itself.

To generate the unique 128 bit Input message the java.util.UUID package was imported. UUID stands for Universally Unique Identifier. The following code was used to generate an immutable unique input string for 128 bit strings for the longer input message operation and a 64 bits for the shorter input message operations.

```
import java.security.Security;
import java.security.MessageDigest;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
```

Figure 7.1: Imported Packages

```
String plainString = UUID.randomUUID().toString().replace("-", "");
plainString = plainString.substring(0,16);
```

Figure 7.2: Unique String Generation

To obtain the performance both Whirlpool and SM3 was used to generate 1000 hashes - first with 128 bits of Input String and second with 64 bit Input String - and timed using the System.currentTimeMillis() function. The difference between the start time and stop time provides us with the run-time in milliseconds for each 1000 message digest operations. The result is then printed using System.out.println() fucntion.

```
startTimer = System.currentTimeMillis();

for (int i = 0; i < 1000; i++) {
    MessageDigest messageDigest = MessageDigest.getInstance("sm3");
  //MessageDigest messageDigest = MessageDigest.getInstance("Whirlpool");
    String plainString = UUID.randomUUID().toString().replace("-", "");
    plainString = plainString.substring(0,16);
    hashedString = messageDigest.digest(plainString.getBytes());
}
    stopTimer = System.currentTimeMillis();
    runtime = stopTimer - startTimer;
    System.out.println(runtime + " ms  ");
    totalRuntime += runtime;
```

Figure 7.3: Test Code

7.4 Result and Analysis

As shown in Table 7.2 and Table 7.3, we first conducted the test with input string of 64 bits and then with 128 bits for both Whirlpool and SM3. Each test is comprised of generating one thousand hashes with a random unique input for each hash operation. The test is performed 5 times with each hash function and the following results are represented in a graph as shown in Figure 7.4 and Figure 7.5.

Input Bit	Run-time for Hash Algorithm	
	SM3	Whirlpool
64 bits	243 ms	150 ms
	233 ms	181 ms
	219 ms	156 ms
	217 ms	140 ms
	236 ms	195 ms
	235 ms	171 ms
	216 ms	188 ms
Average	228 ms	169 ms

Table 7.2: Data set for Run-time Caparison using 64 bits of Input

In both Figure 7.4 and Figure 7.5, it is observed that the time taken for Whirlpool is lower compared to SM3's time. The average time for 64 bits input message is 169 milliseconds for Whirlpool and 228 milliseconds for SM3 this makes Whirlpool 34.91% faster than SM3. For 128 bits input messages the average time is 191 milliseconds for Whirlpool and 236 milliseconds for SM3 here Whirlpool is 23.56% faster than SM3.

Input Bit	Run-time for Hash Algorithm	
	SM3	Whirlpool
128 bits	275 ms	244 ms
	224 ms	218 ms
	219 ms	180 ms
	232 ms	164 ms
	219 ms	187 ms
	235 ms	171 ms
	251 ms	172 ms
Average	236 ms	191 ms

Table 7.3: Data set for Run-time Caparison using 128 bits of Input

Using this data set, we evaluated that shorter input messages are faster for Whirlpool. Even though the difference in time is only a few milliseconds when considering that SM3 has collision resistance of 2^{128} and Whirlpool has a collision resistance of 2^{256} the performance difference becomes very evident.

