Lightweight Security Solutions for LTE/LTE-A Networks

Soran Hussein

UNIVERSITÉ PARIS SUD

Comprendre le monde, construire l'avenir®

cnrs

LABORATOIRE DE RECHERCHE EN INFORMATIQUE

Université Paris-Sud

Ecole Doctorale Informatique Paris Sud

Laboratoire Recherche en informatique

Discipline : Computer Science

DOCTORAL THESIS

Defended 8/12/2014 by

Soran Sabah Hussein

Lightweight Security Solutions for LTE/LTE-A Networks

Advisor :	Dr. Lila Boukhatem	Université Paris-Sud
Co-advisor :	Pr. Steven Martin	Université Paris-Sud

Composition of the jury: :

Reviewers: :	Pr. Hakima Chaouchi	Institut Télécom Sud-Paris
	Dr. Hassnaa Moustafa	Intel Corporation
Examiners :	Pr. Joffroy Beauquier	Université Paris-Sud
	Dr.Thi-Mai-Trang NGUYEN	Université Pierre et Marie Curie, Paris 6
	Dr. Nadjib Ait saadi	Université Paris Est Créteil Val de Marne

Abstract

Recently, the 3rd Group Project Partnership (3GPP) has developed Long Term Evolution/ Long Term Evolution-Advanced (LTE/LTE-A) systems which have been approved by the International Telecommunication Union (ITU) as 4th Generation (4G) mobile telecommunication networks. Security is one of critical issues which should be handled carefully to protect user's and mobile operator's information. Thus, the 3GPP has standardized algorithms and protocols in order to secure the communications between different entities of the mobile network. However, increasing the security level in such networks should not compel heavy constrains on these networks such as complexity and energy. Indeed, energy efficiency has become recently a critical need for mobile network operators for reduced carbon emissions and operational costs. The security services in mobile networks such as authentication, data confidentiality and data integrity are mostly performed using cryptographic techniques. However, most of the standardized solutions already adopted by the 3GPP depend on encryption algorithms which possess high computational complexity which in turn contributes in consuming further energy at the different network communication parties. Data confidentiality which mainly refers to the protection of the user's information privacy is achieved at the Packet Data Convergence Protocol (PDCP) sub-layer in the LTE/LTE-A protocol stack by one of the three standardized algorithms (EEA1, EEA2 and EEA3). However, each of the three algorithms requires high computational complexity since they rely on Shannon's theory of encryption algorithms by applying confusion and diffusion for several rounds. In this thesis, we propose a novel confidentiality algorithm using the concept of substitution and diffusion in which the required security level is attained in only one round. Consequently the computational complexity is considerably reduced which in return results in reducing the energy consumption during both encryption and decryption procedures. Similarly, the same approach is used to reduce the complexity of 3GPP data integrity algorithms (EIA1, EIA2 and EIA3) which the core cipher rely on the same complex functions. Finally, we investigate in this thesis the authentication issue in Device to Device paradigms proposal in 4G systems. Device to Device communications refer to direct communications between two mobile devices without passing through the core network. They constitute a promising mean to increase the performance and reduce energy consumptions in LTE/LTE-A networks. In such context, the authentication and key derivation between two mobile devices have not been well investigated. Thus, a novel lightweight authentication and key derivation protocol is proposed to authenticate two communicating devices during session establishments as well as deriving necessary keys for both data encryption and integrity protection.

Résumé

Récemment, le 3GPP (3rd Generation Partnership Project) a standardisé les systèmes LTE/LTE-A (Long Term Evolution/LTE-Advanced) qui ont été approuvés par l'UIT (Union Internationale des Télécommunications) comme des réseaux de télécommunications mobiles de 4éme génération. La sécurité est l'une des questions essentielles qui doivent être traitées avec soin pour protéger les informations de l'opérateur et des utilisateurs. Aussi, le 3GPP a normalisé plusieurs algorithmes et protocoles afin de sécuriser les communications entre les différentes entités du réseau. Cependant, l'augmentation du niveau de sécurité dans ces systèmes ne devrait pas leur imposer des contraintes lourdes telles qu'une grande complexité de calcul ou encore une forte consommation d'énergie. En effet, l'efficacité énergétique est devenue récemment un besoin critique pour les opérateurs afin de réduire l'empreinte écologique et les coûts opérationnels de ces systèmes. Les services de sécurité dans les réseaux mobiles tels que l'authentification, la confidentialité et l'intégrité des données sont le plus souvent effectués en utilisant des techniques cryptographiques. Toutefois, la plupart des solutions standardisées déjà adoptées par le 3GPP dépendent des algorithmes de chiffrement qui possèdent une grande complexité, induisant une consommation énergétique plus élevée dans les différentes entités communicantes du réseau. La confidentialité des données, qui se réfère principalement au fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, est réalisée au niveau de la sous-couche PDCP (Packet Data Convergence Protocol) de la pile protocolaire de LTE/LTE-A par l'un des trois algorithmes normalisés (EEA1, EEA2 et EEA3). Or, chacun des trois algorithmes exige une forte complexité de calcul car ils reposent sur la théorie de chiffrement de Shannon qui utilise les fonctions de confusion et de diffusion sur plusieurs itérations. Dans cette thèse, nous proposons un nouvel algorithme de confidentialité en utilisant le concept de substitution et de diffusion dans lequel le niveau de sécurité requis est atteint en un seul tour. Par conséquent, la complexité de calcul est considérablement réduite ce qui entraîne une réduction de la consommation d'énergie par les fonctions de chiffrement et de déchiffrement. De plus, la même approche est utilisée pour réduire la complexité des algorithmes 3GPP d'intégrité des données (EIA1, EIA2 et EIA3) dont le concept de chiffrement repose sur les mêmes fonctions complexes. Enfin, nous étudions dans cette thèse le problème d'authentification dans le contexte du paradigme D2D (Device to Device communications) introduit dans les systèmes 4G. Le concept D2D se réfère à la communication directe entre deux terminaux mobiles sans passer par le cœur du réseau. Il constitue un moyen prometteur pour améliorer les performances et réduire la consommation d'énergie dans les réseaux LTE/LTE-A. Toutefois, l'authentification et la dérivation de clé entre deux terminaux mobiles dans le contexte D2D n'ont pas fait l'objet d'études. Aussi, nous proposons un nouveau protocole léger d'authentification et de dérivation de clé

permettant d'authentifier les terminaux D2D et de dériver les clés nécessaires à la fois pour le cryptage et pour la protection de l'intégrité des données.

Acknowledgements

I would like to express my heartfelt gratitude to the many people who have supported me as I completed my graduate studies and dissertation. First, I would like to sincerely thank my advisor, Dr. Lila Boukhatem, for providing continuous support and instructive guidance throughout my studies.
I present my sincere thanks to my co-advisor Prof. Steven Martin which he has supported me not only by providing a research assistantship, but also academically and emotionally through the rough road to finish this thesis.

I also owe a debt of gratitude to my colleagues of the Network Group in the Laboratory of the Research in Informatics (LRI), with special thanks to Dr. Hassan Noura who was a post doc at the time for being my another advisor to finish the thesis in time. I wish to thank the reviewers, Prof. Hakima Chaouchi and Dr. Hassnaa Moustafa , to have the patience to read this dissertation and to give me valuable and detailed comments on my thesis. Thanks also to all the members of the jury, as it is a great honor for me to have them to evaluate my work.

I would like to emphasize my love and thanks to my family, with special thanks to my mother and father, for providing a loving and supportive environment throughout my childhood that fostered my academic success and for continued support today.

Finally, I would also like to appreciate Kurdistan Regional Government's funding support during my 5 year study in France.

Contents

List of Figures

List of Tables

Abbreviations

1G	**1**st **G**eneration
2G	**2**nd **G**eneration
3G	**3**rd **G**eneration
3GPP	**3**rd **G**eneration **P**artenership **P**roject
4G	**4**th **G**eneration
AS	**A**symetric **E**ncryption
AES	**A**dvanced **E**ncryption **S**tandard
AKA	**A**uthentication and **K**ey **A**greement
AS	**A**ccess **S**tratum
BIC	Output **B**it**I**ndependence **C**riterion
CK	**C**iphering **K**ey
CMAC	**C**ipher-based **M**essage **A**uthentication **C**odes
D2D	**D**evice to **D**evice
DC	**D**ata **C**onfidentiality
DI	**D**ata **I**ntegrity
DoS	**D**enial **o**f **S**ervice
DP_F	**D**ifferential **P**robability Approximation Boolean **F**unction
ECC	**E**lliptic **C**urve **C**ryptography

ECDF	**E**lliptic **C**urve **D**iffie-**H**ellman
EEA	**E**PS **E**ncryption **A**lgorithm
EIA	**E**PS **I**ntegrity **A**lgorithm
EPS	**E**volved **P**acket **S**ystem
EPC	**E**volved **P**acket **C**ore
ERCA	**E**fficient **a**nd Robust **C**ipher-**A**lgorithms
eNB	**e**NodeB
E-UTRAN	**E**volved -**U**niversal **T**errestrial **R**adio **A**ccess **N**etwork
FN	**F**eistel **N**etworks
GSM	**G**lobal **S**system for **M**obile communications
GMAC	**G**alois **M**essage **A**uthentication **C**odes
HSS	**H**ome **S**ubscriber **S**erver
HMAC	**H**ash **M**essage **A**uthentication **C**odes
IBC	**I**dentity **B**ased **C**ryptography
IK	**I**ntegrity **K**ey
IP	**I**nternet**P**rotocol
KHF	**K**eyed **H**ash **F**unctions
LFSR	**L**inear **F**eedback **S**hift **R**egister
$\boldsymbol{LP_F}$	**L**inear **P**robability Approximation Boolean **F**unction
LSB	**L**east **S**ignificant **B**it
LTE	**L**ong **T**erm **E**volution
LTE-A	**L**ong**T**erm **E**volution **A**dvanced
MAC	**M**essage **A**uthentication **C**odes
MDC	**M**essage **D**etection **C**odes
MitM	**M**an **i**n **t**he **M**iddle

MME	**M**obility **M**anagement**E**ntity
MTC	**M**achine **T**ype **C**ommunications
NAS	**N**on **A**ccess **S**tratum
NIST	**N**ational **I**nstitute of **S**tandareds and **T**echnology
PDCP	**P**acket **D**ata **C**onvergence **P**rotocol
PKG	**P**rivate **K**ey **G**enerator
PDNGW	**P**acket **D**ata **N**etwork **G**etWay
RNC	**R**adio **N**etwork **C**ontroller
SAC	**S**trict **A**valanche **C**riterion
SDN	**S**ubstitution **D**iffusion **N**etwork
SE	**S**ymetric **E**ncryption
SG	**S**ervice **G**etway
SN	**S**ervice **N**etwork
SAE	**S**ystem **A**rchitecture **E**volution
UE	**U**ser **E**quipment
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
WMN	**W**ireless **M**esh **N**etwork

Chapter 1

Introduction

1.1 Overview

The continuous and rapid growth of mobile data consumption especially due to the tremendous increase of Smartphone device usage has motivated the standardization organizations to develop 4G technologies such as (Long Term Evolution/Long Term Evolutions-Advanced) LTE/LTE-A, moving to higher data rates compared to 3G networks. This 4G systems deployment has triggered the transition from the existing 3G combined circuit and packet switching network to an all IP (Internet Protocol) architecture system which made LTE/LTE-A networks to possess a new and different security architecture.

With the proliferation of mobile networks usage in our daily live, security has attracted more and more attentions in order to ensure that the system is properly functioning without any fault or misuse. Security is provided through features such as encryption, integrity protection and authentication, which are required to guarantee the user's privacy as well as ensuring revenue for the mobile network operators [1]. The security architecture of mobile networks has been subject to subsequent evolutions. The first analog generation was in lack of any security mechanisms which later evolved within the definition of successive generation of 3GPP: Global System for Mobile communications (GSM) then 3GPP Universal Mobile Telecommunication System (UMTS) and now 3GPP LTE/LTE-A. The GSM has rather concentrated on the protection of the air interface. Then, substantial improvements have been adopted for UMTS security, such as adding new security features for radio access networks and services [2].
Security features as many other features of mobile networks should possess world-wide interoperability to achieve global relevance and this is done through the standardization

of these features. Accordingly, the 3GPP which is the main dominant standardization organization for mobile networks has handled the security issues in 4G LTE/LTE-A systems through the normalization of the protocols and algorithms at different network security levels. At the network access level, authentication of the users and key agreement are performed through EPS-AKA protocol, an authentication protocol based on symmetric cryptography. Moreover, in order to achieve user's privacy i.e. data confidentiality, the 3GPP has standardized for 4G LTE/LTE-A networks three algorithms EEA1, EEA2 and EEA3. Similarly, three other algorithms have been standardized for data integrity (EIA1, EIA2 and EIA3) [3].

Nowadays one of the important issues which have significant negative impact on global health, social and economic wellbeing is global warming which is resulted from excessive Carbon Dioxide (CO2) emissions in the atmosphere. Currently, wireless and mobile technologies contributes in about 2 to 3 percent of the overall emission of CO2 into the atmosphere and this amount is subjected to further increase due to the exponential growth in wireless and mobile networks subscribers and usages [4]. Later studies have proved that the largest part of the consumed power in wireless and mobile networks is located in the base stations, but an important part is also consumed in the mobile terminals [5]. Yet, considerable computation power is requested when performing security services in LTE/LTE-A networks which are carried out at base stations (denoted as eNodeB (eNB)) and mobile terminals denoted as (User Equipments (UE)). Furthermore, during the standardization procedure, the main objectives of the selected algorithms and protocols were achieving maximum security without taking in consideration any environmental or ecological issues such as energy savings. Therefore, it would be desirable to consider new design structures for new protocols and algorithms acquiring less computational power to reduce energy consumptions and consequently contributing in the reduction of CO2 emissions.
In the light of all above considerations, our objective in this thesis is to propose lightweight security algorithms and more particularly Data Integrity (DI) and Data Confidentiality (DC) algorithms by designing efficient cipher algorithms in terms of complexity and at the same time possessing sufficient security strength. These objectives will be achieved by exploring the compromise between these two controversial properties (less complexity and maximum security).

Another objective of our work is to consider the security issue in D2D paradigms. Recently, Device to Device (D2D) communications have attracted large research attention to develop efficient solutions for direct communications between two proximate devices

without passing through a base station or another third-party device. Indeed, the majority of D2D related research works concentrate mainly on licensed band (in band) modes using cellular resources where the service providers prefer to maintain a stable and permanent control over the communication rather than using other uncontrolled environments (out band) such as (ad hoc Wi-Fi and Bluetooth) networks using unlicensed bands [6]. The D2D paradigm has been proposed to be employed in cellular LTE/LTE-A networks between two UEs in order to enhance the performance. It has been adopted by 3GPP in LTE Release 12 to enable LTE becoming a competitive broadband communication technology for public safety networks [7]. These type of communications allow the eNBs to reduce their power consumption through decreasing the signaling load since the two UEs will not use the cells resources for communication. In addition, the UEs will also save a portion of energy during data transmission since a closer transmission path is expected between the two devices. To authenticate the UEs as well as providing necessary keys for DC and DI during D2D communications, a secure and efficient protocol is requested. However, although 3GPP has already adopted EPS-AKA as an authentication protocol for UEs, the concept of D2D have not been considered in this protocol. Hence, developing an efficient and secure authentication protocols for D2D poses a new research challenge which have not been well investigated in the literature. Another objective in our thesis is to investigate this research issue and also providing efficient and secure solutions.

1.2 Research objectives

1.2.1 Lightweight data integrity and data confidentiality algorithms

According to 3GPP, five security levels are defined in LTE/LTE-A security architecture: network access, network domain, user domain, application domain and non 3GPP domain security [8]. In this thesis, we are mainly concentrating on network access security and specifically between UE and eNB. However, to ensure a secure communication between any two communication nodes DC and DI security services are inevitable in any security system. DC refers to the prevention of an unauthorized disclosure of data between two communication nodes to the third party attackers or intruders, such as individuals, entities or processes. While DI is used to ensure that the received data has not been modified during transmission. In LTE/LTE-A system architecture as described in [9], UE and eNB are connected through the Access Stratum (AS) protocol, where both DC and DI security features are carried out in the Packet Data Convergence Protocol (PDCP) sub-layer. The PDCP performs ciphering/deciphering of both user and the control plane data at both UE and eNB sides, similarly it performs DI but only

for control plane data. The keys to be used by PDCP are managed by upper layers and derived during authentication procedure. Although the 3GPP has already standardized till now three pairs of algorithms; (EEA1, EIA1), (EEA2, EIA2) and (EEA3, EIA3) [10], [11] to achieve DC and DI, these solution are mostly require high computational time and some of them surfers from security flaws. Therefore, it becomes vital to propose lightweight and effective algorithms offer the decreased computational time and at the same time a strong security level.

1.2.2 Authentication key agreement protocol for D2D communications

Direct communications between two device terminals, denoted as D2D in LTE/LTE-A systems is a new paradigm in 4G mobile networks and has not been yet standardized. Our first contribution suggested two algorithms for the two services DC and DI for achieving privacy and integrity of users data could also be employed in D2D communications by the two involved UEs. However, to the best of our knowledge D2D key management and users' authentication has not been yet addressed. 3GPP stated that LTE /LTE-A networks should use EPS-AKA protocol for mutual authentication between UEs and the core network which is a long and costly process. Moreover, the EPS-AKA protocol is designed to rely on several entities in the core network which are not necessarily available during D2D communications. Henceforth, it is desirable to propose for such communication scenarios a novel method to achieve authentication as well as deriving the necessary keys for DC and DI services.

1.3 Thesis's Contributions

Following the aforementioned research objectives, the contributions of this thesis can be summarized as follows:

1.3.1 Novel and lightweight data confidentiality algorithm for LTE/LTE-A networks

Shannon demonstrated in [12] that the conventional technique to obtain a powerful encryption of a block of bytes is achieved by using the confusion and diffusion layers for several rounds. The standard ciphers are based on r multi-round functions, where each one is composed of several simple iterated functions. Round functions can be categorized into two classes: Feistel Networks (FN) and Substitution Diffusion Networks (SDN).

Accordingly, the security level depends on the number of rounds, which leads to a trade-off between the security level and the required computational time (complexity) and consequently the energy consumption. The multi round concept has been well applied in the standardized solutions. In this thesis, we propose a novel stream cipher technique based on SDN structure which showed a reduced complexity (one round only) and at the same time possesses similar security strength compared to the standardized solutions. The proposed stream cipher algorithm candidate has an almost-similar architecture as the Advance Encryption Standard (AES) employed in EEA2 and EIA2. It consists of an addition, a substitution and a diffusion layer. The addition layer uses binary XOR operation with a constant block value to ensure key uniformity. The substitution layer is constructed from the nonlinear transformation of RC6 algorithm to add confusions to the cipher. Finally, the diffusion layer is built from the output of the substitution layer by forming a sub-matrix.

1.3.2 Novel and lightweight data integrity algorithm for LTE/LTE-A networks

The DI is performed using cryptographic hash functions that convert strings of variable lengths to fixed-size strings called hash values, hash codes or simply hash. Cryptographic hash functions can be keyed or un-keyed. The un-keyed ones are called Modification Detection Codes (MDCs) which provide only data integrity. The keyed hash functions are Message Authentication Codes (MACs), which besides the integrity protection helps in the authentication of the origin of the data. The EIA algorithms use universal keyed hash functions to generate a 32-bit MAC value based on key streams generated from a stream cipher.

As LTE/LTE-A networks intend to support high data rates and an enhanced data, voice, and video experience for end users, it is desirable to develop a low computation DI algorithm to speed up data processing and at the same time reducing the computational power to save energy. Our second contribution in this thesis it to propose a new DI algorithm based on a Keyed Hash Function (KHF). The key advantage of this proposed algorithm is the use of a Substitution Diffusion (SD) technique in its core cipher which requires only one round of processing instead of several processing rounds as it is the case for the standardized reference solutions. However, in addition to the addition, substitution and diffusion layers, a chaining layer has also been employed in the core cipher to provide more bit dependency to the algorithm.

1.3.3 Authentication and key agreement scheme for D2D communications

Our last contribution consists in the design of a lightweight authentication and key derivation protocol between the two UEs communicating through a D2D link. Our proposed solution is based on the concept of elliptic curve cryptography which is considered as a promising tool for such security requirements, since the key exchange is done by a secure manner without the diffusion of the real identity of the communication nodes. This concept has been already employed in the security and authentication of vehicular Ad Hoc networks, Mobile ad hoc networks, and authentication of Machine Type Communications (MTC) and MTC group communications.

The key idea of our methodology is, in one hand using Elliptic Curve Diffie-Hellman (ECDH) to realize Key Forward/Backward Security (KFS/KBS) and performing authentication between the two devices and on the other hand using secured hash functions to derive both the ciphering and integrity keys which can be employed as DC and DI keys respectively. Our simulation analysis proved that our authentication protocol has the same security level as EPS-AKA and can also resist MitM, DoS and replay attacks while requiring minimum computation and communication complexity.

1.4 Organization of the Thesis

The content of this thesis is organized as follows:

- Chapter 2 describes the security architecture of LTE/LTE-A mobile networks. After a general overview of LTE/LTE-A systems, their different security levels are presented with a particular focus on the access level security. Then the EPS-AKA authentication and key derivation protocol is presented followed by a detailed description of the key derivation procedure and the related enhanced protocols proposed in the literature. The standardized algorithms proposed by the 3GPP for both DI and DC services are described with a discussion about their identified security flaws and drawback.

- In Chapter 3 we first introduce an overview of data confidentiality as well as the paradigms used to perform it. Then, the realization of a confidentiality algorithm in LTE/LTE-A networks is described. After, our proposed data confidentiality algorithm we baptized ERCA is presented which consists of three layers and a

detailed description about the functionality of each layer is presented. Finally, the analysis of simulation results is presented to prove the security strength of the ERCA and compared it to a current standard in terms of complexity.

- Chapter 4 presents ERADI, our lightweight data integrity algorithm for LTE/ LTE-A systems. First, we introduce briefly the general aspects and methodologies of data integrity. Then, the realization of a data integrity algorithm in LTE/LTE-A networks is illustrated. Hence, ERADI algorithm is detailed. ERADI is based on a keyed hash function which the core cipher is composed from four layers and a detailed description is given about each layer. Extensive simulation are carried out to prove the security strength and the efficiency of the proposed hash function.

- Chapter 5 first, presents an overview of D2D communications in LTE/LTE-A systems and the concept of authentication and key agreement in D2D. Then, D2D authentication and key managements in other mobile and wireless technologies is detailed. Hence, we detail the main arguments which make. Thereafter, we introduce the main concepts and operational steps of our lightweight authentication and key agreement scheme is presented for LTE/LTE-A D2D communications. Finally, the security analysis shows the effectiveness of our proposal as regards to the reference approaches.

- In the final chapter (Chapter 6) we review the main contributions of this dissertation and provide some perspectives and directions for future researches.

Chapter 2

LTE/LTE-A Security Architecture

2.1 Background

The 3rd Generation Partnership Project (3GPP) standardized LTE in its Release 8 as the successor of the Universal Mobile Telecommunications System (UMTS) standard in order to provide a high-data rate, low-latency, and packet-optimized radio-access technology supporting flexible bandwidth deployments. The LTE standard has been finalized in 2009 and has been deployed by different mobile operators in different countries all around the world. However, the continuous growth of mobile traffic has lead to the evolution of radio technologies towards International Mobile Telecommunications-Advanced (IMT-Advanced) which is an ITU-R initiative for developing 4G global mobile standard. The 3GPP and IEEE 802.16 started to develop standards compatible with IMT-Advanced requirements. This was the driving force for 3GPP to further develop LTE towards LTE–Advanced in its Release 10 to provide higher data rates in a cost efficient way and at the same time, completely fulfill the requirements set by IMT-Advanced. Finally, the IMT-Advanced had selected the LTE-A along side with LTE as the candidate technologies for 4G mobile networks.

Because of the possible security threats in the 3G UMTS security architecture such as Man-in-the-Middle (MitM) attacks, rogue base station attacks and Deny of Service (DoS) attacks, better and enhanced security services were among the main goals of LTE/LTE-A and have been taken in to consideration from the start by addressing the security in many different levels. Instead of UMTS-Authentication and Key Agreement

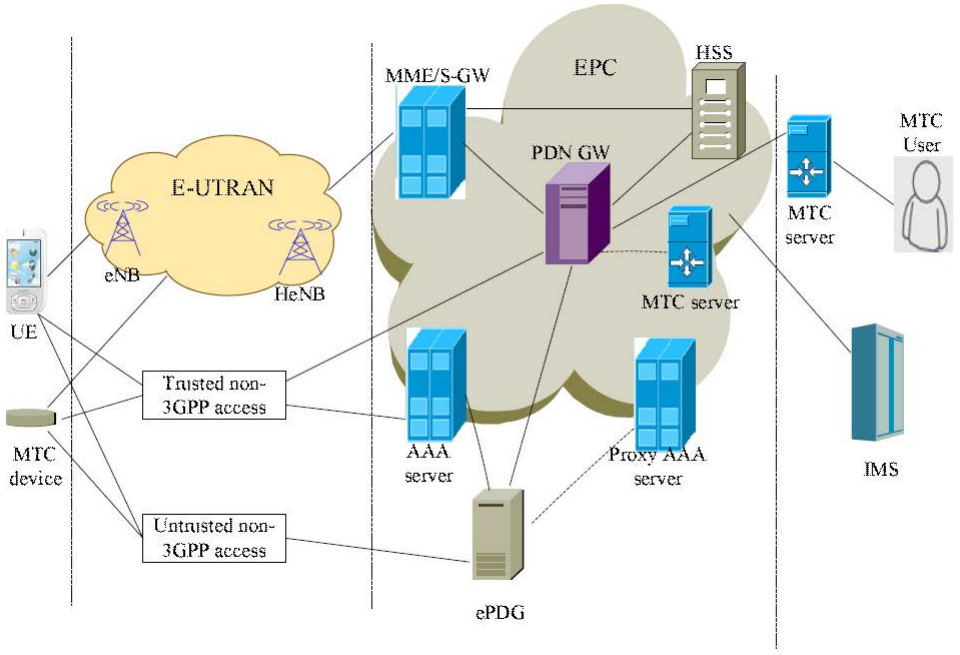


FIGURE 2.1: The LTE/ LTE-A architecture

(UMTS-AKA), the SAE/LTE architecture adapted an enhanced new access security approach. In addition, new standardized sets of algorithms have been proposed to achieve privacy and integrity protections. In this chapter, we first study the LTE/ LTE-A security levels, describing briefly how different security levels are achieved between the communication entities. Then, the security services supported by LTE/ LTE-A in the network access level are presented followed by a detailed description of each of the services as well as the algorithms and protocols employed to support them. Finally, we conclude the chapter with a discussion about the main security features and the limitations of current security services of LTE/LTE-A networks as well as the improvements suggested by our proposal.

2.2 Security levels and services of LTE/LTE-A networks

The security architecture of mobile networks has been subjected to subsequent evolutions since the first analog 1G system, which was in lack of the main security features such as authentication and data encryption. The Advanced Mobile Phone Service (AMPS), which was employed in the USA and its European version Total Access Communication System (TACS), provided no security services. Therefore, it was rather easy for an attacker to intercept the calls and consequently, extract Identification Number (MIN) and Electronic Serial Number (ESN). Similarly, the Nordic Mobile Telephone NMT, which

was mainly used in the European Nordic countries, Eastern Europe and Russia had the disadvantage that the voice traffic was not encrypted [8]. The security of 2G systems such as GSM has rather concentrated on the protection of the air interface. Several security services have been implemented for GSM such as authentication of subscribers, protection of subscriber's identity using SIM cards and finally the encryption of communication between the subscriber and the base station using A5/1 and A5/2 stream ciphers. However, serious weaknesses have been reported in both algorithms, as it is possible to break A5/2 in real-time using cipher-text-only attack.
The 3G systems security is based on those elements of 2G security that have proven to be robust and also important new security features and were services integrated while correcting the security issues of GSM by addressing its real weaknesses. Furthermore, key lengths were increased to allow for stronger algorithms of encryption and integrity [8].

The 4G LTE/LTEA architecture shown in Figure 2.1 and also denoted as Evolved Packet System (EPS) brings two new major ingredients into the 3GPP environment: the radio network Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) with a new radio interface, and the flat IP-based core network Evolved Packet Core (EPC). Additionally, the EPS must also be able to interwork with legacy systems and achieve backward-compatibility. In the (3GPP TS 33.401), the security architecture is divided into five different functional security levels or (domains) where different security services are achieved in these levels (see Figure 2.2). The 3GPP TS 33.401 defines these levels as the following:

- Network domain security (II): this security level mostly related to the protection of the control plane data as well as user plane data during transmission from the access network to the service network mostly through the wireline network.
- User domain security (III): it can be defined as the necessary security features to access for mobile terminals (UE in LTE/LTE-A) access.
- Application domain security (IV): stands for the set of security features that enable applications in the user and in the provider domains to securely exchange messages.
- Visibility and configurability of security (V): the set of features that enables the user to discover whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.
- Network Access security (I): this level is mainly related to the radio access network i.e. (E-UTRAN) and described as the set of security services that provide users with secure access to services and protecting the user against attacks. The subject

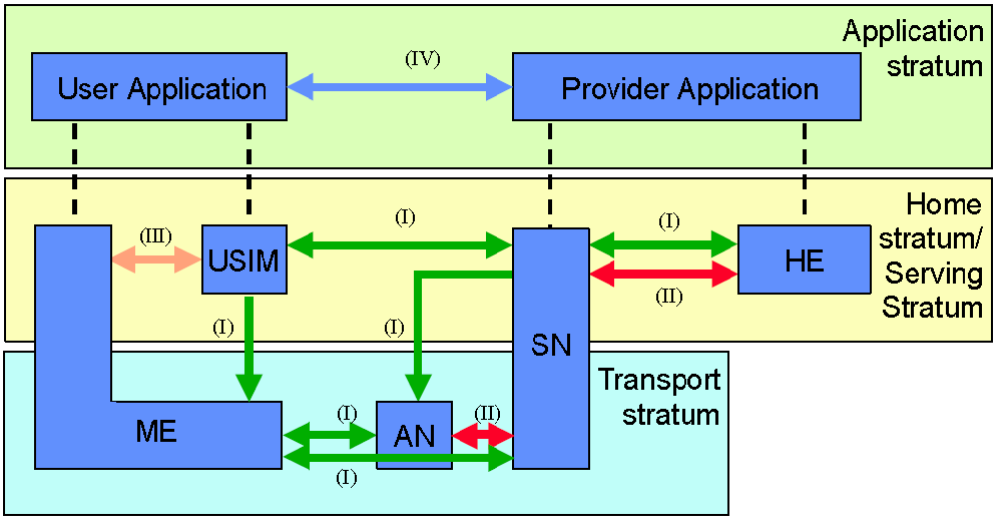


FIGURE 2.2: Security levels of LTE/LTE-A networks

of this thesis is particularly related to the network access security; therefore, the rest of this document is mainly related to this topic rather than to the other security levels.

In the following, we present the most important security services of EPS which are mostly performed in the access network level.

2.2.1 Authentication and key derivation

Mutual authentication between UEs and network and key derivation to establish key sessions for ciphering and integrity protection are essential security features for any mobile network. The EPS shall support authenticity of information between the mobile terminal and the network to ensure that unauthorized users cannot establish communications through the system. Moreover, without authentication it would be impossible to securely connect users to each other. Hence, the functionality of the whole system would be questionable if this feature is not available.

Compared to 3G systems where the authentication only provides assurance that the serving network is authorized by the home network to serve the user, there is an enhancement in EPS authentication that provides means for the UE to directly verify the serving network identity.

Indeed, the secret key derivation would be also tightly integrated with authentication where the derived shared secret keys are used for confidentiality and integrity protection during data transmission. The 3GPP adopted for LTE/LTE-A a new authentication and

key agreement protocol called EPS-AKA which will be described in details in section 2.3.

2.2.2 Confidentiality of user plane and control plane data

According to the 3GPP security requirements, EPS shall provide several appropriate levels of user privacy for communication, location, and identity. Additionally, communication contents, origin, and destination shall be protected against disclosure to unauthorized parties. Confidentiality is achieved by ciphering the digital communication in order to protect the content packets of being seen by the eavesdroppers especially on the radio interface. Unlike the 3G mobile systems where the end point of the encryption is the Radio Network Controller (RNC), in LTE/LTE-A the endpoint is in the eNB. Hence, additional confidentiality protection mechanism is introduced for Radio Resource Control (RRC) signaling (control plane data) between the UE and eNB [13]. Further details about confidentiality algorithms already adopted for LTE/LTE-A will be presented in section 2.4.

2.2.3 Integrity of control plane data

In order to fulfill 3GPP security requirements, EPS shall support authenticity of information between the mobile terminal and the network. The purpose of this feature is to ensure the authenticity of each control plane message separately i.e. assuring that the message has not been altered during transmission and has been received by the destination as it was actually sent by the source. However, no integrity protection is provided for user plane data in 4G LTE/LTE-A except for Relays as stated in [13]. In order to ensure data integrity, the 3GPP has standardized three algorithms which will be described in details in section 2.5

2.3 EPS Authentication and Key Agreement (EPS-AKA)

As illustrated in Figure 2.1, the LTE/LTE-A network is composed of the Evolved Packet Core (EPC) and the E-UTRAN. The EPC consists of a Mobility Management Entity (MME) and a Serving Gateway (SGW), a Packet Data Network Gateway (PDNGW) together with the Home Subscriber Server (HSS). When a UE connects to the EPC, the MME represents the EPC to perform a mutual authentication with the UE, whilst the E-UTRAN, including the eNB, passes the traffic from UE to MME. The AKA protocol for UTMS was adopted by the 3GPP and proposed at the network level for authenticating

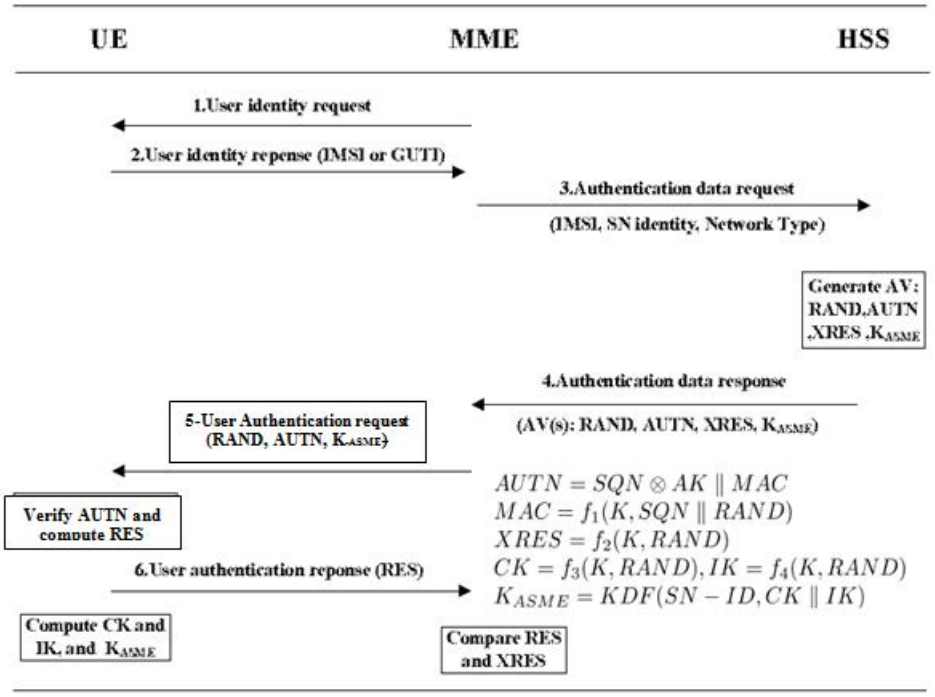


FIGURE 2.3: EPS-AKA procedure

3G mobile subscribers and also to tackle the vulnerabilities of the GSM system. Due to a substantial architecture modification of the 4G LTE/LTE-A, the AKA has been replaced by a new protocol (EPS-AKA) which is based on its predecessor in order to ensure backward compatibility. In this section the EPS-AKA procedure is described as well as the key derivation procedure and the functionality of the employed keys. Then, we highlight the weak and strong aspects of the protocol along with the various enhancements proposed by different research works.

2.3.1 EPS-AKA procedure

In the EPS-AKA protocol as illustrated in Figure 2.3, first the UE sends an access request message to the MME, then the MME launches an authentication procedure by interrogating the UE's identity. When the UE returns back its identity by sending its International Mobile Subscriber Identity (IMSI), the Service Network (SN) sends an authentication data request message containing UE's identity to the HSS for acquiring Authentication Vectors (AVs). Any AV consists of four parameters: an expected result (XRES), a network authentication token (AUTN), the intermediate key K_{ASME} (based on the CK and IK and other parameters such as the serving network identity (SN ID) as well as the random challenge (RAND). The HSS generates AVs for the MME and sends back an authentication data request message including the generated AV. Upon AVs

reception, the MME sends RAND and AUTN piggy backed on the authentication request to the UE enabling it verifying the correctness of the sequence number (SQN) associated with that IMSI and compute the RES. The validity of SQN is checked by computing MAC and comparing it with the MAC carried in AUTN. If so, the UE computes and sends the corresponding response RES back to the SN in an authentication response message. Once the MME receives and verifies RES validity, it chooses the corresponding intermediate key K_{ASME} as the session key to protect its communication with the UE. At the same time, the UE calculates its K_{ASME} accordingly. Finally, both the UE and MME hold a symmetric session key from which other encryption and integrity protection keys will be derived.

2.3.2 EPS key hierarchy

After the authentication, all necessary cryptographic keys for various security mechanisms are derived from the intermediate key (K_{ASME}). The main advantages of this key hierarchy are cryptographic key separation and also providing the system with key freshness property. However, the main disadvantage is adding further complexity to the system since there are more types of keys in the system, all of which need to be computed, stored and protected. Moreover, one of the most important properties of the key derivation procedure is the one-way property i.e. computing upper layers keys is impossible using lower layers keys. In the procedure of key derivations as illustrated in Figure 2.4, an arrow between two keys indicates that one key is derived from the other. However, there is one special arrow in the figure, namely the loop arrow pointing from the box representing keys K_{eNB}/NH to itself. Indeed, there are also additional parameters that will be mixed during keys derivation which are assumed not be secret. The topmost key derivation from K to CK and IK is different from the rest of key derivations in the sense that its details are not standardized [8]. Moreover, in Figure 2.5 the details of key derivation are presented in the network nodes. In the figure, KDF denotes the generic Key Derivation Function based on HMAC-SHA-256 and 'Trunc' stands for a simple truncation function that uses only the 128 least significant bits of a 256-bit value and eliminates the most significant half. In the following, the purpose and the functionality of each of the master and specific derived keys related to the network access security are explained:

- K is the subscriber-specific master key, stored in the USIM and the AuC and it is not derived from any other key.
- CK and IK are128-bit keys derived from K using additional input parameters.

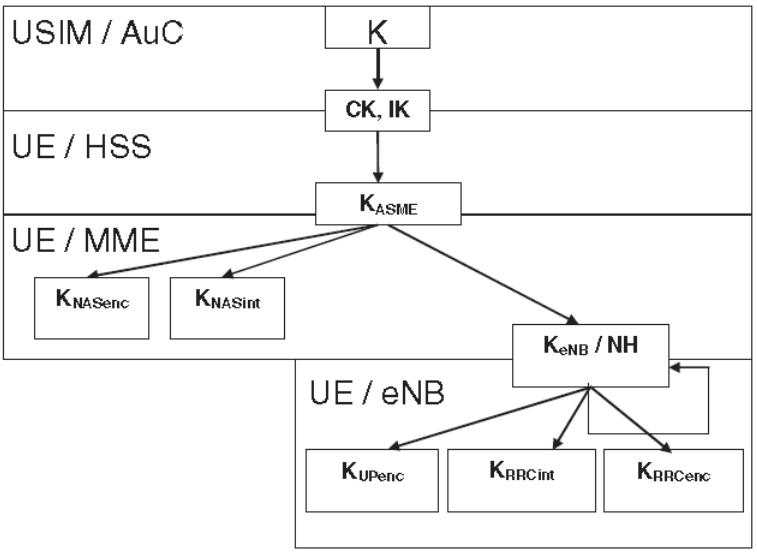


FIGURE 2.4: EPS key hierarchy

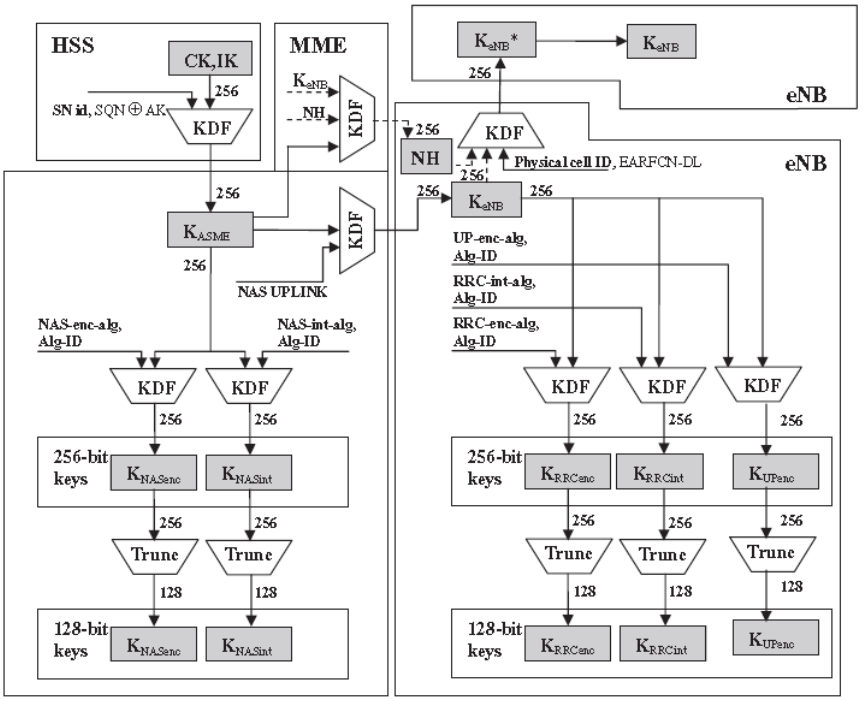


FIGURE 2.5: EPS key derivations on network side

- K_{ASME} is derived from CK and IK using two additional inputs to be a local master key in the MME.
- K_{eNB} is derived from K_{ASME} and the additional input NAS uplink COUNT which is a counter parameter. This parameter is needed to ensure that each new K_{eNB} derived from K_{ASME} differs from the ones derived earlier. The purpose of this key is to be a local master key in an eNB.
- K_{RRCenc} is a key that is used to encrypt RRC signaling traffic. It is derived from K_{eNB} and two additional parameters: the first one (algorithm type distinguisher) indicates that this key is used for RRC encryption, and the second one is the identifier of the encryption algorithm.
- K_{RRCint} is used to protect the integrity of RRC signaling traffic. It is derived from K_{eNB} and two parameters: the first one indicates that this key is used for RRC integrity, and the second one is the integrity algorithm identifier.
- Finally, K_{UPenc} is used to encrypt user plane traffic. This key is derived from K_{eNB} and two parameters: the first one indicates that this key is used for user plane encryption, and the second one is the encryption algorithm identifier.