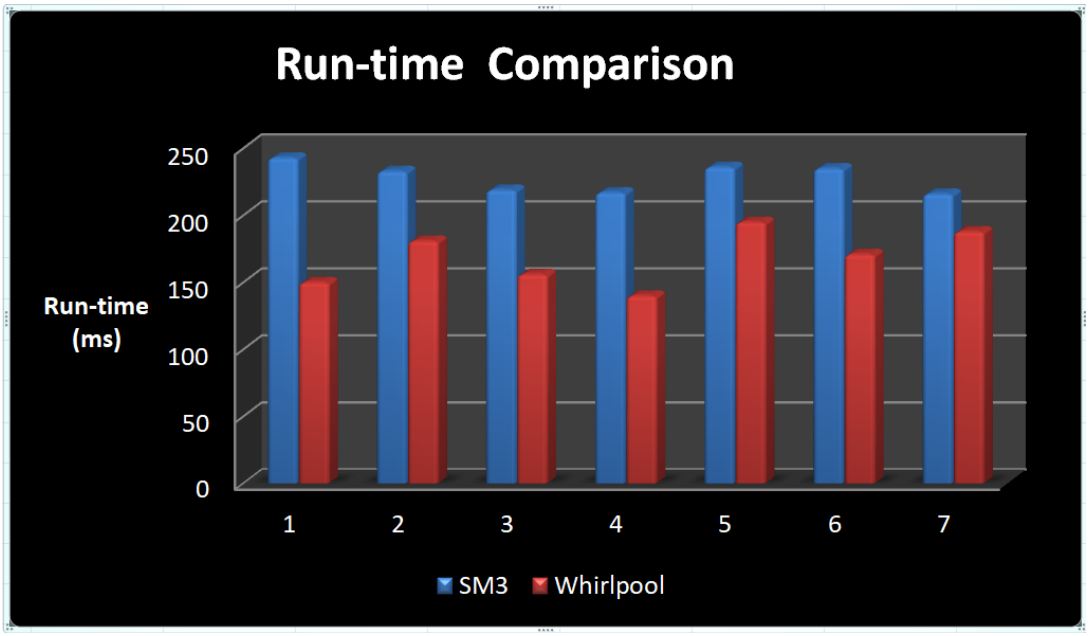


Figure 7.4: Run-time Comparison between SM3 and Whirlpool using 64 bits of Input

To generate the results attained, we compiled and ran our code at fixed time intervals for a total of 7 times. Both the Whirlpool operation and SM3 operation of 1000 hash generation were run at the same time.

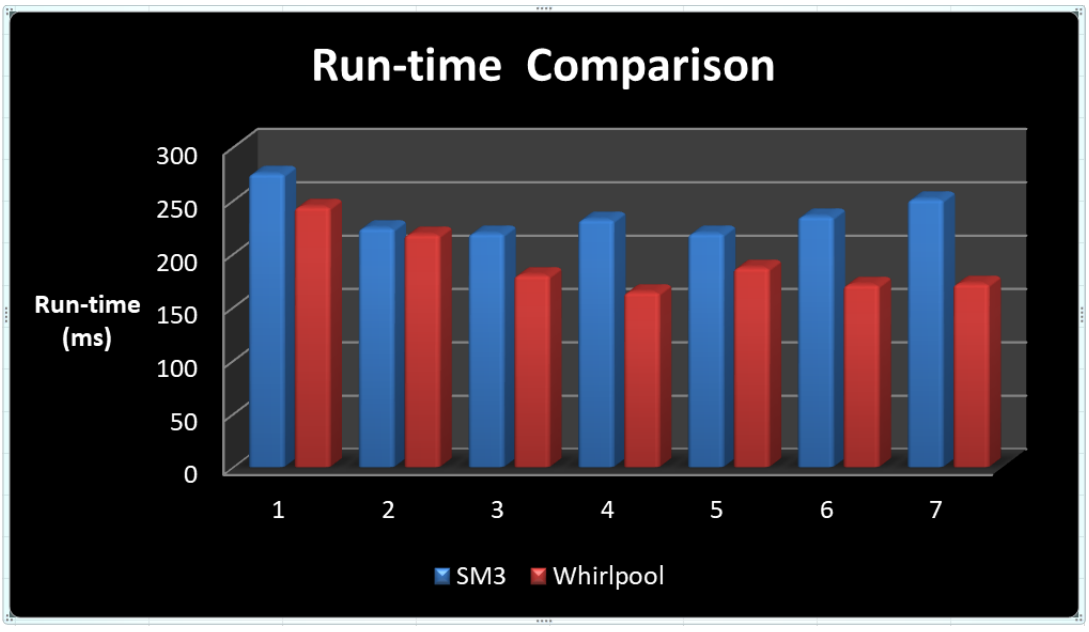


Figure 7.5: Run-time Comparison between SM3 and Whirlpool using 128 bits of Input

This was done so that the time taken for the Java Virtual (JVM) to compile, allocate and run the code would equally effect the run-time of the hash generation giving us a more accurate result.