The generated keys from the key hierarchy are separated in a way that each key has a specific usage for either control or user plane traffic. The principle idea behind this separation is providing more security since even though an attacker may find a key used for a specific context; he cannot easily get the other keys used for a different purpose. Additionally, a key renewal without affecting the other keys is another advantage of the key hierarchy. Accordingly, any change to a specific key, affects only the keys derived from in which affected and have to be changed; the other keys may remain the same.

2.3.3 EPS-AKA functionality and related works

Although EPS-AKA has several security improvements over UMTS AKA by preventing some attacks like redirection attacks, rogue base station attacks and MitM attacks, it still has some vulnerabilities inherited from UTMS AKA due to compatibility issues. Therefore, many research works were interested in overcoming these issues.
Privacy protection is among the main security flaws of EPS-AKA, which results from the diffusion of the IMSI mainly in plane-text in two typical scenarios [14]:

- In some cases, the SN cannot obtain UE Globally Unique Temporary Identity (GUTI) which is transmitted instead of IMSI to hide real identity of the UE, such

as when a UE registers to the network for the first time or during roaming which leads to the transmission of IMSI in a plane-text.

- In case of a MAC verification failure, a MAC failure message (Mac_Fail) is sent to the network to require a new MAC verification procedure. Therefore, the IMSI could be leaked in a plane-text.

The discloser of the IMSI enables an adversary to obtain sensitive information about the subscriber identity and consequently lunch identity related attacks. Moreover, the EPS-AKA is vulnerable to potential DoS attacks which may cripple the network when an adversary disguises as legitimate UE and constantly sends fake IMSIs to overwhelm the HSS/AuC. As a consequence, the HSS is overloaded by generating excessive AVs for the UE.

In order to overcome this drawback, several solutions have been proposed to improve the security of EPS-AKA. Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI) has been proposed in [15] in order to ensure the security of user identity using Elliptic Curve Cipher (ECC) encryption. The authors have employed the Elliptic Curve Diffie-Hellman (ECDH) with symmetric key cryptosystem to overcome the vulnerabilities presented in EPS-AKA protocol. Furthermore, the authors in [16] have proposed an ensured confidentiality authentication and key agreement (EC AKA) to enhance the user's confidentiality by protecting AKA messages through encryption. Consequently, the real identity of the subscriber is preserved and cannot be tracked. The drawbacks of the above mentioned methods are that they employ the public-key to overcome the shortcoming of the EPS-AKA protocol by ensuring the security communication between the UE and HSS/AuC through the use of the certificates. However, using certificates results in large number of computational, storage and communication costs.
Unlike the aforementioned works, the authors in [17] presented a slightly modified version of the EPS-AKA protocol to overcome its security flaws. The scheme introduces a new subscriber module ESIM instead of the USIM and provides a direct online mutual authentication between the ESIM and the MME/HSS with minor modifications of the access security architecture. However, this method does not attain the identity privacy and requires a lot of message exchange causing signaling congestion on the HSS [18].
The use of the password authentication key exchange by Juggling Password Authenticated Key Exchange (J-PAKE) protocol was proposed in [19]. The authors proposed the use of J-PAKE protocol for authentication due to its high flexibility and lightweight making it very well suited for use in mobile terminals. However, this protocol still suffers

from security issues presented in the EPS AKA protocol such as identity protection. Finally, the AES ciphering is used in EAP Archie method proposed in [20] was intended to achieve a mutual authentication and key agreement between the users and the network access layer. Yet, this scheme also suffers from the disclosure of the user identity and spoofing attacks.

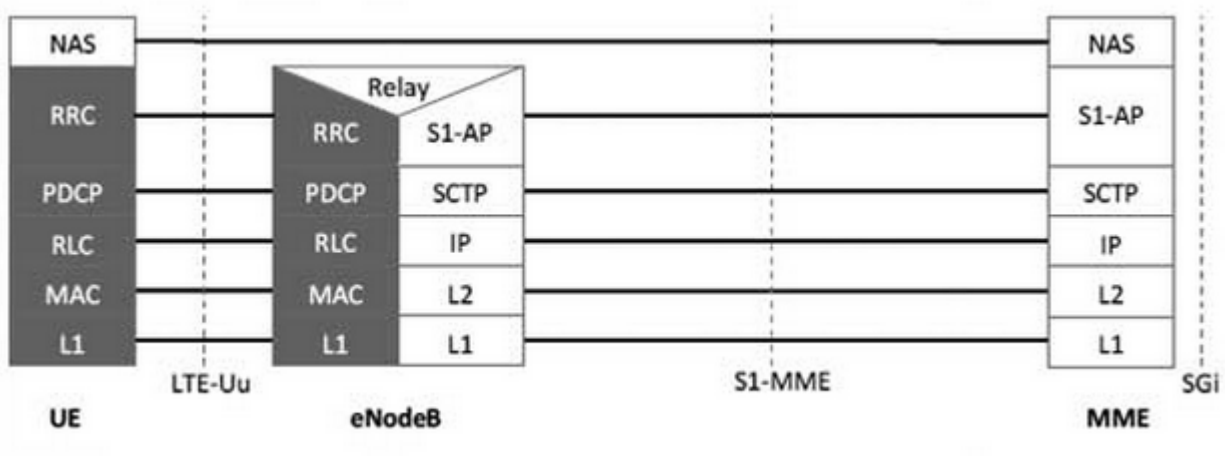


FIGURE 2.6: AS and NAS Protocols

2.4 EPS Encryption Algorithm (EEA)

As illustrated in Figure 2.6 the three main important components in LTE/LTE-A architecture where the security services are achieved are: UE, eNB and MME. Accordingly, UE and MME are connected with Non Access Stratum (NAS) security protocol and NAS messages exchanged between UE and MME are integrity protected and ciphered with extra NAS security header. While UE and eNB are connected through the Access Stratum (AS) protocol and the security services are performed for both control and user plane data in the (PDCP) layer of UE and eNB. The PDCP layer in UE and eNB sides is responsible for the confidentiality and integrity protection. The confidentiality cryptographic algorithm EPS Encryption Algorithm (EEA) is achieved after the authentication between the UE and SN is fulfilled by EPS-AKA. The EEA algorithm is assigned a 4-bit identifier included in K_{NASenc}, K_{RRCint} and K_{UPenc} to indicate the type of the encryption algorithm to be used. Accordingly, the 3GPP standardized three algorithms namely EEA1, EEA2 and EEA3 to be used in 4G LTE/LTE-A networks. A detailed description and convenient and inconvenient of each algorithm is given below.

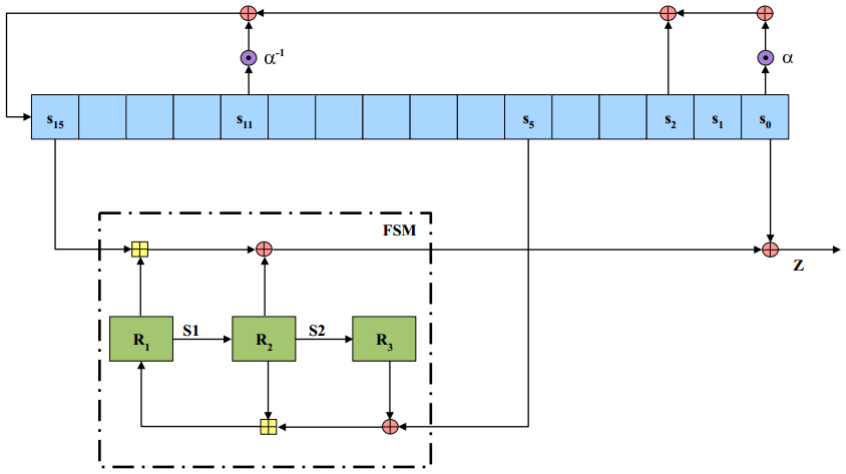


FIGURE 2.7: SNOW 3G Algorithm

2.4.1 EEA1

Four bits identifier "0001" is used for defining 128-bit EEA1 stream cipher which is based on another stream cipher of SNOW 3G depicted in Figure 2.7. SNOW 3G algorithm was originally used as the cryptographic kernel of the second set of 3G UMTS confidentiality and integrity algorithms (UEA2) and has been kept as the first set of security algorithms for LTE/LTE-A. Originally, SNOW 3G was derived from the stream cipher SNOW 2.0, with improvements against algebraic cryptanalysis and distinguishing attacks. It is a word oriented stream cipher that generates a sequence of 32-bit words using a 128-bit key and a 128-bit initialization variable [21]. The structure of SNOW 3G is composed of a Linear Feedback Shift Register (LFSR) with 16 chained 32-bit stages and a Finite State Machine (FSM) with 2 S-boxes. Although the authors in [22]are assuming a fault attack to recover the secret key with only 22 fault injections, but SNOW 3G still offers adequate protection against new forms of algebraic attacks. However, in terms of time complexity SNOW 3G is quite complicated especially in terms of hardware implementation [23].

2.4.2 EEA2

The four bit identifier "0002" is used to define the 128-bit EEA2 algorithm based on AES using CTR mode. It is a block cipher that can process data blocks of 128-bit (16 bytes block) using cipher keys of 128, 192 and 256 bits. Yet, the 3GPP adopted the128-bit cipher key as a standard for EEA2. The design of AES depends on the principle of SDN, as the encryption procedure for128-bit is composed of 10 rounds of processing. Each round except the last one includes four layers as shown in the Figure 2.8: *ByteSubstitution* layer (S-Box), $ShiftRow$ layer, $KeyAddition$ layer and $MixColumn$ layer, which will

be eliminated in the last round. First, a 128-bit round key is XORed to the state, then in the next layer a byte-by-byte substitution is performed using 16×16 look up table to provide the confusion property. Permutation is realized at the $ShiftRow$ layer at the byte level. Finally, $MixColumn$ layer combines blocks of four bytes by using a matrix operation. The $ShiftRow$ and $MixColumn$ layers provide the diffusion property. However, AES-CTR mode is similar to a stream cipher since, instead of encrypting the plain text directly, the counter is encrypted then Xored with the plain-text to produce the cipher-text for transmission. Until now no known attacks have been reported yet against AES. Apart from offering strong encryption via 128-bit keys, AES computational time is high since it uses 10 rounds of iterations [24].

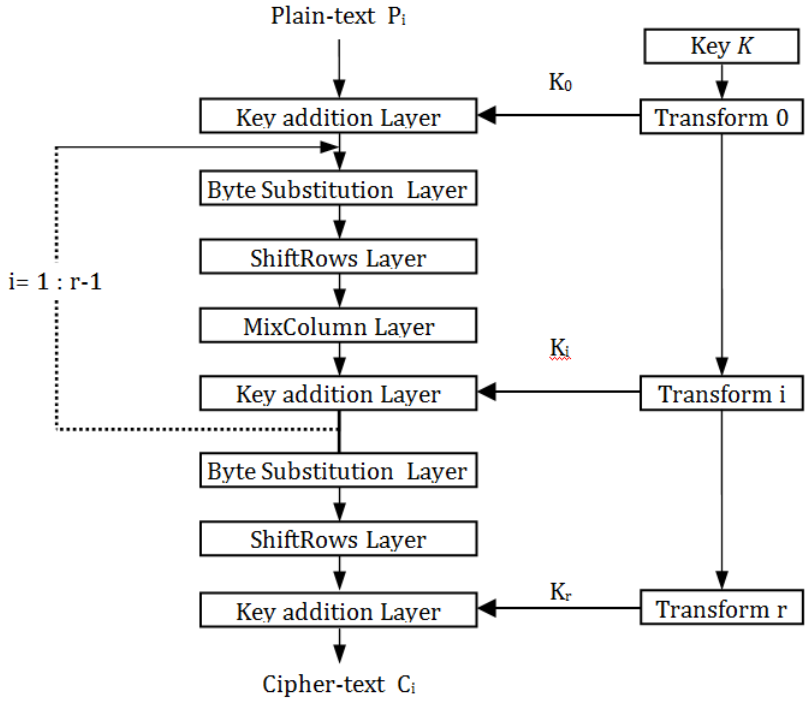


FIGURE 2.8: AES Algorithm

2.4.3 EEA3

The four bits identifier "0003" is used to define the 128-bit EEA3 algorithms and the core which is based on a new stream cipher called ZUC [11]. Although ZUC was designed by Chinese Academy of Science to be permitted for use in China. It is a word oriented cipher that takes as input a128-bit initial cipher key and a128-bit initial vector. The output is 32-bit word key-stream, also called key-word that would be used to encrypt/decrypt the plain text. The ZUC stream cipher as shown in the Figure 2.9 has three main

logical layers: LFSR, Bit-Reorganization (BR) and Non-Linear Function (NLF). The LSFR is composed of 16 registers, each one containing 31 bits and taking values from 1 to $2^{31} - 1$. Additionally, it has two modes of operation: the initialization mode and the working mode. During the initialization mode, LSFR takes a 31-bit input word computed by removing the rightmost bit from the XORing the cipher key and the initial vector. However, in the working mode, the LSFR does not receive any input. The BR makes four words by extracting 128 bits from LSFR states. The first three words are used by the NLF and the last one is used to construct a key-stream. Indeed, despite the fact that ZUC appears to have a sound design with a large security spectrum, it requires more analysis to gain further confidence [23].

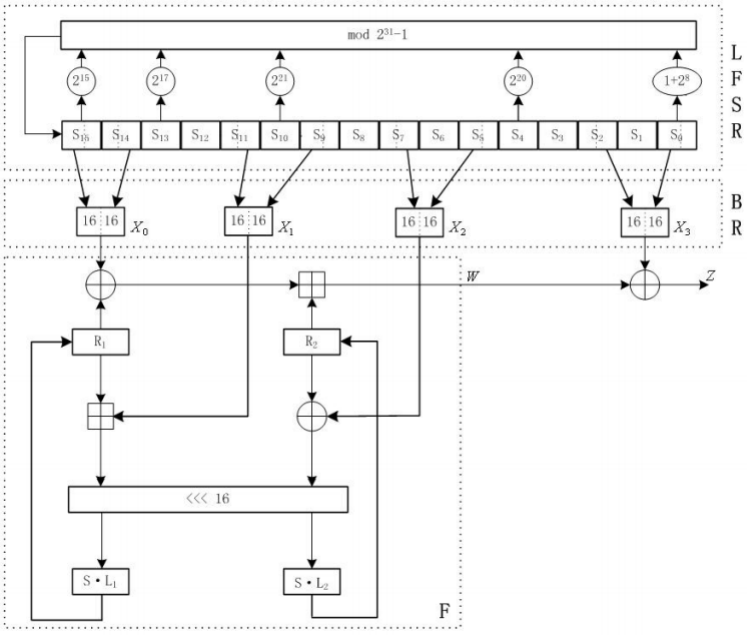


FIGURE 2.9: ZUC Algorithm

2.5 EPS Integrity Algorithms (EIA)

The 3GPP standardized three EIA algorithms to be used for data integrity in LTE/LTE-A. The main principle of the three standardized algorithms (EIA1, EIA2, and EIA3) is applying an under layer stream cipher as a tool to encrypt the public and secret keys, and making use of the encrypted result in the upper layer using secure hash functions to compute the MAC-I of the message. For a better understanding of the proposed solution, we present in the following the description and the flaws of each of the three standardized algorithms.

2.5.1 EIA1

EIA1, similarly to EEA1 is identified by 4 digits "0001" and is based on universal hashing and Galois Message Authentication Code (GMAC) scheme for the generation of the MAC [25]. The core cipher of EIA1 is based on SNOW 3G as illustrated in Figure 2.10. EIA1 suffers from two different forgery attacks as has been demonstrated by [26], the first attack is linear forgery attack, and the second one is known as a trace extension forgery attack. Furthermore, as already mentioned, the core cipher of SNOW 3G is quite complicated especially in terms of hardware implementation [23] .

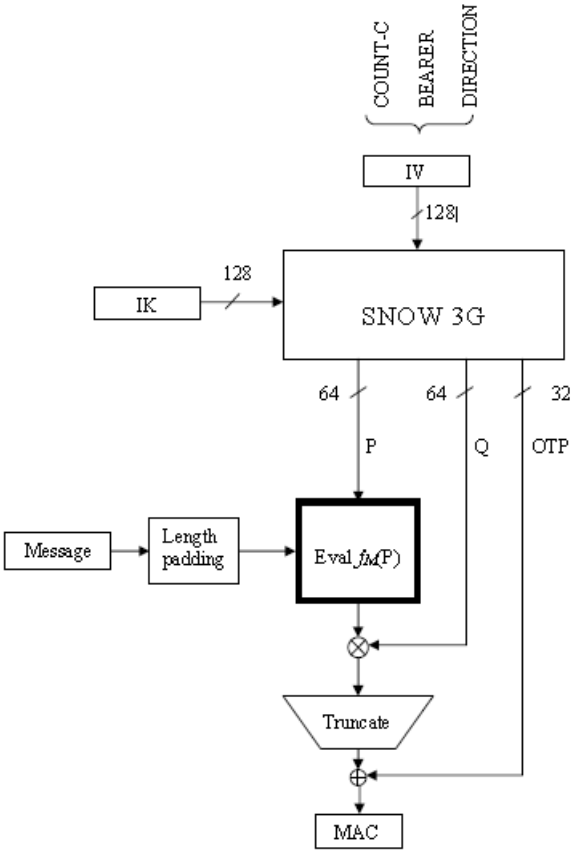


FIGURE 2.10: EIA1 Algorithm

2.5.2 EIA2

Likewise EEA2 the four digit "0002" is identifying the 128-bits EIA2. The cipher core of EIA2 is based on a 128-bit AES in the CMAC (cipher-based MAC) mode [27]. In CMAC mode as shown in Figure 2.11, a block cipher is used instead of a hash function. This mode is divided into two phases: Sub-key generation and MAC generation. The

IK is used to generate two sub-keys: K1 and K2 with 128-bits length each. To the best of our knowledge, there are no known attacks against EIA2. However, similar to EEA2 its computational time is high since its core cipher AES uses 10 rounds of iterations to produce the hash value for each message block.

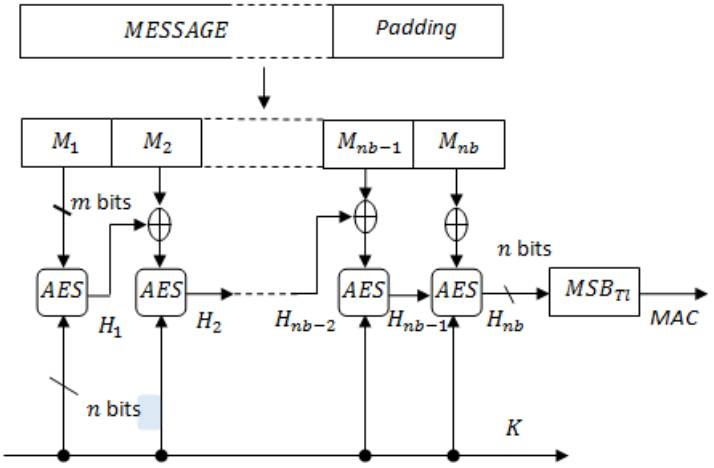


FIGURE 2.11: EIA2 Algorithm

2.5.3 EIA3

As for EEA3, a four bit identifier "0003" is used to define the 128-bit EIA3. The 128-EIA3 algorithm is based on a universal hashing and a one-time-pad masking, and uses the GMAC mode as EIA1. The EIA3 algorithm as depicted in Figure 2.12 takes as inputs to its ZUC core cipher a 128-bit IK and IV. However, like EIA1, EIA3 suffers from linear and trace extension forgery attacks [26]. In addition, as already mentioned, the computational complexity of EIA3 is also high since its core cipher ZUC uses multi round operations to achieve maximum diffusion and confusions.

2.6 Conclusions and Discussions

This chapter was dedicated to provide a general overview of the security architecture of LTE/LTE-A networks. The 3GPP has rigorously defined the security architecture of LTE/LTE-A networks and divide it into five different functional levels. The access level security constitutes the main objective of this thesis. Thus, the majority of the chapter was dedicated to the security services of the access level and more particularly between UE and eNB. Furthermore, the three main security features in the access network namely

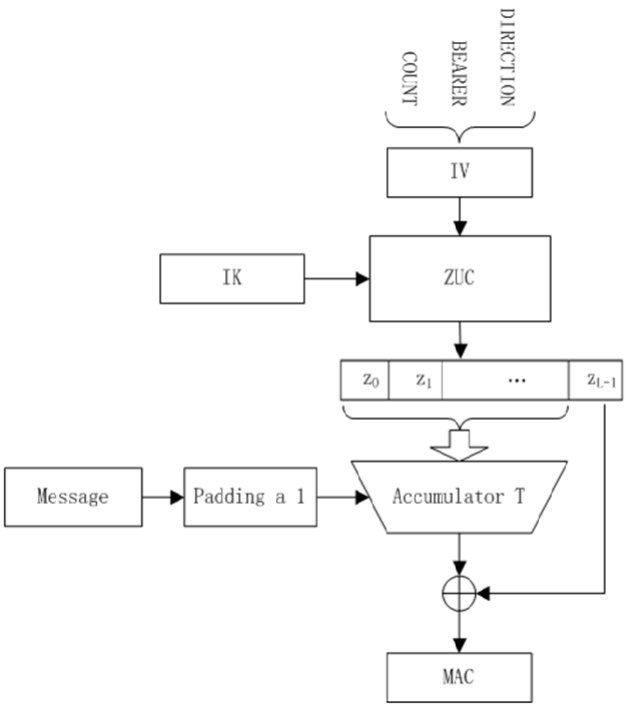


FIGURE 2.12: EIA3 Algorithm

authentications, confidentiality and integrity were presented while indicating their importance and their necessity for protecting user's information as well as its privacy.

Authentication of subscribers followed by key agreements between the UE and the LTE/LTE-A network are considered as the most important security features in the network access. Any failure of the authentication procedure or leak of the secret keys during key agreement would made the whole network security system questionable. Therefore, the 3GPP has standardized EPS-AKA protocol for authentication of the subscribers with the SN as well as the derivation procedure of the symmetric keys requested during encryption and integrity protection of user's and signaling data. Moreover, the key hierarchy employed for the different sessions and entities in the LTE/LTE-A architecture enforces the security but at the expense of additional complexity to the procedure. As regards to D2D authentication in LTE/LTE-A which constitutes one of the main contributions of this thesis, there is no specific standardized protocol adopted by the 3GPP since the D2D concept within 4G systems is very recent and has not been yet handled by the 3GPP. Although D2D authentication has already been well investigated in other wireless and mobile network technologies [28], [29], [30],[31],[32] but these solutions are not very appropriate for LTE/LTE-A technologies because of the considerable differences in their security architecture. More specifically, the main issue with EPS-AKA and its related enhanced versions is that they were originally not been designed

to support D2D communications since the engagement of four network entities (UE, eNB, MME and HSS) are necessary in the authentication and key derivation procedure. While in D2D communications scenario, only two entities (UE and eNB) are involved in the authentication procedure.

Using EPS-AKA or any other of its enhanced versions for D2D authentication results in high communications and computation overhead and leads in extra energy consumptions as well as higher latency. Furthermore, as previously introduced, the methodologies of authentication and key agreement between two communication devices have been well investigated in other wireless and mobile technologies. In VANETs and MANETs most of the methodologies are using digital certificates which is one hand the infrastructures handling certificates is not supported in LTE/LTE-A networks in the second hand because of high computation overheads followed by using such methods. Others are proposing using symmetric polynomials in the authentication and key derivation for MANETs and WMN respectively but with a pre-assumption of a secure channel. As a consequence we conclude there is no suitable protocol is available which could be adapted in a way or another for authentication and key derivation in D2D communications. Hence, the authentication and key derivation for D2D communication is a novel topic which will be addressed throughout this thesis.

The privacy of user's information which is denoted as data confidentiality is another important security future which is has been taken in consideration by 3GPP. The first standardized algorithm denoted as EEA1 is based on the SNOW 3G which has been already used in 3G UMTS, while the second one is based on AES with further security enhancements. A third algorithms is based on ZUC has been proposed and designed in China in order to fulfill Chinese government regulation requirements [33]. Moreover, the standardized algorithms have been subjected to different security analysis and computational complexity in several research works to assess their efficiency in terms of security and computational complexity. Furthermore, since LTE/LTE-A networks intended to support high data rates to the end users, substantial computational power and energy are required during ciphering and deciphering procedure at both UE and the core network sides. The traditional ciphering algorithms employed by the 3GPP standardized solutions depend on the concept of multi-round operations i.e. applying confusion and diffusion on the plane text for several rounds in order to achieve maximum security. A trade-off between strong and sufficient security and computational complexity should be taken into account during the conceptions of ciphering algorithm and trying to minimize energy consumption. A novel ciphering algorithm for LTE/LTE-A to achieve data confidentiality and at the same time reduce the computational complexity would be a

promising tool to decrease energy consumption at both UE and the core network. The proposed solutions in this thesis is based on novel method by applying confusion and diffusion for only one round to perform ciphering/deciphering procedure and achieving the required security, which by consequence leads in reduced complexity and less energy consumption.

The integrity protection denoted mostly as DI is also considered as an important security future for LTE/LTE-A networks especially for control plane data in which the 3GPP made it mandatory. Likewise data confidentiality, three algorithms has been proposed for data integrity where the same stream ciphers have been reused in the core algorithms. However using the same core cipher in both data integrity and data confidentiality has not any cryptographic objectives rather than re-usability purposes [8]. Data integrity algorithms have been also subjected to security analysis in the literature to test their efficiency. At least two different attacks has been reported against EIA1 and EIA3 and even no known attack still not reported for EIA2 but in terms of complexity the algorithms still acquire high complexity. Again, reducing complexity of the algorithms used in integrity protection is another method to decrease energy consumption in LTE/LTE-A networks. ..

Chapter 3

Efficient and Robust Ciphering Algorithms forr LTE/LTE-A Data Confidentiality (DC)

3.1 Introduction

An important service which is essential of any secure communication in mobile networks is Data Confidentiality (DC) which refers to the prevention of an unauthorized disclosure of data transmitted between two communication nodes to a third party attackers or intruders, such as individuals, entities or processes. The disclosure of sensitive data can result in loss or damage, such as identity theft, lawsuits, loss of business, or regulatory fines. To achieve DC in the networks, encryption is the best method to protect sensitive data contained in a message. Unencrypted data, which is known as plain-text, is converted to encrypted data, which is known as cipher text. Data is encrypted with an algorithm and a cryptographic key. Cipher-text is then converted back to plain text at its destination.

Accordingly, two different cryptographic methods are mainly used to perform ciphering/deciphering procedure: Asymmetric Encryption (AE) and Symmetric Encryption (SE). AE refers to the encryption methods which require two keys: a public one used for data encryption and a private one used for decrypting the message. While in the SE the two parties of the communication use the same symmetric key for both encryption and decryption.

In the LTE/LTE-A systems architecture as described in [3], the UE and the eNB are connected through the AS protocols where the DC is performed at the Packet Data Convergence Protocol PDCP sub-layer. The PDCP performs ciphering/deciphering of user and control plane data at both UE and eNB sides through an encryption algorithm. As it has already been explained in Chapter 2, the 3GPP has standardized three SE algorithms for DC to ensure confidentiality of user and signaling data in LTE/LTE-A networks. The first algorithm is a 128-bit key EPS Encryption Algorithm (128-EEA1), which is a stream cipher algorithm, based on SNOW 3G and already employed in Universal Mobile Telecommunication System (UMTS). The second one is 128-EEA2 which is based on the AES block cipher algorithm used in its CounTeR mode (CTR mode) [34]. The last standard 128-EEA3 has been recently designed and it is now published for public evaluation, its core is based on ZUC stream cipher [3].

Nevertheless, the flaws and drawbacks related to security and complexity of the standardized solution have been well addressed in Chapter 2. Therefore, designing a less complex DC algorithm has adequate security strength is desirable, since it would require lower computation power and consequently lower energy consumption at both eNB and UE sides during ciphering/deciphering procedure.

Shannon had demonstrated in [12] that the conventional technique to obtain a powerful encryption of a block of bytes is achieved by using the confusion and diffusion layers for several rounds. A round in a cipher algorithm is typically consists of a number of building blocks that are composed together to create a function that is run multiple times. Consequently, larger number of rounds results in stronger security performance but with higher computation overheads. Thus, one should find a trade-off between computation complexity and strong security.

In this chapter, we propose a novel stream cipher technique based on SDN structure which its main advantage is in one hand its reduced complexity to one round instead of several rounds employed in the standardized algorithms, and on the other hand it possesses strong security strength as the standardized solutions. The proposed one round cipher algorithm consists of an addition, a substitution and a diffusion layer. The addition layer uses binary XOR operation with constant block value to ensure key uniformity. The substitution layer is constructed from the nonlinear transformation of RC6 to add confusion. Finally, the diffusion layer is built from the output of the substitution layer. The output results of the cipher are key-streams used for encryption/decryption of data.

The rest of this chapter is organized as follows: The procedure of cryptographic realization in LTE/LTE-A networks is presented in Section 3.2. In Section 3.3, we introduce and describe our proposed algorithm and the functionality of each layer is described in detail. Simulation tests for the cryptographic strength and performance are introduced in Section 3.4. Finally in Section 3.5 the chapter will be discussed and concluded.

3.2 Cryptographic realizations in LTE/LTE-A

Cryptology is sometimes defined as the art and science of secret which are considered as useful and effective tool for pocketing confidentiality of communications. Modern cryptography is based on mathematical functions. These functions either have significant complexity to be computed or they can only be computed with extra information i.e. (the key). Indeed, most cryptographic protection methods rely on the concept of using keys and these keys themselves have to be managed and protected in an efficient way especially in the SE methodologies widely used in communication networks.
The concept of SE algorithms is based on the principle of using the same keys for encrypting the plane-text as well as decrypting the cipher-text and they are divided into two main classes: block ciphers and stream ciphers. In a block cipher, a fixed-length plain-text block is transformed into cipher-text block of the same length using symmetric keys. Thus, for any fixed key if the plain text is p and the symmetric key used is k , encryption function is E and the decryption function is D the block cipher is a bijection: $c = E(p, k); p = D(c, k) = D(E(p, k), k)$.
While in the stream ciphers, the plain-text bits are combined with a pseudorandom cipher bit stream (key-stream), typically by an exclusive-or (XOR) operation. The idea of a stream cipher is based on a simple secure cipher called the one-time pad and the cipher text is calculated as: $c = k \oplus p$. Similarly at the decryption side the plain text is obtained as: $p = k \oplus c$.

In LTE/LTE-A networks the concept of stream ciphering is employed in the standardized algorithms EEA1 EEA2 and EEA3. However, the AES (Core cipher of EEA2) which is originally considered as a block cipher, is used in the counter (CTR) mode to produce key streams and acting as a stream cipher [35]. The encryption/decryption algorithms are located at PDCP sub-layer in the protocol stack of LTE/LTE-A networks as shown in Figure 3.1 and the keys to be used by PDCP sub-layer are managed by the upper layers. The input parameters to the ciphering algorithm are; a 128-bit cipher key (usually K_{UPenc} for user plane data encryption and K_{RRCenc} for control plane data encryption) and a 128-bit Initial Vector (IV). The IV is a fixed-size input to a cryptographic primitive

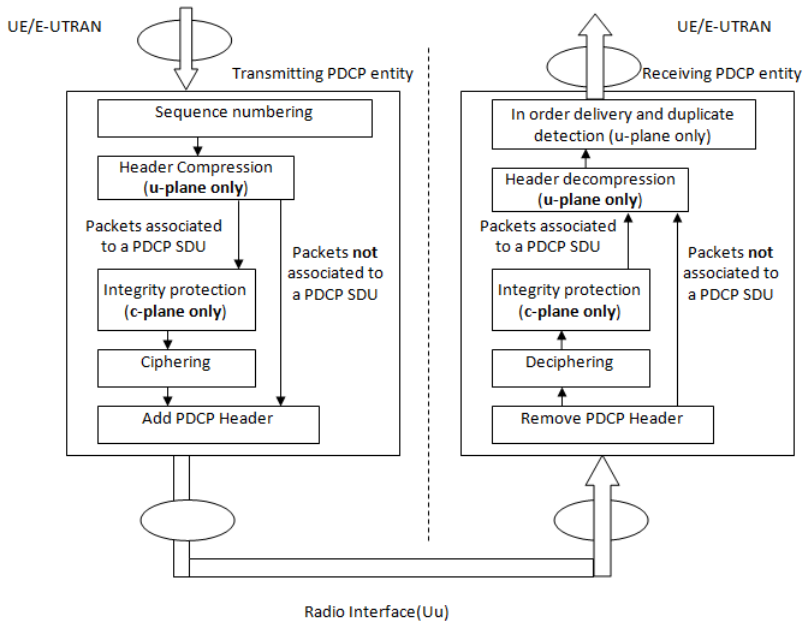


FIGURE 3.1: PDCP Layer.

that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message [36].

For LTE/LTE-A networks, the IV is composed of a 32-bit counter, a 5-bit bearer identity, the 1-bit direction of transmission (shall be 0 for uplink and 1 for downlink) and the length of the required key-stream. In addition, bits are padded in order to fill a 128-bit block [37]. Typically, the cipher algorithm considers a stream of packets in plain-text P exists at the source (UE or eNB) and requires to be transmitted safely. This stream is divided into many packets P^w, $(w = 1, \ldots, h)$ and each packet is divided into many blocks M_j^w $(j = 1, 2, \ldots, q)$ of 128-bit length. The process of encryption/decryption in EEA is depicted in Figure 3.2, for the j^{th} plain-block of the w^{th} packet. More precisely, at the encryption side, the cipher-text $C_j^w = \{c_{j,1}^w, c_{j,2}^w, \ldots, c_{j,n}^w\}$ is obtained by XORing the bytes of the j^{th} plain-data block (plain text) $\{m_{j,1}^w, m_{j,2}^w, \ldots, m_{j,n}^w\}$ with their corresponding output byte key-stream $S_j^w = \{s_{j,1}^w, s_{j,2}^w, \ldots, s_{j,n}^w\}$ obtained from the ciphering algorithm:

$$c_{j,i}^w = m_{j,i}^w \oplus s_{j,i}^w \tag{3.1}$$

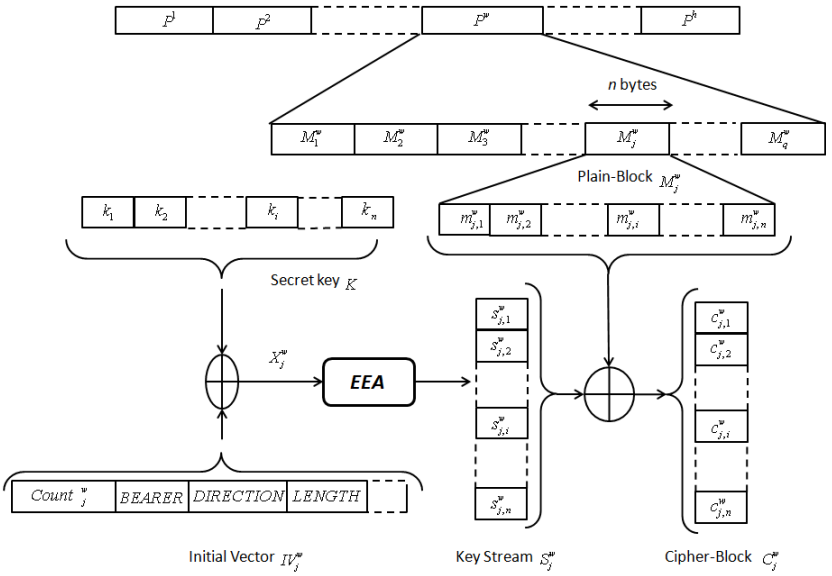


FIGURE 3.2: Ciphering a block of data.

Likewise, at the decryption side, the i^{th} byte of cipher block is XORed with the i^{th} byte of key-stream $s^{w}_{j,\,i}$ to recover the i^{th} byte of the plain block $m^{w}_{j,\,i}$:

$$m^{w}_{j,\,i} = c^{w}_{j,\,i} \oplus s^{w}_{j,\,i} \tag{3.2}$$

3.3 Efficient and Robust Ciphering Algorithm (ERCA)

In Section 3.2, the realization of a cipher algorithm in LTE/LTE-A networks has been presented with a description of the necessary parameters included in the IV construction. In this section a novel and practical cipher algorithm is presented to achieve DC in LTE-/LTE-A networks. Usually, the term efficiency refers to having the fastest execution time while keeping necessary security of the network. This permits to overcome previously-described drawbacks of the standardized solutions. The main properties of our proposed solution are: high level of security and efficiency in computation complexity without any need for memory overhead. The effectiveness of secure stream cipher is a necessary condition for practical implementation. The proposed stream cipher algorithm candidate has similar architecture to AES in the sense that it is a block cipher used in its CTR mode.

The basic scheme of the proposed ciphering algorithm is presented in Figure 3.3. For each input block, the process of addition layer is applied first, then the process of substitution. After that, we reshape the output of substitution process (row) to form a sub-matrix, which is used to construct the diffusion matrix. Finally, the process of diffusion is applied using the obtained diffusion matrix on the output of substitution layer. The proposed cipher algorithm uses secret key $K = \{k_1,\ k_2, \ldots,\ k_{16}\}$ with 128-bit length. Indeed,the ciphering algorithm is performed on a set of bytes of input block $X_j^w = \{x_{j,\,1}^w,\ x_{j,\,2}^w, \ldots,\ x_{j,\,16}^w\}$, which is obtained from the XOR between the bytes of K generally referred as (K_{UPenc} or K_{RRCenc}) in the LTE/LTE-A networks and IV_j^w as follow:

$$x_{j,\,i}^w = k_i \oplus IV_{j,\,i}^w, \quad i = 1, 2, \ldots, 16 \tag{3.3}$$

ERCA takes the X as an input to its first layer i.e (addition layer) following the procedure until we get the ciphered result at the end of the algorithm. In the following, the functionalities of each layer are described in details.

3.3.1 Initial Key Addition Layer

The addition layer uses constant block value, that has been chosen with uniform bit distribution to provide the uniformity to the key-stream by mixing the input block with a constant block, which would be carried out on bytes (byte by byte) using logical XOR operation as follows:

$$y_{j,\,i}^w = x_{j,\,i}^w \oplus t_i \tag{3.4}$$

where $x_{j,\,i}^w$ is a byte of the input block and t_i is a byte of the constant block which all the bits are zeros. The use of logical operation XOR ensures the uniformity, which makes the differential cryptanalysis extremely difficult.

3.3.2 Substitution Layer

The substitution process is the most important operation in any cipher algorithm due to its non linearity which makes the algorithm immune against differential and linear cryptanalysis. The substitution layer could be in forms of S-box as it is the case in AES and ZUC, or could be a nonlinear transformation as we used here. Mathematically, an $m \times m$ substitution layer is a nonlinear mapping $F : (0,1)^m \rightarrow (0,1)^m$, where $(0,1)^m$ represents the vector spaces of elements from binary Galois field. The proposed substitution layer uses the nonlinear transformation of RC6 [38], with an efficient modification, since the original RC6 has poor cryptographic properties, especially high differential probability approximation which makes it useless to be used as a substitution layer. The nonlinear

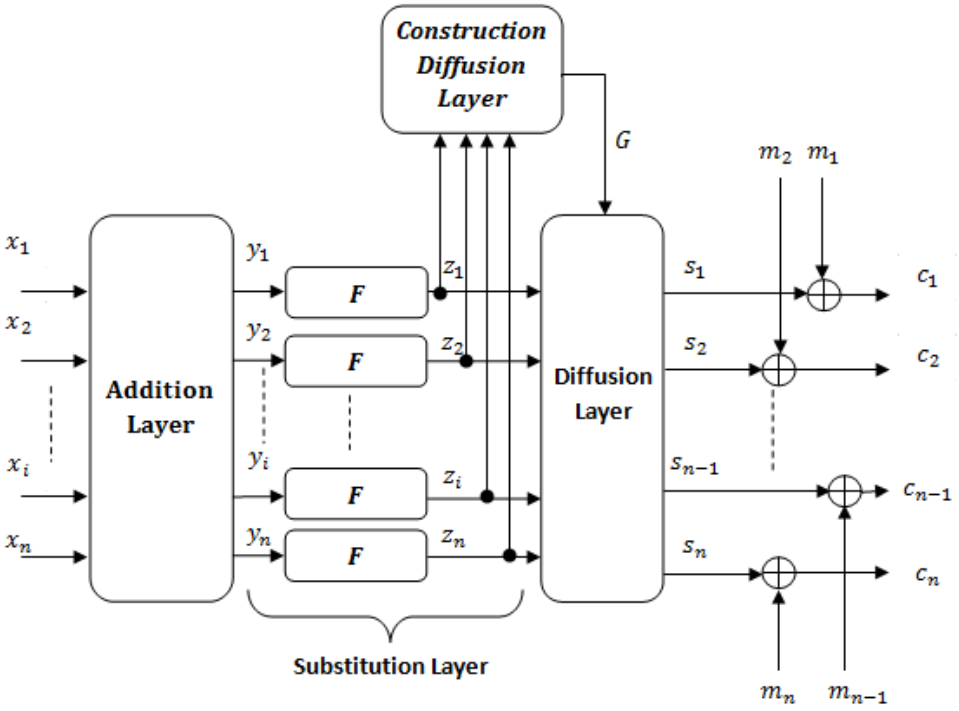


FIGURE 3.3: ERCA stream cipher

transformation of RC6 is performed as below:

$$z = F(y) = mod(y \times (2 \times y + 1), 2^Q) >> log_2(Q) \tag{3.5}$$

where $>>$ is bitwise right shift and Q is equal to 8, since the substitution layer is applied on byte level. This transformation is applied for multi-iteration $irs = 1, 2, \ldots, rs$. Hence, a substantial enhancement of its cryptographic properties is achieved. Starting with initial vector V, where $V_j = j$ and $j = 0, 1, \ldots, 255.$, the output vector after each iteration becomes the input vector for the next one. The obtained results in Figure 3.6 and 3.7 show that the optimal number of iterations to attain a good performance (LP_F, SAC, BIC and DP_F) as described in Section 3.4 is $log_2(Q) = 3$. Therefore, in our implementation each byte is substituted by applying the RC6 nonlinear function for three iterations.