5G is designed to support 100 times growth in providing traffic capacity and maintaining network efficiency. As it gives 10 gigabits per second (Gbps), i.e around 100 times faster than 4G, 5G networks can bring a massive rise in performance required for growing interconnected world. Whereas 4G takes 50 minutes for downloading an average high-definition video, 5G beat 4G by doing the same in just 9 minutes. This is due to increased data rates of at least 1 Gbps for tens thousands users at a time.

Feature	**Network**	
	4G	**5G**
Speed	100 Mbps	10,000 Mbps
Frequency Band	2 - 8 GHz	3 to 300 GHz
Latency	200 ms	1 ms
Data Bandwith	2 Mbps - 1 Gbps	1 Gbps or higher
Millimeter Wave Spectrums	4,000 devices/km^2	1 million devices/km^2
NB-IoT Device Performance	Upto 10 years	Upto 20 years

Table 7.4: Differences between 4G and 5G network

Lower latency is a prominent variation between 5G and 4G, which makes 5G an ultimate choice for modern work nerwork [26]. It can also increase the data transmission efficiency for NB-IoT devices as it has a reduced latency of 1 millisecond, far better that 4G having 200 millisecond latency as shown in Table 7.4.Its increased energy efficiency which results in upto 10 years for IoT devices performance, can increase the battery lifetime of NB-IoT devices for upto 20 years.

Chapter 8

Conclusion and Future Work

This paper represents our overview of the 5G Core network associated with NB-IoT that has better authentication based on PUF and key generation, providing faster secure connection and more UE support per eNB. We have discussed the representation of Whirlpool algorithm and mentioned its benefits. We have explored better and faster authentication using Whirlpool hash function along with PUF with promising performance for more secure NB-IoT networks. We also conducted simple a run-time performance test between SM3 and Whirlpool hash functions, which resulted in Whirlpool having the faster algorithm. Therefore, we have propose that it is much faster and significantly reliable to implement Whirlpool hash function than SM3 or SHA-256 for authenticating resources constrained devices such as NB-IoT devices over 5G network. With the increasingly extensive demand of Narrow Band IoT devices, the need for a more secure and faster authentication technique will always be on the rise. Further down the road, we would like to continue our research on this topic. Running test in Low Powered Low throughput devices and obtaining more accurate result to develop a more optimized and secure NB-IoT system. We also plan to get a deeper understanding of PUF systems and hope to find scopes of refinement in PUF for more secure authentication protocols.

References

[1] G. Association, *Nb-iot deployment guide to basic feature set requirements*, 2019. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf.

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019. DOI: 10.1109/COMST.2019.2910750.

[3] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, "Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot," in *2019 Global IoT Summit (GIoTS)*, 2019, pp. 1–6. DOI: 10.1109/GIOTS.2019.8766430.

[4] V. Kumar, R. K. Jha, and S. Jain, "Nb-iot security: A survey," in *Wireless Personal Communications*, vol. 113, 2020, pp. 2661–2708. DOI: 10.1007/s11277-020-07346-7.

[5] D. Liu, X. Liu, H. Zhang, H. Yu, W. Wang, L. Ma, J. Chen, and D. Li, "Research on end-to-end security authentication protocol of nb-iot for smart grid based on physical unclonable function," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 2019, pp. 239–244. DOI: 10.1109/ICCSN.2019.8905295.

[6] W. Stallings, "The whirlpool secure hash function," *Cryptologia*, vol. 30, no. 1, pp. 55–67, 2006. DOI: 10.1080/01611190500380090.

[7] Y. Hilewitz, Y. Yin, and R. Lee, "Accelerating the whirlpool hash function using parallel table lookup and fast cyclical permutation," in *Fast Software Encryption*, vol. 5086, Feb. 2008, pp. 173–188, ISBN: 978-3-540-71038-7. DOI: 10.1007/978-3-540-71039-4_11.

[8] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (nbiot): Architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16 739–16 776, 2019. DOI: 10.1109/ACCESS.2018.2881533.