3.3.3 Diffusion Layer

The diffusion process includes two steps: secret matrix generation G; and Modular 256 vector matrix multiplication.

3.3.3.1 Construction of the secret matrix G

The diffusion layers are linear transformation, which is represented as matrices. However, the proposed technique of key dependent diffusion layer is designed to be efficient and robust, which means that the avalanche effect has to be achieved in cooperation with the substitution layer. In addition, this method is based on a special rule of algebra, which can provide the properties of flexibility, effortless to be implemented in hardware, key dependent, and non invertible matrix as its determinant is equal to 0 (singular matrix). In the following, the proposed method to build a dynamic diffusion matrix is described. It is based on a particular matrix structure (non invertible 2D matrix), simple to realize and successful in terms of speed of calculation. The 2D matrix is presented below.

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}; det(A) = ad - bc \tag{3.6}$$

Hence, if $det(A) = 0$ then $a \times d = b \times c$. To obtain the proposed structure of non invertible key dependent diffusion layer, considering that d is equal to b, which leads to $a \times b = b \times c$. This gives us that a is equal to c. Then, the form of a secret matrix in 2D is defined as below:

$$A = \begin{bmatrix} a & b \\ a & b \end{bmatrix} \tag{3.7}$$

Assuming that b is equal to $a \times (2 \times a + 1) \bmod 2^{256}$, the non invertible matrix requires only one parameter a. In this formulation called back below, parameter a is replaced by the sub matrices A to form the diffusion matrix with n dimensions.

$$G = \begin{bmatrix} A & B \\ A & B \end{bmatrix} \tag{3.8}$$

A is a non-zero matrix of size $\frac{n}{2}\ times \frac{n}{2}$. The elements of A can be freely chosen from any Galois field such that G is full rank. In our simulation, the elements of this sub-matrix varies between 0 and 255. Having a matrix G constructed from four sub-matrices (A, B, C, D), the non- invertibility of this matrix can be proven as follows.

Its determinant is given by:

$$\begin{aligned} det(G) &= det(A) \times det(D - CA^{-1}B) \\ &= det(A) \times det(B - ABA^{-1}) \\ &= det(A) \times det(B - B) \\ &= 0 \end{aligned} \tag{3.9}$$

where $D = B$, and $C = A$.

Therefore, the necessary condition to not have an inverse matrix is attained and the attackers cannot calculate the inverse secret matrix G^{-1} to get the original substituted data. An example to construct the secret matrix G is shown in Figure 3.4 for $n = 16$. The output of the substitution layer is reshaped to form a sub-matrix parameter *temp* with size $\frac{n}{4} \times \frac{n}{4}$. Later, this sub-matrix is replicated to form a sub-matrix A with size $\frac{n}{2} \times \frac{n}{2}$., which is required to form the final matrix (diffusion layer).

3.3.3.2 The Proposed diffusion Process G

The input of the diffusion layer is n bytes and diffusion is performed on a series of substituted bytes $\{F(y_1),\ F(y_2),\ \ldots,\ F(y_h)\}$, which the output from is the produced key-stream. The key-stream S is obtained by performing a modular multiplication matrix using the secret matrix G, which is obtained from the substituted data. The architecture of the diffusion process is shown in Figure 3.5. The coefficients vector $\{G_1, G_2, ..., G_n\}$ are described as the global diffusion matrix (G). Each global diffusion vector G_i is represented as a sequence of independent random numbers from a byte field. The relationship among input block data, G and S can be described as follows:

$$\begin{aligned} S &= G \times (F(Y)) \\ &= \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix} = \begin{bmatrix} G_{1,1} G_{1,2} \cdots G_{1,n} \\ G_{2,1} G_{2,2} \cdots G_{2,n} \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ G_{n,1} G_{n,2} \cdots G_{n,n} \end{bmatrix} \cdot \begin{bmatrix} F(y_1) \\ F(y_2) \\ \vdots \\ F(y_n) \end{bmatrix} \end{aligned} \tag{3.10}$$

Where $G_{i,j}$ is a diffusion coefficient that varies between 0 and 255 for the line i and column j and $i, j = 1, 2, ..., n$. $F(y_i)$ is a substituted byte, s_i is the resulting byte key-stream

Finally, the output key-stream S is XORed with the plane text M to produce the ciphertext C to be transmitted.

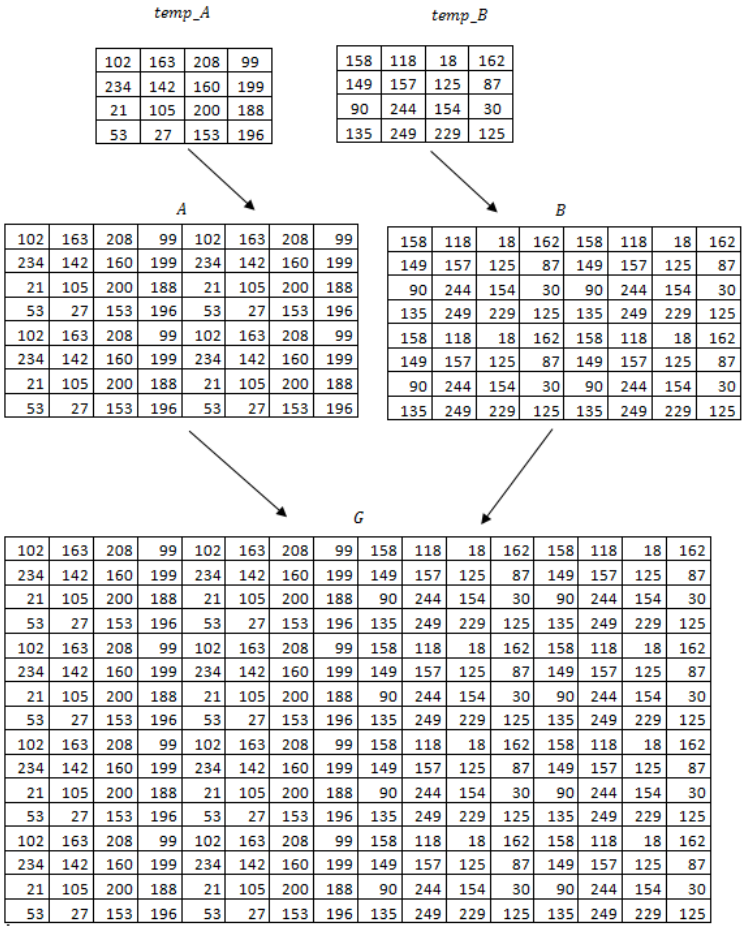


FIGURE 3.4: An example of creation of the diffusion Layer

3.4 Cryptographic strength and performance

In this section, the cryptographic properties of the proposed algorithm are presented. The algorithm is subjected to several tests such as uniformity, randomness and key sensitivity to assess its efficiency and to show how far it is consistent with security standards. In addition, the time complexity is quantified and compared to AES algorithm.

3.4.1 Cryptographic performance of the substitution layer

A strong $n \times n$ substitution layer must have some important properties, based on information theory analysis [39], [40], [41]. The main five properties are: bijectivity, non linearity, Strict Avalanche Criterion (SAC), output Bit Independence Criterion (BIC), and equiprobable input/output XOR distribution.

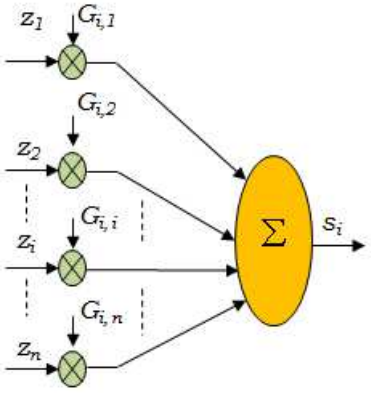


FIGURE 3.5: Proposed Diffusion Technique

3.4.1.1 Linear Probability Approximation Boolean Function (LP_F)

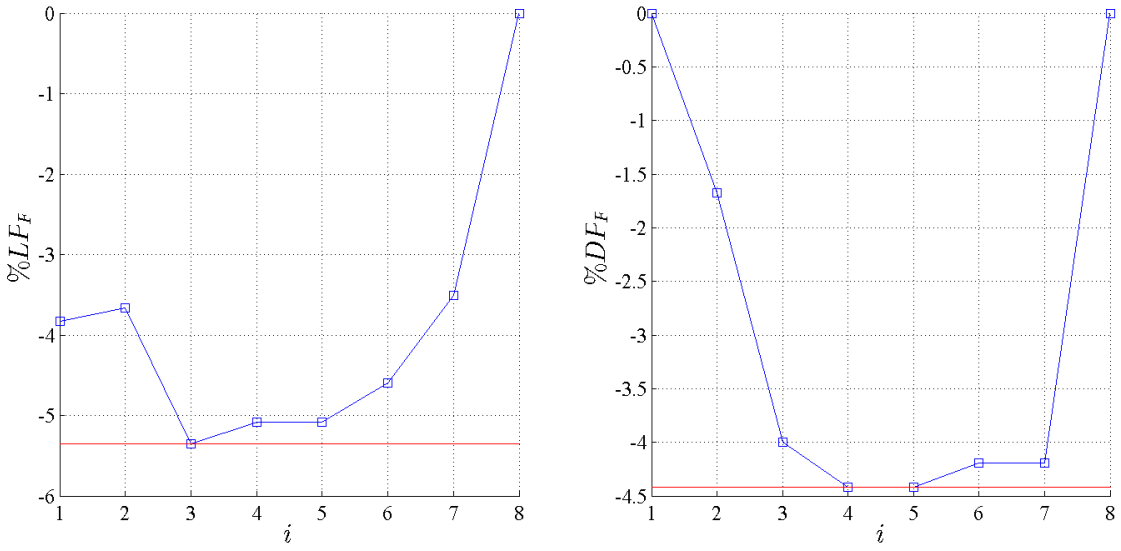
One of the important properties of the substitution layer is non linearity to make it capable resisting linear cryptanalysis attacks. LP_F is used to measure the nonlinear degree of a given substitution layer, it is calculated according to [39]. In Figure 3.6-a, the variation of LP_F against the number of iterations rs is shown. It attains its minimum value after three iterations.

3.4.1.2 Differential Probability Approximation Function (DP_F)

Differential Uniformity is one of the important properties of any substitution layer for obtaining the nonlinear transformation and hence resisting differential cryptanalysis attacks [40]. DP_F is used to measure differential uniformity of our substitution layer as in [42]. Figure 3.6-b, shows the variation of DP_F against the number of iterations rs, which attains its minimum value after 4 iterations.

3.4.1.3 Strict Avalanche Criterion (SAC)

Webster and Tavares were the first to present SAC when they generalized the avalanche effect [41]. A cipher system function is satisfying SAC whenever a single input bit is complemented, the output bit should be changed at least with a probability of half. Certainly, SAC is considered a desirable characteristic of any block ciphering algorithm and used to quantify the degree of security of the s-boxes of substitution-permutation networks. Therefore, any strong ciphering system should fulfill these criteria The average SAC value (mean of 8x8 values of the dependence matrix) versus the number of iteration rs is shown in Figure 3.7-a. We can observe that the SAC value becomes very close to the ideal value 0.5 after three iterations.



(A) (B)

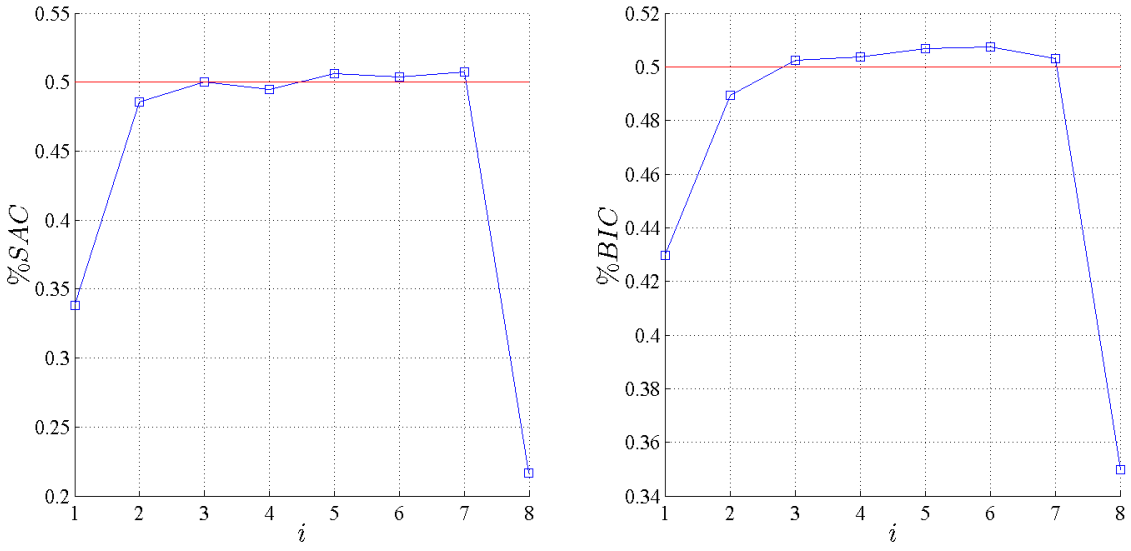
FIGURE 3.6: Variation of the LPF (a) and DPF (b) against the number of iterations

3.4.1.4 Output Bit Independence Criterion (BIC)

BIC is another property which has also been described by Webster and Tavares [41] and considered as another desirable characteristic of cipher algorithms. The BIC specifies that: two output bits j, k should change independently when a single input bit i is changed for all i, j and k. The average value of BIC (mean of 8x8 values of the BIC matrix without the diagonal) versus the number of iteration rs is shown in Figure 3.7-b. We can observe that the BIC becomes very close to the ideal value 0.5 after three iterations. This result is similar compared with SAC, so the number of iterations is set to be equal to 3 to attain an acceptable performance with low complexity possible.

3.4.2 Randomness of the produced key-stream

The security strength of the proposed stream cipher is depending on the produced key-stream; therefore the stream cipher should produce key-streams with high level of randomness. Some parameters of the LTE packet header are used in addition to the counter to form IV, which implies that the sub-matrix used in the construction of the diffusion layer is renewed for each block; consequently the produced key-stream is updated. In Figure 3.8, the recurrence (a) and distribution (b) for a random key-stream are shown. These results indicate clearly a good degree of randomness and uniformity. To prove these properties, the cipher key-stream has been analyzed using the randomness test



(A) (B)

FIGURE 3.7: Variation of the SAC (a) and BIC (b) against the number of iterations

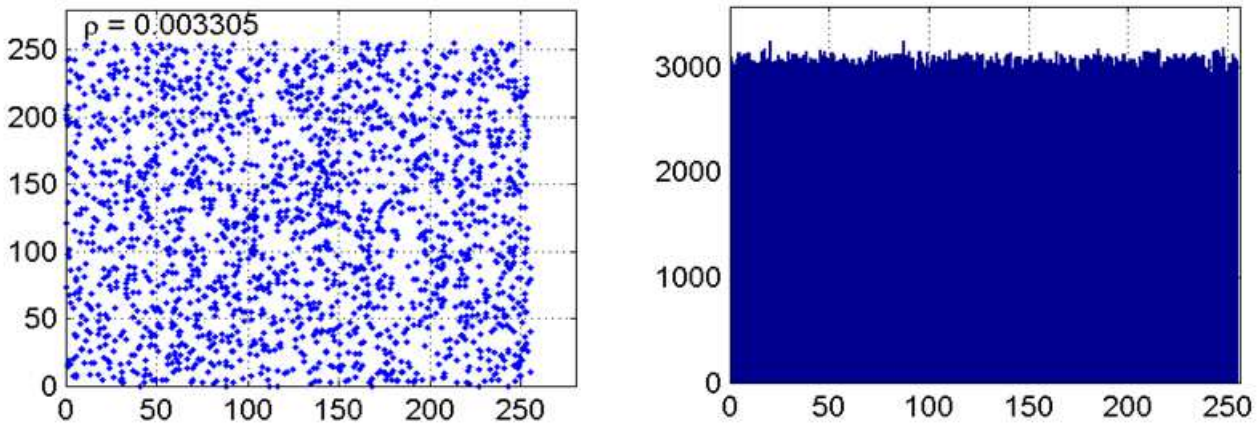
of NIST [43]. In order to get correct statistical results one needs to provide 100 secret keys and each key-stream sequence should be at least 1000000 bit long. The NIST test performs 15 tests on the data sample, and the total amount of executing NIST STS tests is 189. Results of testing the key-stream randomness are shown in Figure 3.9. The obtained proportion values (success rate) show how many samples passed given tests. The red line marks minimum proportion values in order to consider the sequence to be random. Random Excursions and Random Excursions Variant tests represent 26 tests with different parameters, which have other minimum proportion values. The simulation results indicate clearly the randomness of the generated key-streams.

3.4.3 Key sensitivity

The sensitivity of the secret key is analyzed for 1000 random keys. All the elements of K_i' are equal to those of ith key K_i, except the Least Significant Bit (LSB) which was flipped. The percent of Hamming distance is calculated as follows:

$$PDH = \frac{\sum_{k=1}^{T} C_i \oplus C_i'}{T} \times 100\% \tag{3.11}$$

where T is the length in bit level of the encrypted packet, and C_i and C_i' are the corresponding cipher packets using K_i and K_i' respectively.



(A) (B)

FIGURE 3.8: Recurrence of producing key-stream (a) and its distribution (b) using a secret random key K

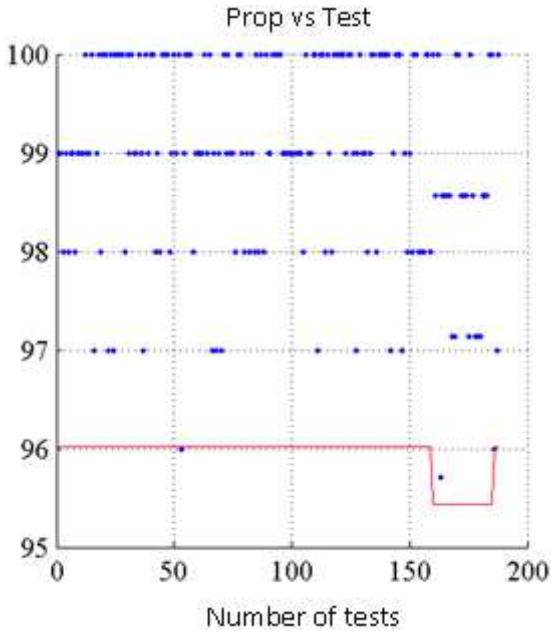


FIGURE 3.9: Proportion values of NIST tests

In Figure 3.10, the sensitivity of the secret key versus 1000 random keys is shown, while only the LSB of K^i is changed. This result indicates a high sensitivity, while the average Hamming distance percent is closer to the optimal values (50%) in bit level.

3.4.4 Statistical properties

To demonstrate the safe use of our stream cipher, it is important to analyze its characteristics, in terms of random recurrence, mixing nature, and low coefficient correlation

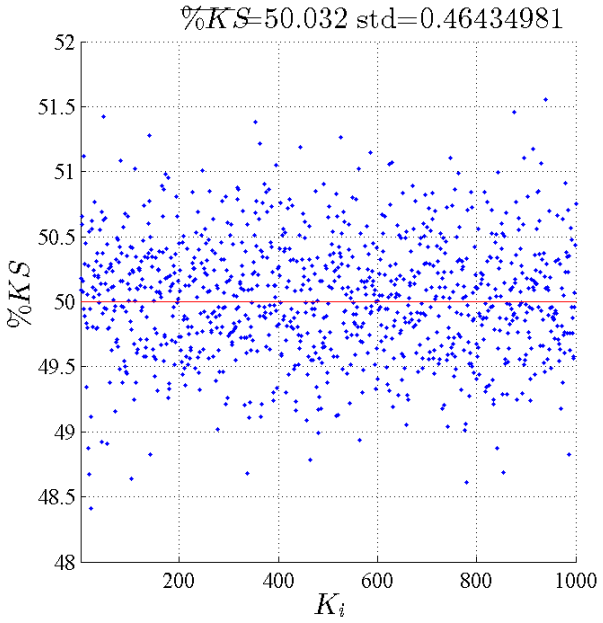


FIGURE 3.10: The key sensibility results for change random LSB of the secret key K versus 1000 random keys

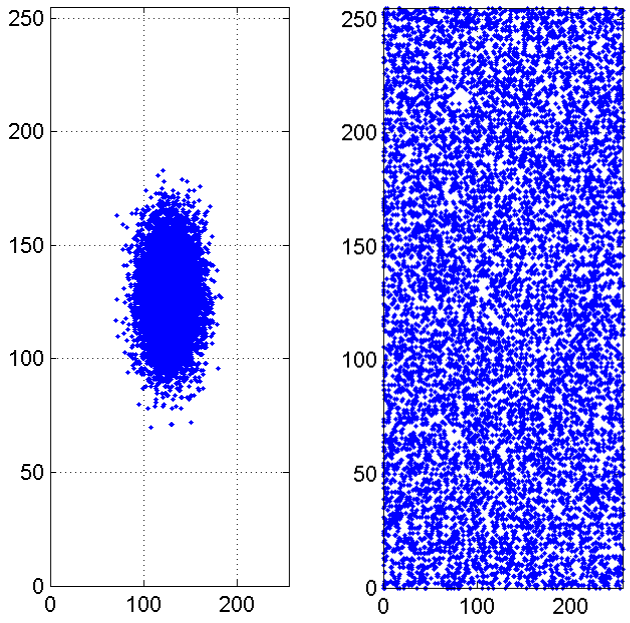
between original and encrypted data packets. In our simulation, the proposed stream cipher scheme is considered as a black box and randomly choosing a set of initial packets with a 125000 byte length, which are normally distributed with a mean equal to 128 and a standard deviation equal to 8.

3.4.4.1 Recurrence

The recurrence plot serves to measure the evaluation of randomness and estimates the correlations among the data of a sequence as in [44]. Considering a packet sequence $x_i = x_{i,1}, x_{i,2}, \ldots, x_{i,m}$, a vector with delay $t \geq 1$ can be constructed by:
$x_i(t) = x_i,\ x_{i+t},\ x_{i,\,2\times t}, ...,\ x_{i,\,m\times t}$. In Figure 3.11 a and b, the variation between $x_i(t)$ and $x_i(t+1)$ from the original and the encrypted packets are shown respectively. We can observe that that no clear pattern is obtained after encryption.

3.4.4.2 Mixing nature

The mixing nature serves as a measure of the uniformity and it can be quantified by a statistical approach. If the frequency counts of the encrypted generation are close to a uniform distribution, then it is possible to categorize that the concerned cipher under test has a good level of mixing. In Figure 3.12-a and b, the distribution of the original packets and their corresponding cipher packets respectively are shown. This result shows clearly that the contents of the encrypted packets are spread overall the space and have



(A) (B)

FIGURE 3.11: Recurrence plot of the original packet (a) and its correspondent encrypted ones (b)

a uniform distribution. To validate this uniformity, the Chi-square test [45] is applied and works as follow:

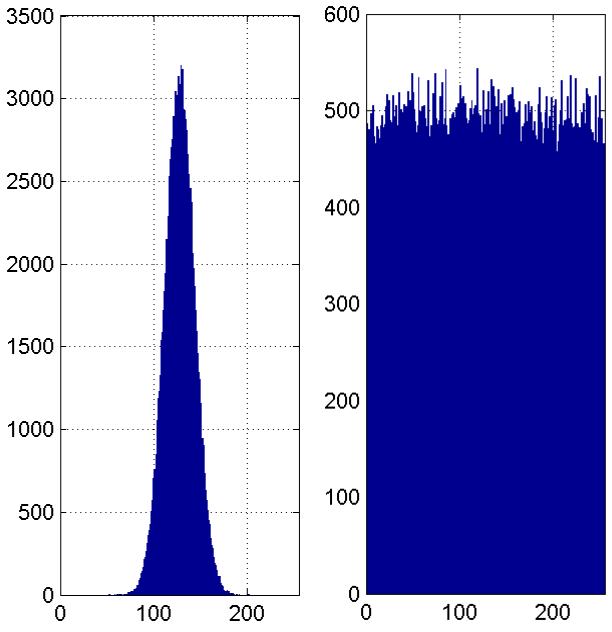
$$\chi^2_{test} = \sum_{i=1}^{l} \frac{o_i - e_i}{e_i} \tag{3.12}$$

where l is the number of levels (here 256), o_i is the observed occurrence frequencies of each level of field size (0-255) in the histogram of ciphered generation contents, and e_i is the expected occurrence frequency of uniform distribution. For a significant level of 0.05, the null hypothesis is not rejected and the distribution of the histogram is uniform if $\chi^2_{test} \leq \chi^2_{theory}(255, 0.05) \approx 293$. The average results of the Chi-square test for 1000 different sets of generation for the whole ciphered packets against h is shown in Figure 3.13. The distribution of the tested histogram is uniform for $\approx 97\%$, that means a strong mixing property is obtained.

3.4.4.3 Low coefficient correlation

Another important requirement for any encryption scheme which must be attained is that the encrypted data should be greatly different from its original form. The encrypted packets should have redundancy and correlation as low as possible. First, the correlation

coefficient between the original and encrypted packets is measured. The correlation coefficient is computed according to the following formulas:



(A) (B)

FIGURE 3.12: The distribution of the contents original stream packet (a) and its correspondent encrypted one in (b)

$$\rho_{x,y} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \tag{3.13}$$
$$where\ cov(x,y) = E[\{x - E(x)\}\{y - E(y)\}];$$
$$E(x) = \frac{1}{n} \times \sum_{k=1}^{n} x_i$$
$$and\ D(x) = \frac{1}{n} \times \sum_{k=1}^{n} \{x_i - E[x]\}$$

In Figure 3.14, the coefficient correlation between the original and encrypted packets versus 1000 different keys and data packets is shown. This result shows the correlation coefficient is always close to zero which indicates that no detectable correlation exists between the original and its corresponding cipher packets.

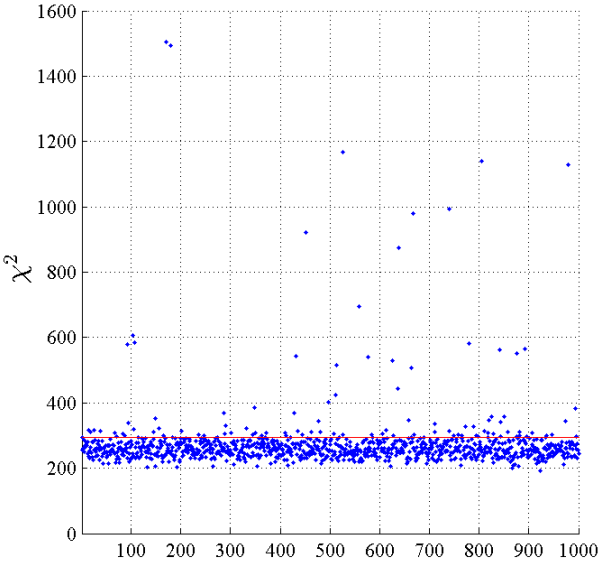


FIGURE 3.13: Variation of the χ^2_{test} of cipher packets for 12508 bytes length versus 1000 random keys

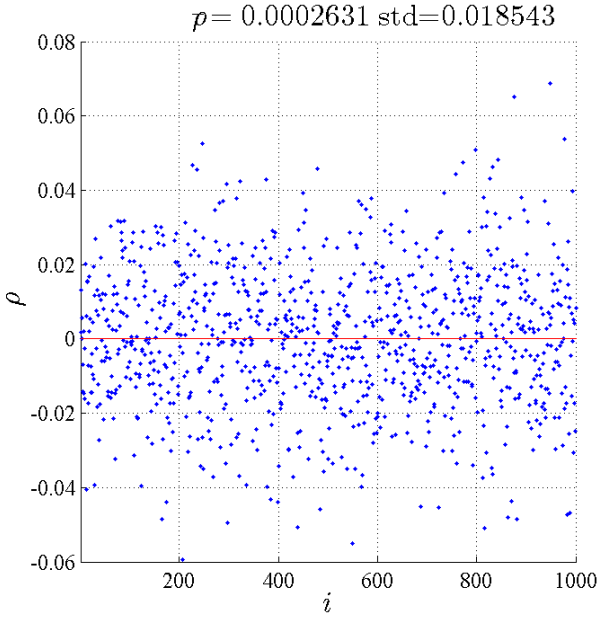


FIGURE 3.14: The coefficient correlation between the original and encrypted stream packets versus 1000 random keys

3.4.5 Execution Time

The execution speed is very important for any DC algorithm since it is directly related to the time and resources required for ciphering/deciphering. The execution time should be maintained very low, especially when a huge amount of data is to be transmitted such as in LTE systems. The average calculation times in ms (on 10000 times) to encrypt a

packet M against Tb is quantified, where Tb represents the length of the block such as 128, 256, 512, 1024, etc. These calculations are performed under the following software and hardware environment: Matlab 2012 and micro-computer Intel Core 2 Duet 2.1 GHZ CPU with 2 GB RAM Intel, under Windows7. we conclude that the variation of average time is linear. The average time necessary against Tb is estimated (approximately) using the linear interpolation method. It shows that the proposed method is indeed sufficiently fast for LTE/LTE-A applications. Finally, we compared the mean encryption time (in ms), versus Tb, of the proposed cipher with AES. The proposed secure scheme is at least 4.5 times faster than the AES algorithm as shown in the Figure 3.15.

3.4.6 Discussion and Cryptanalysis

A cryptographic scheme is considered secure if it is strong enough to resist attacks. According to Shannon's theory, the confusion and diffusion processes must be applied to provide resistance against the powerful attacks that is based on statistical analysis [12].These processes are repeated for several rounds to achieve the avalanche effect which leads to delay in terms of execution times (high computation complexity that lead to high delay and consumption of energy) especially for resource constrained devices. Our proposed stream cipher ERCA is constructed in a new manner, where the diffusion process changes in a dynamic manner (pseudo-random) and doesn't possess the invertible property.

Concerning the substitution layer, when the number of iterations is 8, all properties

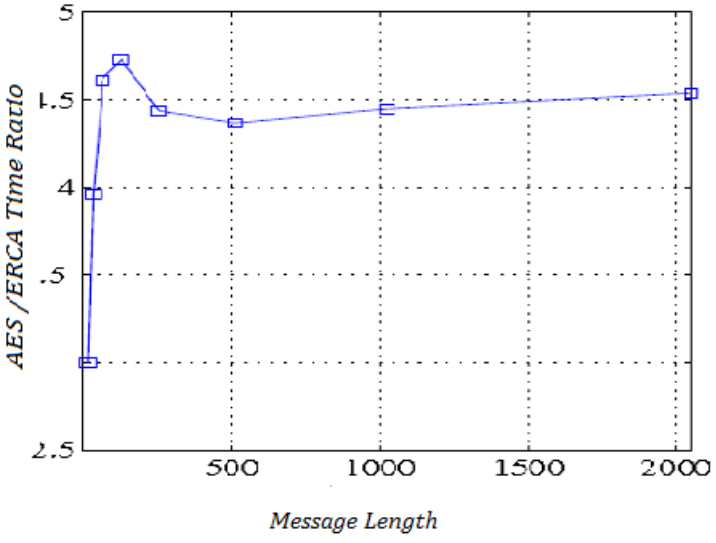


FIGURE 3.15: Variations of the average time ratio for messages encryption (AES/ERCA) in function to its length

become weak, this means that, increasing the number of iterations leads to eliminate totally the advantage of bitwise right shift, since this function without $>>$ is linear and cannot be used as substitution layer. The proposed function is periodic and its periods are 8 iterations and the best performance is attained in three iterations. To demonstrate the performances of the proposed substitution layer, its properties are compared with the substitution layer of AES and ZUC (S_0 and S_1) in Table 3.1. The results showed that the proposed substitution layer possesses sufficient cryptographic performances and the obtained results of LP_F, DP_F, SAC and BIC are very close to the standardized solutions. The cryptographic security of our scheme relies on two properties:

- using a new efficient substitution layer
- using a dynamic diffusion layer with unpredictability and high sensitivity of the G

TABLE 3.1: Comparison Analysis of Substitution Layer

Test	Proposed	AES	S_0	S_1
LP_F	$2^{-5.3}$	2^{-6}	2^{-5}	2^{-6}
DP_F	2^{-4}	2^{-6}	2^{-4}	2^{-6}
SAC	0.5	0.4998	0.494	0.509
BIC	0.502	0.4998	0.4951	0.505

Moreover, the statistical properties of the proposed secure scheme (such as the uniformity of the cipher packets and the low coefficient correlation between the original and encrypted block of packets) are attained, which can provide immunity against the statistical attacks. In addition, differential and linear attacks would become ineffective, since the avalanche effect is attained and the diffusion layer changes for each block. In fact, any change in any bit of secret key or public parameters causes a significant difference in the encrypted blocks as see in Figure 3.10. The key space of the secret key is 2^{128}, which is sufficiently large to make the brute-force attack infeasible. Additionally, the use of non invertible dynamic diffusion layer will limit the ability of the attackers who try to break out the cipher.

3.5 Conclusion

In this Chapter, our novel algorithm ERCA has been presented to be used in data confidentiality protection in LTE/LTE-A networks. The main motivation of the novel algorithm was to achieve the security requirements with minimum complexity. The key idea of ERCA was based particularly on usin substitution diffusion networks similar

as AES algorithm. While AES is based on Shannon's vision of ciphering algorithm by performing diffusion and confusions functions for at least 10 rounds as in EEA2, our proposed algorithms performs the encryption in only one round. Indeed, ERCA is a round function consists of an addition, a substitution and a diffusion layer. We have introduced a new technique of key dependent stream cipher which achieves the avalanche effect with an acceptable trade-off between security and complexity. Additionally, ERCA algorithm has been subjected to several statistical and analytical tests that are essential for any cipher algorithm to be considered credible and robust. Simulation results showed that ERCA possesses most of the necessary cryptographic properties. Moreover, considerable reduced computational time has been achieved if compared to AES algorithm. In consequence, reduced computational power and energy consumption during ciphering/deciphering processes are attained.

.

Chapter 4

Efficient and Robust Algorithm for LTE/LTE-A Data Integrity (DI)

4.1 Introduction

One of the important security services in any wireless channel is Data Integrity (DI) since if compared with wired transmission, active eavesdropping in a wireless environment is relatively easy. Integrity protection of data is mainly responsible for the prevention of modification of messages during transmission over the air interface. It is also responsible for the protection against impersonation attacks [8]. In public key cryptography or asymmetric cryptography, the integrity is mostly protected using digital signatures, while MACs are preferred in symmetric cryptography. The MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. However, because of the high computation requirement of digital signature calculation, the integrity protection in the resource constrained devices such as mobile terminals is mostly based on MAC. In mobile networks such as LTE/LTE-A, the integrity protection is performed using MAC that convert strings of variable lengths to fixed-size strings called hash values, hash codes or simply hash. Cryptographic hash functions can be keyed or un-keyed. The un-keyed ones are called Modification Detection Codes (MDCs) that provide only data integrity. The Keyed Hash Functions (KHFs) are MACs which besides the integrity protection help in the authentication of originality of data [46].
Moreover, as LTE networks intend to support high data rates and an enhanced data, voice, and video experience for end users, it is desirable to develop a low computation

DI algorithm with acceptable security strength, to speed up data processing and consequently reduce the computational time.
In this chapter we propose a new efficient and robust DI algorithm we baptise Efficient and Robust Algorithm for Data Integrity (ERADI). ERADI is based on a KHF and the concept of Merkle and Damgard [47], [48]. Its main advantage is the use of a dynamic substitution-diffusion technique in the core cipher of the algorithm which requires only one round of processing instead of several processing rounds as required by the standardized reference solutions. Likewise the ERCA cipher algorithm already presented in Chapter 3, the core cipher of the proposed hash function consists of addition, substitution and diffusion layers. In addition, a chaining layer is also employed in order to ensure more bit dependency. Notably, the core cipher employed here is not exactly as same as the one that used in the ERCA algorithms as it is the case in the all standardized solutions. By employing ERADI in LTE/LTE-A networks, significant computational complexity reduction and consequently important energy savings are expected.
The rest of this chapter is organized as follows. In Section 2, the realization of integrity protection in LTE/LTE-A networks is presented. In Section 3, the novel proposed ERADI algorithm is detailed. Simulation and test results are discussed in Section 4. Finally, this Chapter's developments and results will be discussed and concluded in Section 5.

4.2 Realization of integrity protection in LTE/LTE-A networks

While the digital signatures are mostly used for the integrity protection in public key cryptography, MACs are widely preferred in the integrity protection of the mobile networks where the symmetric cryptography is employed in such scenarios. There exist several of widely used MACs, such as HMAC [49], EMAC [50], XCBC [51], OMAC [52], [53] and XOR MAC [54]. The conventional MAC algorithms consist of two components: the underlying cipher and the upper-level structure. An underlying cipher could be a keyed hash function, block cipher or stream cipher. Moreover, the input message for a MAC generation algorithm is allowed to have an arbitrary length, it passes through the underlying cipher and becomes the cipher text. Then, the cipher text is assembled by the upper-level structure to get a fixed-length string, which is the output of the MAC.
Although most of the traditional MACs are based either on hash functions or block ciphers, recently the use of a stream cipher as an underlying cipher for MAC attracts more and more attentions in current research works. The three standardized DI algorithms for LTE/LTE-A networks EIA1, EIA2 and EIA3 apply an under layer cipher as a tool to encrypt the public and secret keys, and make use of the encrypted result in the upper

layer to compute the Message Authentication Code for Integrity (MAC-I) of the message. EIA1 and EIA3 algorithms adopt the concept of Galois Message Authentication Code (GMAC) [25] which its basic idea is to employ a block cipher in its counter mode to act as a stream cipher. While EIA2 algorithm is based on the concept of CMAC i.e. using the output from the cipher algorithm directly as a MAC.

In LTE/LTE-A systems specifications, the integrity protection is mostly mandatory for control plane data but the user plane data is not integrity protected except for Relay networks [13]. When a communication session is started, the UE and the eNB are connected through the Access Stratum (AS) protocol [55], and the DI feature is achieved in the PDCP sub-layer. It is important to note that the DI algorithm and the key to be used by the PDCP entity are configured by upper layers. Generally, an EIA algorithm, as shown in Figure 4.1, takes as input a 128-bit Integrity Key (IK), which is the K_{RRCint} in (LTE/LTE-A key derivation hierarchy) subsequently a 32-bit COUNT, a 5-bit bearer identity, a 1-bit direction representing the transmission direction (shall be 0 for uplink and 1 for downlink), and finally the message itself which is the control plane data (denoted also as RRC signaling traffic). The derived output is a 32-bit MAC-I. The sender appends the MAC-I to the message when sent. In the same way, for DI checking, the receiver computes the expected message authentication code (XMAC-I) using the received message and compares it to the MAC-I.
However, the standardized solutions have their own drawbacks especially in terms of computational complexity as already explained in Chapter 2. The next sections describe our contributions to solve the previously mentioned drawbacks, and more particularly the computational complexity. we propose a novel efficient DI algorithm which computational complexity will be reduced significantly.

4.3 ERADI Algorithm Description

In this section,we detail our ERADI algorithm based on CMAC we called ERADI is proposed for LTE/LTE-A networks, which has to ensure the data integrity protections for the control plane data at PDCP sub-layer. The process of MAC generation which uses the concept of Merkle and Damgard [47], [48] is depicted in Figure 4.2. It consists of a round compression function (a hash function based on a block cipher), which is applied in an iterative process.
In fact, the input message M (control plane data of LTE PDUs) with a random length N is padded if necessary to ensure that the length of M is multiple of Tb (here $Tb = 128$). M is subsequently divided into nb blocks ($M_1,\ M_2,\ \ldots,\ M_{nb}$), where $nb \geq 1$, and each

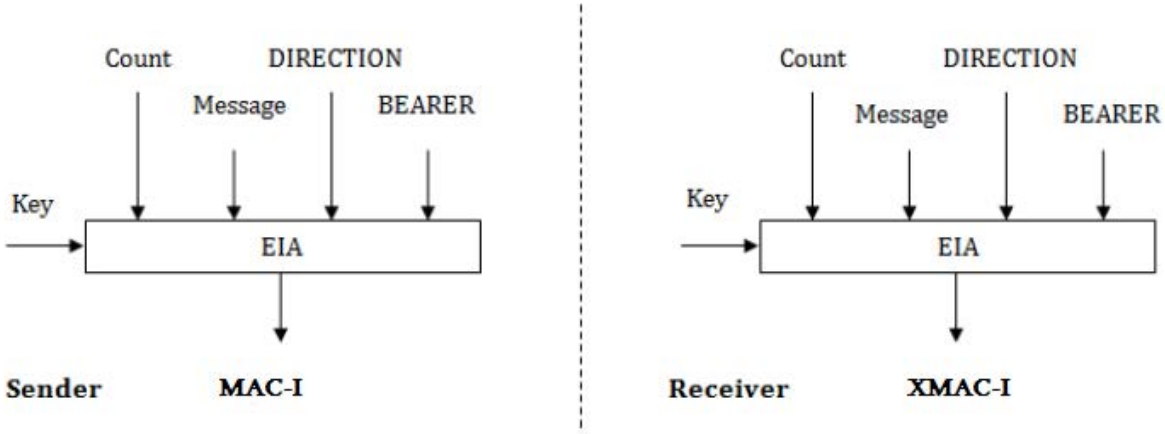


FIGURE 4.1: Derivation of MAC-I/XMAC-I

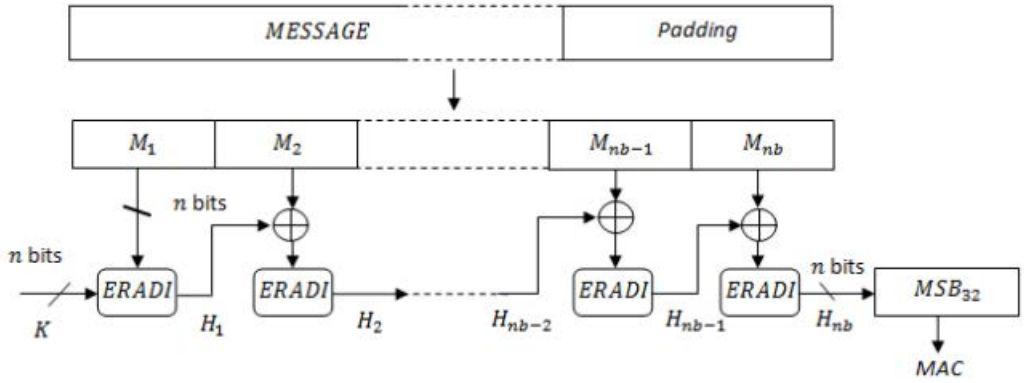


FIGURE 4.2: The iterated design of the proposed keyed hash function for ERADI

block consists of $n = Tb/8$ bytes. Likewise, IV is formed from a 32-bit COUNT, a 5-bit bearer identity and the 1-bit direction of the transmission; it is also is padded with zeros to form a 128-bit block. The hash value is calculated according to the following equation:

$$H_i = ERADI(H_{i-1}, M_i) \qquad i = 1,\ 2, \ldots, nb \tag{4.1}$$

where H_0=IK$\oplus$IV. The last output H_{nb} is truncated by getting the 32 MSB (Most Significant Bits), which is exploited directly as MAC-I. Indeed, every M_i, IK and IV are divided to $n = 16$ bytes before being taken as inputs to the cipher.
The proposed core cipher of ERADI function compromises four layers: addition, chaining, substitution and diffusion layers, which is depicted in Figure 4.3.