[9] L. B. Martinkauppi and Q. He, *Performance evaluation and comparison of standard cryptographic algorithms and chinese cryptographic algorithms*, May 2009. [Online]. Available: http://www.diva-portal.se/smash/get/diva2:1332244/FULLTEXT01.pdf.

[10] L. B. Martinkauppi, Q. He, and D. Ilie, "On the design and performance of chinese oscca-approved cryptographic algorithms," in *2020 13th International Conference on Communications (COMM)*, 2020, pp. 119–124. DOI: 10.1109/COMM48946.2020.9142035.

[11] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for nb-iot terminals in 5g networks," *IEEE Access*, vol. 7, pp. 114 721–114 730, 2019. DOI: 10.1109/ACCESS.2019.2936123.

[12] P. Salva, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5g nb-iot: Efficient network traffic filtering for multitenant iot cellular networks," *Security and Communication Networks*, vol. 2018, pp. 1–12, 2018. DOI: 10.1155/2018/9291506.

[13] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science (New York, N.Y.)*, vol. 297, no. 5589, Aug. 2002. DOI: 10.1126/science.1074376.

[14] Y. Lin, F. Jiang, Z. Wang, and Z. Wang, "Research on puf-based security enhancement of narrow-band internet of things," in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, 2018, pp. 702–709. DOI: 10.1109/AINA.2018.00106.

[15] *3gpp ts 36.331 version 13.2.0 release 13*, 3GPP, Aug. 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.02.00_60/ts_136331v130200p.pdf.

[16] *33gpp ts 36.305 version 14.2.0 release 14*, 3GPP, Jul. 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136300_136399/136305/14.02.00_60/ts_136305v140200p.pdf.

[17] *3gpp ts 22.186 version 15.4.0 release 15*, 3GPP, Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122100_122199/122186/15.04.00_60/ts_122186v150400p.pdf.

[18] *33gpp ts 37.324 version 16.2.0 release 16*, 3GPP, Nov. 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/137300_137399/137324/16.02.00_60/ts_137324v160200p.pdf.

[19] B. Clauss, *Choosing the right hashing algorithm - it's all about slowness*, Mar. 17, 2019. [Online]. Available: https://www.novatec-gmbh.de/en/blog/choosing-right-hashing-algorithm-slowness/.

[20] P. Kitsos and O. Koufopavlou, "Efficient architecture and hardware implementation of the whirlpool hash function," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 208–213, 2004. DOI: 10.1109/TCE.2004.1277864.

[21] M. McLoone, C. McIvor, and A. Savage, "High-speed hardware architectures of the whirlpool hash function," in *Proceedings. 2005 IEEE International Conference on Field-Programmable Technology, 2005*, IEEE, 2005. DOI: 10.1109/FPT.2005.1568539.

[22] T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, and B. Schott, "Comparative analysis of the hardware implementations of hash functions sha-1 and sha-512," in *Information Security*, Oct. 2007, pp. 75–89, ISBN: 978-3-540-44270-7. DOI: 10.1007/3-540-45811-5_6.

[23] F. Crowe, A. Daly, T. Kerins, and W. Marnane, "Single-chip fpga implementation of a cryptographic co-processor," in *Proceedings. 2004 IEEE International Conference on Field- Programmable Technology (IEEE Cat. No.04EX921)*, 2004, pp. 279–285. DOI: 10.1109/FPT.2004.1393279.

[24] R. Lien, T. Grembowski, and K. Gaj, "A 1 gbit/s partially unrolled architecture of hash functions sha-1 and sha-512," in *Topics in Cryptology–CT-RSA 2004*, vol. 2964, Jan. 2004, pp. 1995–1995, ISBN: 978-3-540-20996-6. DOI: 10.1007/978-3-540-24660-2_25.

[25] P. Kitsos and O. Koufopavlou, "Whirlpool hash function: Architecture and vlsi implementation," in *2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No.04CH37512)*, vol. 2, 2004, pp. II–893. DOI: 10.1109/ISCAS.2004.1329416.

[26] E. Hajlaouim, A. Zaier, A. Khlifi, J. Ghodhbane, M. B. Hameda, and L. Sbita, "4g and 5g technologies: A comparative study," in *2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, IEEE, 2020. DOI: 10.1109/ATSIP49331.2020.9231605.