It is important to note that the overall structure of this cipher is almost similar to the structure of ERCA algorithms. The main difference is that in the ERADI algorithm a chaining layer is added to the original structure. Therefore, the different layers will

be explained briefly since their functionalities details have been largely introduced in Chapter 3.

4.3.1 Addition Layer

Let us consider a given block M_i, $i \in [1, nb]$. The addition layer uses a constant block value, that has been chosen with uniform bit distribution to provide the uniformity to the message by mixing this constant block with the input block, which should be carried out on bytes (byte by byte) using logical XOR operation as follows:

$$y_{i,j} = h_{i-1,\,j} \oplus m_{i,j} \oplus t_j \tag{4.2}$$

where $h_{i-1,\,j}$ is the j^{th} byte of the input to the addition layer, which is the previous output of the compression function (with $h_{0,j} = IK_j \oplus IV_j$), t_j is the j^{th} byte of the constant block and $m_{i,j}$ is the j^{th} byte of the considered message block M_i.

4.3.2 Chaining Layer

The chaining layer can be considered as a CBC mode, where each byte of the input block is XORed with the previous output chaining byte, and would be carried out on bytes (byte by byte) as follows, starting with $u_{i,1} = y_{i,1}$:

$$u_{i,j} = y_{i,j} \oplus u_{i,j-1} \qquad j = 2, 3, \ldots, n \tag{4.3}$$

This means that, each output byte of the block depends on all input byte blocks processed up to that point. The chaining layer has been chosen to ensure a high sensibility for the parameters of the substitution layer and consequently for the diffusion layer. In addition, this guarantees that the avalanche effect, key and initial vector sensibilities are attained.

4.3.3 Substitution Layer

The proposed substitution layer presents a potential modification of the Non Linear Transformation (NLT) of RC6 [38], which is originally expressed as:

$$y = RC6(x) = mod(x \times (2 \times x + 1), 2^W) >> log_2(W) \tag{4.4}$$

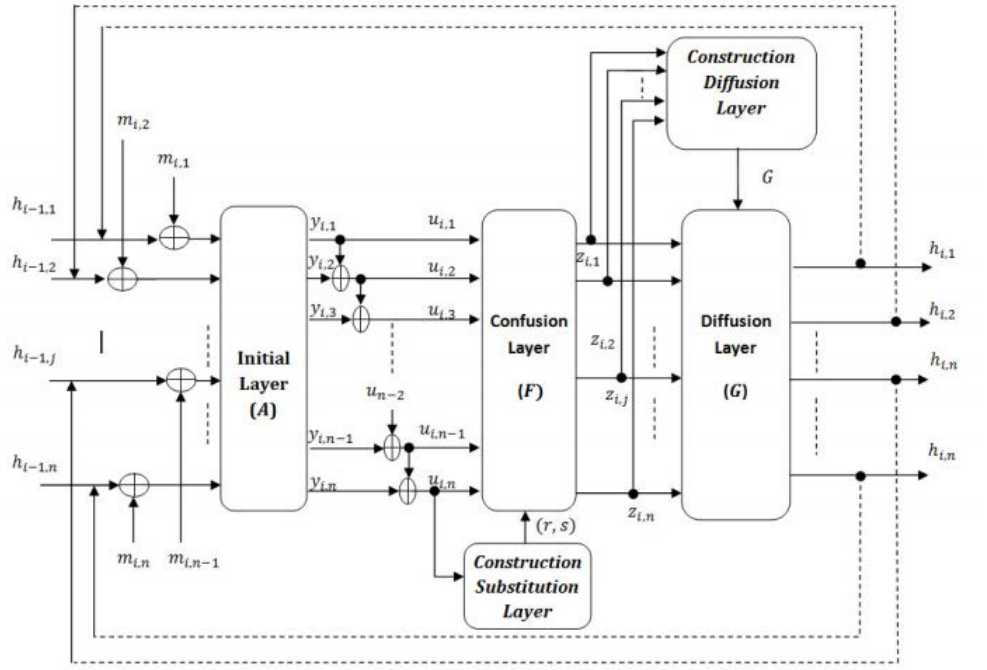


FIGURE 4.3: Proposed compression function (ERADI)

where $>>$ is bitwise right shift and W is equal to 8. A modified version of RC6 is employed to ensure a dynamic nonlinear transformation. Indeed the proposed dynamic substitution layer is reformulated as:

$$\begin{aligned} Z_w &= F(Z_{w-1}) \\ &= mod(Z_{w-1} \times (r_w \times Z_{w-1} + t_w), 2^w) >> log_2(w) \end{aligned} \tag{4.5}$$

where $Z_0 = U$, $w = 1, \ldots, 4$ and (r_w, t_w) are the control parameters for iteration w. In fact, r_w and t_w have to be an even and odd bytes respectively.

These different control parameters are generated as:

$$\begin{aligned} &r_0 = u_n \text{ and } s_0 = \overline{u_n} \\ &r_w = RC6(r_{w-1}), \\ &s_w = RC6(s_{w-1}), \quad w = 1, 2, 3, 4 \end{aligned} \tag{4.6}$$

where u_n is used since it is the last output byte of the chaining layer and represents the XORed value of all elements of the vector $Y = \{y_1, y_2, \ldots, y_n\}$. After that, the Least Significant Bit (LSB) for each element r_w and s_w is set to 0 and 1 respectively, to ensure the bijectivity property (one-to-one). Accordingly, each byte is substituted by applying the RC6 non linear function using four different couples of control parameters

$(r_w,\ t_w)$, $w = 1, 2, 3, 4$. In the Table 3.1, we present the corresponding cryptographic properties of the original RC6 and our proposition. These results indicate clearly that the original transformation has poor cryptographic properties, especially a high differential probability approximation which makes it useless for being used as a substitution layer. Accordingly, a potential enhancement of the cryptographic properties is achieved using our modification compared to the original one.

4.3.4 Diffusion Layer

The diffusion process is a linear transformation which is represented as matrices. This layer includes two steps: secret matrix generation G and Modular 256 vector matrix multiplication. Indeed, the proposed dynamic diffusion layer is based on a special rule of algebra, which can provide the properties of flexibility, through the use of non invertible matrix as its determinant is equal to 0 (singular matrix). Equally important to note, it is effortless to implement this diffusion technique in hardware since it can be executed in parallel as shown in Figure 3.5.

4.3.4.1 Secret matrix generation G

The output of the substitution layer is reshaped to form a sub-matrix parameter *temp* with size $\frac{n}{4} \times \frac{n}{4}$. Later, this sub-matrix is replicated to form a sub-matrix A with size $\frac{n}{2} \times \frac{n}{2}$. The form of the diffusion matrix with n dimension is given as below:

$$G = \begin{bmatrix} A & B \\ \\ A & B \end{bmatrix} \tag{4.7}$$

Assuming that B is equal to $A \times (2 \times A + 1) \bmod 2^{256}$. Besides, having a matrix G constructed from four sub-matrices ($A,\ B,\ C,\ D$), it can be proven that this matrix is non-invertible. Indeed, the determinant is given by:

$$\begin{aligned} det(G) &= det(A) \times det(D - CA^{-1}B) \\ &= det(A) \times det(B - ABA^{-1}) \\ &= det(A) \times det(B - B) \\ &= 0 \end{aligned} \tag{4.8}$$

where $D = B$, and $C = A$.

Therefore, the necessary condition for not having an inverse matrix is attained and the attackers cannot calculate the inverse secret matrix G^{-1} to get the original substituted block data, which in turn ensures the one way property.

4.3.4.2 Modular matrix multiplication of G

Considering any block message M_i, $i \in [1, nb]$, the diffusion process is performed on a series of n substituted bytes $\{z_{i,1},\ z_{i,2},\ \ldots,\ z_{i,n}\}$ and its output is the produced hashed block H_i, which is obtained by performing a modular multiplication matrix using the secret matrix G, derived from the substituted data. The architecture of the diffusion process is shown in Figure 3.5.

The coefficients vector $\{G_1, G_2, ..., G_n\}$ are described as the global diffusion matrix (G). Each global diffusion vector G_i is represented as a sequence of independent random numbers from a byte field. The relationship between input block data, G and S can be described as follows:

$$\begin{aligned} H_i &= G' \times Z_i \\ &= \begin{bmatrix} h_{i,1} \\ h_{i,2} \\ \vdots \\ h_{i,n} \end{bmatrix} = \begin{bmatrix} g_{1,1}\, g_{1,2} \cdots g_{1,n} \\ g_{2,1}\, g_{2,2} \cdots g_{2,n} \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ g_{n,1} g_{n,2} \cdots g_{n,n} \end{bmatrix} \cdot \begin{bmatrix} z_{i,1} \\ z_{i,2} \\ \vdots \\ z_{i,n} \end{bmatrix} \end{aligned} \tag{4.9}$$

Where $G_{il,ic}$ is a diffusion coefficient that varies between 0 and 255 for the line il and column ic, with il and ic from 1 to n.

Finally, after the calculation of MAC-I from the sender, which is obtained directly by truncating 32-bits of MSB of H, the result is appended to the original message and sent to the receiver. Similarly, on the receiver side the IK and IV with ERADI function are used to calculate XMAC-I in order check the integrity of the message.

4.4 Cryptographic Strength and Performance Evaluation

In this section, different cryptographic properties of the proposed substitution layer of the core cipher of the algorithm is presented since the chaining layer is added and the cipher should be again tested to ensure its security strength. Moreover, most important

substitution layer testes are applied in order to prove its performance. Then, the overall algorithm is analyzed using several statistical tests such as uniformity, randomness, key sensitivity, etc. to assess its efficiency and to show how far it is consistent with the main security requirements. Finally, the time complexity is quantified and compared to EIA2 algorithm.

4.4.1 Cryptographic performance of the proposed dynamic substitution layer

As been already described in the previous chapter, a strong $n \times n$ substitution layer must have some important properties, based on information theory analysis [39], [40], [41]. These main properties are: bijectivity, non linearity SAC, BIC, and equiprobable input/output XOR distribution. The LP_F can be calculated according to [39]. In Figure 4.4-a, the variation of LP_F against the seed (byte) u_n is shown and the probability of $LP_F < 2^{-4}$ is 0.968, those of $2^{-6} \leq LP_F \leq 2^{-5}$ is 0.322 and those of $LP_F > 2^{-4}$ is only 0.0313. Moreover, LP_F maximum, minimum and average values are: $2^{-2}, 2^{-5.3561}$, and $2^{-4.749}$ respectively. The majority of LP_F results produced from the substitution layer have acceptable values. This indicates that the proposed dynamic substitution layer possesses an acceptable non-linearity property which can ensure the resistance against linear attacks.

Another test is performed forDP_F and the results represented in Figure 4.4-b, show the variation of DP_F against the seed (byte) u_1. The probability of $DP_F < 2^{-4}$ is 0.8477 and that of $DP_F > 2^{-2}$ is only 0.0156. Moreover, maximum, minimum, and average values of DP_F are: $2^{-1}, 2^{-4.6781} and 2^{-4.1758}$ respectively. These results show that the substitution layer can resist the differential attacks.

Similarly, concerning the SAC, the average value (mean of 8x8 values of the dependence matrix) against the seed u_1 is shown in Figure 4.5-a. We can observe that the SAC is always very close to the ideal value 0.5. Finally, the average value of BIC (mean of 8x8 values of the BIC matrix without the diagonal) versus the number of iterations r is shown in Figure 4.5-b. We can observe that the majority of the BIC average values is around the optimal value of 0.5. The simulation results indicate clearly that the proposed substitution layer satisfies the two criteria of SAC and BIC and hence can resist the known and chosen plain/cipher-text attacks. In conclusion, the substitution layer has suitable properties for being used in the proposed core cipher of the ERADI algorithm.

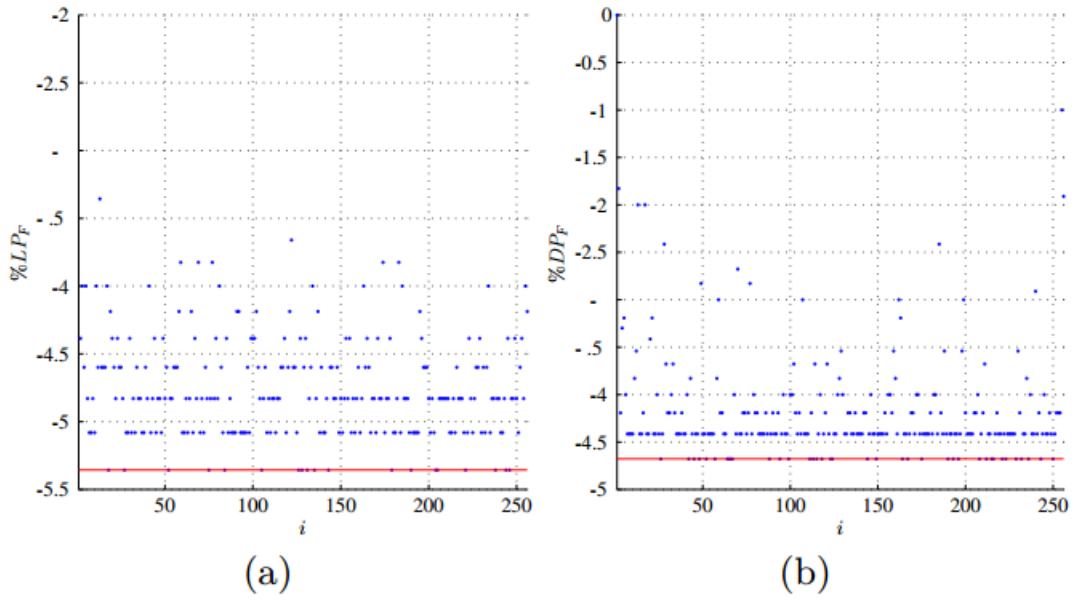


FIGURE 4.4: Variation of the LPF (a) and DPF (b) versus the number of random keys

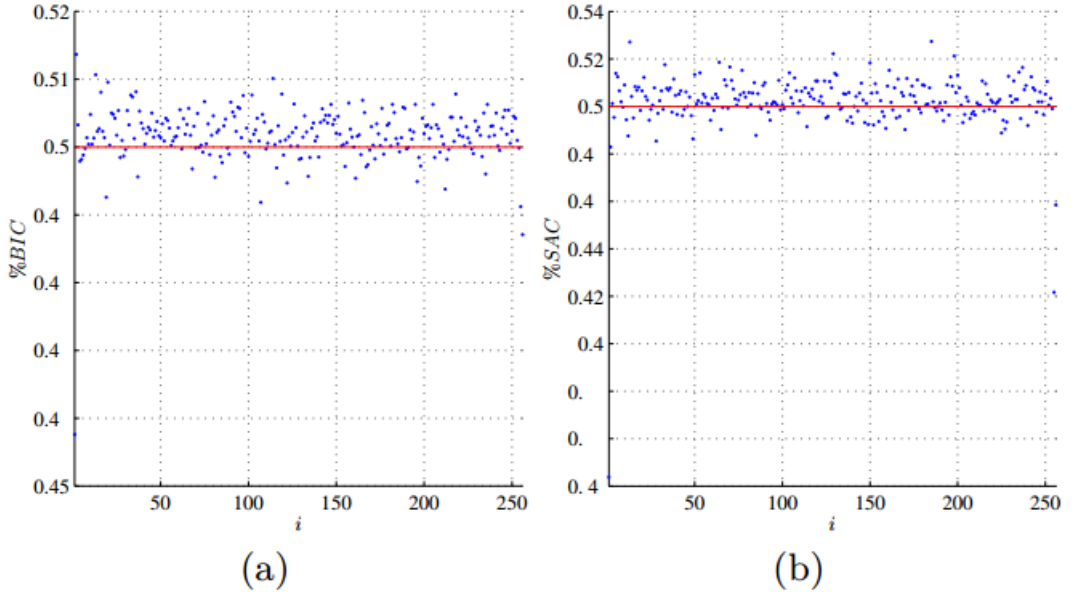


FIGURE 4.5: Variation of the SAC (a) and BIC (b) versus the number of random keys

4.4.2 Security analysis and performance of the proposed hash function

In this section, several tests are performed to analyze and prove the feasibility and the strength of our proposed algorithm. Several simulation tests have been carried out and the results of collision, key space and sensibility tests have been analyzed. Furthermore,

a comparison is carried out between ERADI algorithm and the recent EIA2 standard in terms of the speed of execution.,

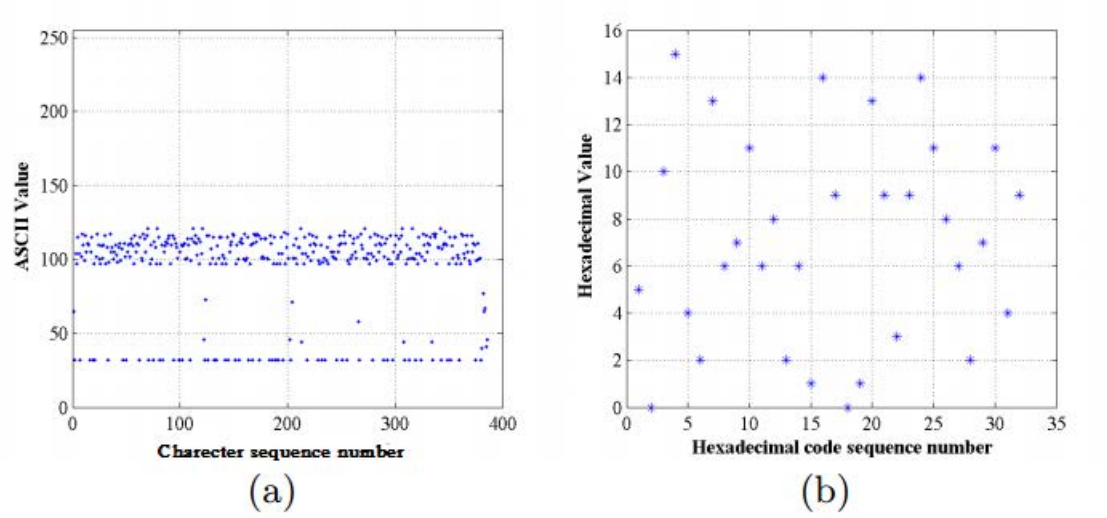


FIGURE 4.6: Spread of the message and hash value: (a) distribution of the message in ASCII code; (b) distribution of the hash value in hexadecimal format

4.4.2.1 Hash value distribution

The security of any hash function is much related to the uniform distribution of the hash value. To verify the uniformity of the hash value to the original text, a simulation of input message in ASCII code is performed using first 10 lines of the introduction section of this chapter.

The original paragraph distribution as depicted in Figure 4.6 is distributed in the range of ASCII codes, and its corresponding hash value distribution is spread out randomly. Similarly, another test has been performed on an input message consisting of a string of zeros. The results as illustrated in Figure 4.7 show that even in this special case the output hash value still shows a random distribution. Furthermore, in order to check the uniformity of hash value, another test is applied by simply computing the length of unique elements of the obtained hash values. Table 4.1 presents the corresponding percent of unique elements for 10000 hash values, where each value is obtained from a random secret key and the message. The percentage distribution of unique elements verifies its uniformity, since approximately 92.312% of hash values have at least 15 different elements, which indicates that a strong uniformity is achieved.

TABLE 4.1: Frequency of the different number of ASCII characters for $N = 10000$

Number of different ASCII characters	16	15	14	13
Frequency	6238	3043	649	70

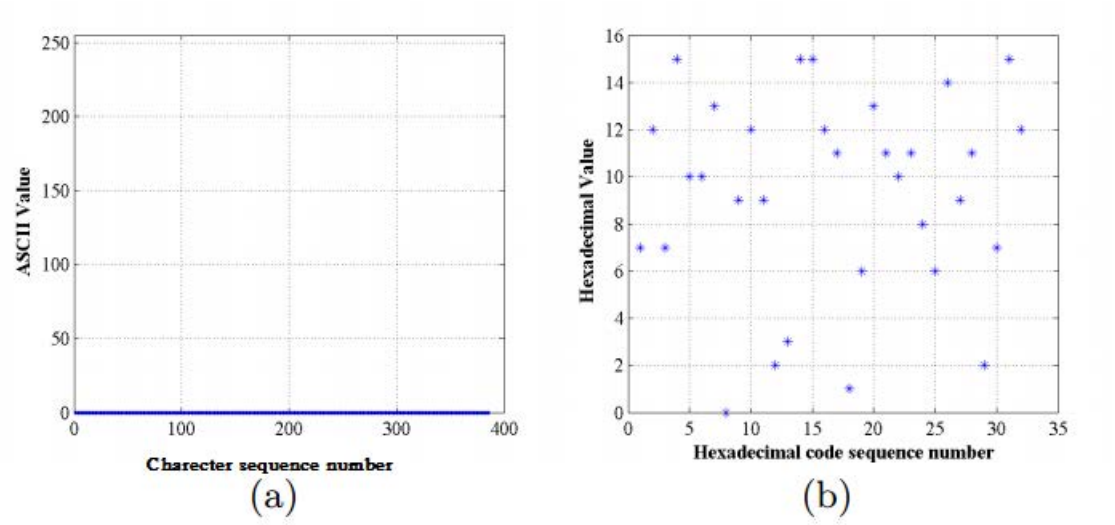


FIGURE 4.7: Spread of all zeros message and hash value: (a) distribution of all Zeros message; (b) distribution of the Hash value in hexadecimal format

4.4.2.2 Hash value sensitivity to the original message

Another criterion of the hash function security is its sensitivity to the original input message. For verifying the sensitivity of hash values, hash simulations have been performed under the following conditions:

C1-The original paragraph (first 10 lines of the introduction of this chapter);

C2-Replacing the first character O from the original paragraph by S;

C3-Modifying the word DI in the original paragraph to DE;

C4-Replacing the full stop from the original paragraph to comma;

C5-Adding a blank space to the original paragraph.

TABLE 4.2: Distribution of changed bit percent under different conditions

Case	C1	C2	C3	C4	C5
C1	0	48.4375	49.0625	50.7813	52.3438
C2	48.4375	0	48.7500	53.9063	57.0313
C3	49.0625	48.7500	0	55.4688	53.9063
C4	50.7813	53.9063	55.4688	0	51.5625
C5	52.3438	57.0313	53.9063	51.5625	0

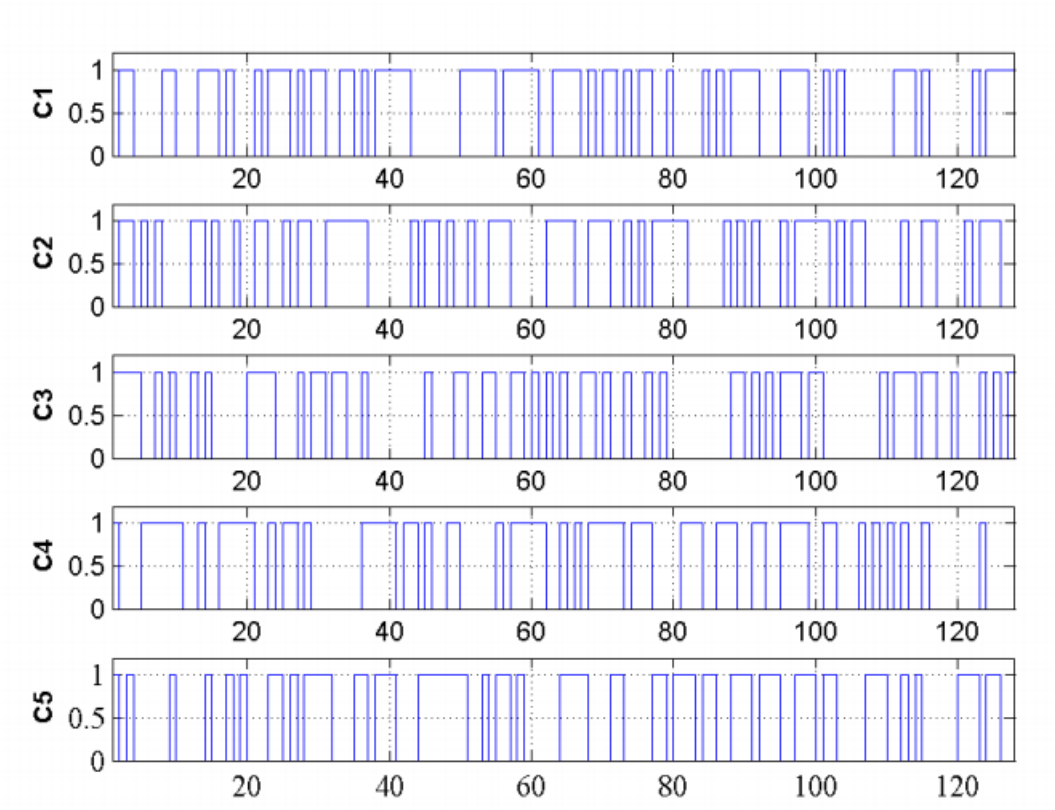


FIGURE 4.8: Hash values under different conditions

The simulation results of binary sequences are depicted in Figure 4.8 and the corresponding percent of changed bits are presented in Table 4.2. These results indicate clearly that a very small change in the original message produces an enormous change in the output hash value.

4.4.2.3 Diffusion and Confusion: Key and message sensitivity

The sensitivity refers to a huge change in the hash value with respect to a slight change in the keys IK or IV and the original message itself. A DI algorithm is considered as robust against related key attacks if it ensures the sensitivity of the secret keys IK and initial vector IV. In particular, when the payload of a control data packet is treated, a tiny change of keys or IV should give two completely different hash values and consequently MAC values. The sensitivity of IK and IV are analyzed for 1000 random keys and IVs respectively using the percent of Hamming distance for IK_w where $w = 1,\ 2,\ \ldots,\ 1000$. that can be calculated as follows:

$$KS_w = \frac{\sum_{k=1}^{T} H_{IK_w\,,\,IV}(M) \oplus H_{IK'_w\,,\,IV}(M)}{T} \times 100\% \tag{4.10}$$

where T is the length in bit level of the hash value, and H_IKw, H_IKw' are the corresponding hash values using IK_w and IK'_w respectively. All the elements of IK'_w are equal to those of the wth key IK_w, except a random LSB which was flipped. Indeed, the same processing is realized for measuring the sensitivity of IV which gives a similar result, since IK and IV are mixed together to form H_0. Likewise, the sensibility of the original message is performed and calculated as follows:

$$PS_w = \frac{\sum_{k=1}^{T} H_{K_w\,,\,IV}(M) \oplus H_{K_w\,,\,IV}(M')}{T} \times 100\% \tag{4.11}$$

where all the elements of message M' are equal to those of message M, except a random LSB which was flipped.

Furthermore, in Figures 4.9 and 4.10, the sensitivity of the secret key and original message versus 1000 random keys and messages are shown respectively, while only a LSB is changed of the secret key IK_w or M. We can observe that the majority of samples is closer to the optimal values in bit level (50%). Additionally, 87.88% and 87.61 % of samples have KS and $PS \geq 45\%$ respectively. We can also see that KS and PS follow a normal distribution. Their minimum, maximum, average and standard deviation are presented in Table 4.3. Similarly, the same results are obtained for changing a single bit in IV. Consequently we can conclude that the chosen/known plain-text attacks would become ineffective.

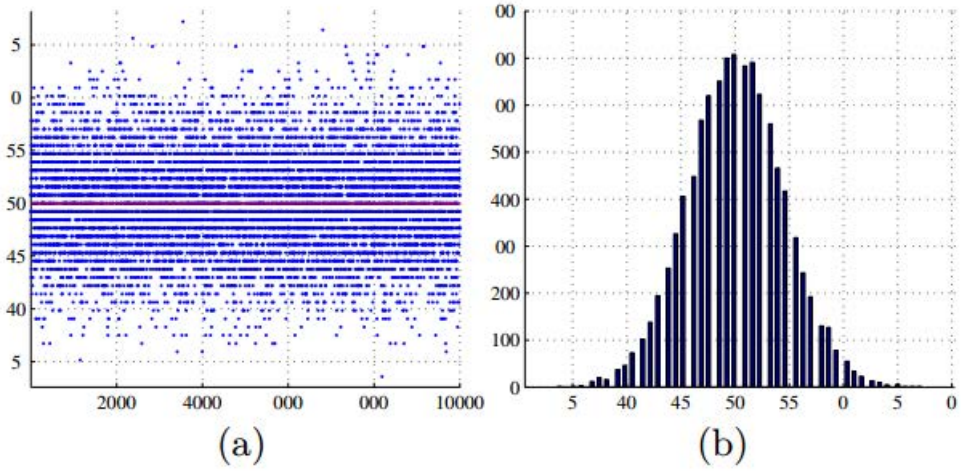


FIGURE 4.9: Percent of number of the changed bits versus 1000 random secret keys (changed random bit of the secret key) (a) and its corresponding distribution (b)

Finally, the properties of diffusion and confusion of the function are attained, since the sensibility of secret key and initial vector are achieved, which indicates that the necessary security requirement is attained within one round.

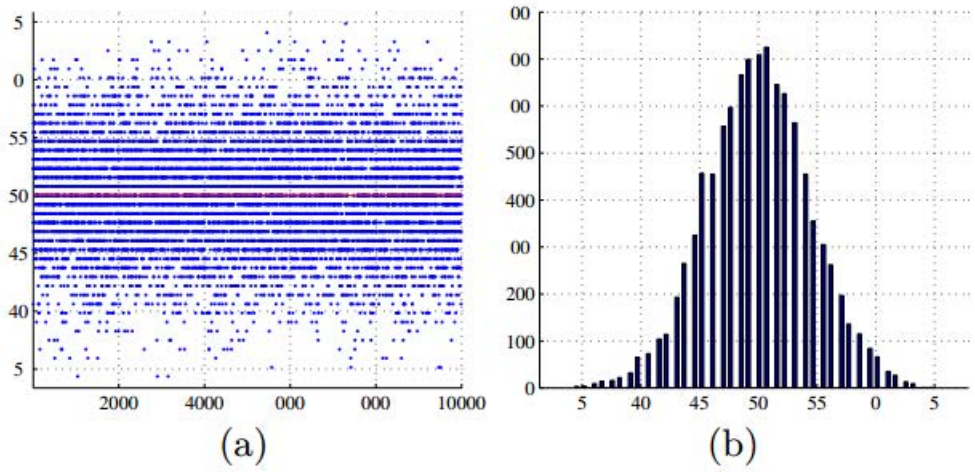


FIGURE 4.10: Percent of number of the changed bits versus 10000 original tests (changed random bit of the message) (a) and its corresponding distribution (b)

TABLE 4.3: Statistical Results

	$\%KS$	$\%PS$
min	33.593	34.3750
max	67.187	64.8438
Avg	50.04	49.9663
STD	4.42	4.4505

4.4.2.4 Collision resistance

Collision resistance refers to the difficulty to find two diverse inputs to the hash function whose outcomes are the same. Generally, the resistance against the collision is verified using the following test, which is conducted for a hash value randomly generated from a paragraph of the input message and stored in ASCII format. Randomly a bit will be selected from the chosen paragraph and flipped; the output hash value of the modified message will be also stored in ASCII format. A comparison between the two hash values is achieved by counting the number of identical positions of ASCII characters i.e (having the same value in the same location) and is calculated as follows:

$$Diff = \sum_{i=1}^{n} D\{H(i), H'(i)\}, \tag{4.12}$$

where $D(x, y) = 1$ if $x = y$ and $D(x, y) = 0$ otherwise.
Simulation results presented in Table 4.4 indicate that the maximum number of equal

characters (hits) attained is three for our proposition. Consequently, a stronger collision resistance is ensured, which makes our proposition immune against birthday, man-in-the-middle and differential attacks [56].

TABLE 4.4: Percent distribution of the number of ASCII characters with the same value at the same location in the hash value for random LSB bit of secret key K (a) or the plain-message P (b)

Number of Hits	0	1	2	3
% (a) (random LSB bit of K)	94.1	5.75	0.15	0
% (b) (random LSB bit of P)	93.69	6.12	0.18	0.01

4.4.3 ERADI Execution Time

Besides the security features, the execution speed is an important criterion to quantify the computational complexity of our proposed algorithm and compare it to the standardized solution. The comparison is achieved with the EIA2 (AES) algorithm since it is considered as the most secure compared to the two other algorithms EIA1and EIA3. The average calculation time ratio (ERADI/EIA2) to the hashed message M with different lengths is depicted in Figure 4.11.
These results were obtained using the following software and hardware environment: Matlab 2012 and micro-computer Intel Core 2 Duet 2.1 GHZ CPU with 2 GB RAM Intel, under Windows7. Clearly, the variation of time ratio is linear and the average requested computational time ratio between EIA2 and ERADI is close to 4.5, which indicates that AES requires 4.5 more times than our proposal during encryption/decryption procedure. Consequently, lower computational complexity leads to faster data processing and less energy consumption by the devices (both the UE and the eNB).

Conclusions and discussion

As the available standardized approaches such as EIA1, EIA2 and EIA3 have their own drawbacks regarding security and/or performance, we have proposed in this Chapter ERADI, a novel data integrity algorithm for 4G LTE/LTE-A mobile networks. The cipher core of ERADI is based on a new technique using chaining with dependent substitution and diffusion layers to attain the avalanche effect, secret key and initial vector sensibility. The chaining layer is added to add more bit dependency and attain the requirements of a secure MAC. Moreover, the statistical properties such as the uniformity of the produced hash value, key sensibility are attained, which can provide immunity

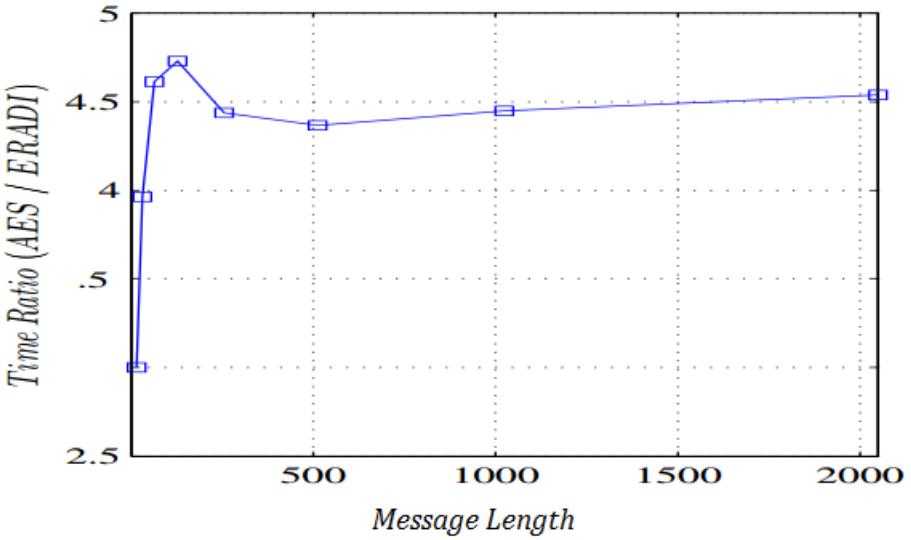


FIGURE 4.11: Variations of the average time ratio versus message length

against the statistical attacks. Furthermore, known attacks such as linear attacks, differential attacks and chosen plain/cipher-text attacks would become ineffective, since the avalanche effect is attained. In fact, any change in any bit of the message, secret key or public parameters i.e(initial vector) results in a significant difference in the produced hash value as been illustrated in the analyses section. The key space of the secret key is 2^{128}, which is sufficiently large to make the brute-force attack infeasible. Besides, the use of non invertible dynamic confusion and diffusion layer will limit the ability of the attackers to try breaking out the underlying cipher algorithm.

In addition, the advantage of the proposed ERADI scheme is its reduced complexity compared to other standardized algorithms recently in use, since it operates one round of iteration to achieve the necessary cryptographic properties, instead of several rounds of iterations deployed by the reference algorithms. This ERADI lower complexity results in reduced latency and higher data processing speed which is a desirable feature for mobile terminals supporting LTE/LTE-A networks with restricted and limited resources. Moreover, to confirm better performance of our proposal, a comparison with the core cipher of EIA2 is performed. Consequently, all simulations results demonstrated clearly the proposed ERADI scheme has the necessary sufficient security features to be considered as a secure MAC and could be considered as a new and interesting candidate for LTE/LTE-A network's integrity protection.

Chapter 5

Device to Device Lightweight Authentication and Key Agreement Protocol

5.1 Introduction

Recently, D2D communications have attracted large research attentions to develop efficient solutions for direct communications between two proximate devices without passing through a base station or another third-party device. D2D paradigm is proposed to be employed in cellular networks between two UEs in order to enhance the performance. Indeed, the majority of D2D related research works concentrate mainly on licensed band (in band) modes using cellular resources where the service providers prefer to maintain a stable and permanent control over the communication rather than using other uncontrolled environments (out band) such as (ad hoc Wi-Fi and Bluetooth) networks using unlicensed bands [6]. At the standardization level, the concept of D2D has been adopted by 3GPP in LTE Release12 to enable LTE becoming a competitive broadband communication technology for public safety networks [57].
D2D is considered an efficient communication method since the proximity UEs may allow for extremely high bit rates, low delays and low energy consumption. In addition a portion of traffic of which was originally had to be passed through the eNB would be offloaded which leads in again low delays and low energy consumption. Furthermore, better security is expected since the communicated data is not routed through Internet cloud and hence not stored in anywhere but on the specified devices.

Nevertheless, one of the major concerns in any wireless and mobile communication system is the security of the data during transmission over unsecured channels as it is the case in the D2D communications. Authentication and key agreement are among the most difficult and important aspects of security in any data transmission between two transmitting nodes. Unlike the traditional mobile communications, where the key derivation, authentication and ciphering/deciphering between two devices are passed through the core network, D2D in LTE/LTE-A supposes direct communication between two UEs without any involvement of the core network.
The current 3GPP authentication and key agreement protocol (AKA) deployed for 3G mobile networks and its successor for 4G mobile systems, called Evolved Packet System authentication and key agreement (EPS-AKA) are used to authenticate UEs with the Serving Network (SN) and also to generate the diverse necessary symmetric keys to ensure DI and DC [13]. The procedure of authentication and key derivation of the AKA protocol is achieved through four entities in LTE/LTE-A; the UE, the eNB, the Mobility Management Entity (MME) and the Home Subscriber Server (HSS). However, the involvement of all these entities in AKA protocol may have a negative effect on the latency and bandwidth consumption if AKA is to be employed for D2D communications. Therefore it is desirable to have an independent protocol to ensure the authentication of the two UEs as well as deriving the necessary keys for both DC and DI services. Accordingly, using public cryptography would be a promising tool for such kind of authentication since it has been already employed in similar scenarios for different wireless and mobile technologies. The principle idea is employing ECC in the authentication procedure besides using security hash functions in derivation of symmetric keys used for both DI and DC.

The rest of the chapter is organized as follows. In Section II, concepts of D2D in wireless and mobile technologies are presented. Section 3 describes the proposed security mechanism with its different phases. In Section 4, the security properties of the proposed scheme are analyzed and discussed. Finally, we conclude the chapter in Section 5.

5.2 D2D Authentication and key management in mobile and wireless technologies

In Chapter 2 we have already explained in detail the authentication and key agreement protocol AKA-EPS and we have explained why this protocol is not well suited for being used in the D2D scenario in LTE/LTE-A networks. Moreover, the concept of D2D such as ad-hoc WLAN mode has been available in IEEE 802.11 for many years but with a

limited usage compared to infrastructure mode. Additionally, authentication and key management for D2D communications have been already well studied in other wireless and mobile technologies such as Mobile Ad hoc Networks (MANET) [28], Wireless Sensor Networks (WSN) [29], Wireless Mesh Networks (WMN) [30], Bluetooth [31] and Vehicular Ad hoc Network (VANET) [32]. Yet, the employed paradigms and methodologies are not well suited for D2D in LTE/LTE-A because of the computation and communication overheads followed by deploying such methods, as well as the explicit difference in their security architecture.

Digital certificates issued by certificate authorities are among the cryptographic techniques employed for authentication in the aforementioned networks. However, the storage and transmission of the certificates are followed by a tremendous computation and communication overheads. In addition, the network should be provided with an infrastructure supporting such kind of certificates [58]. The authors in [59] propose using symmetric polynomial based key distribution for authentication and generation of symmetric keys using a cellular system. The main drawback of the suggested scheme is that the authors assume a secure channel for distributing the polynomials, which is not the case in reality. A similar concept has been used in the WMN in [60] (i.e. using polynomial based cryptography for key derivation). The Identity Based Cryptography (IBC) has been employed in [61] and the authors proposed using pairing to distribute the key between two neighboring nodes. However, this method is not well adapted for D2D in LTE-A due to the architecture difference between LTE-A and sensor networks. Besides in this method the derived key is used to sign the message which could not be realized in LTE/ LTE-A terminals due to the 3GPP requirements [13].

In this chapter, we propose an authentication and key agreement scheme for D2D communications in LTE-A. The presented solution is constructed to use asymmetric cryptography to authenticate two UEs wishing to start D2D communication with each other and later deriving symmetric keys for data encryption and integrity protection, but without any involvement of the core network. Our proposal aims to maintain security at the access level (E-UTRAN) by integrating a new entity to eNBs to function as a trusted third party and act as Private Key Generator (PKG). The proposed solution is based on Elliptic Curve Diffie-Hellman (ECDH) [62] which employs the elliptic Curve Cryptography (ECC) and is considered as a Discrete Logarithm Problem (DLP) that requires fully exponential time to be solved. The proposed key derivation and authentication scheme is divided into five phases: initialization (access request), temporary key generation, identification, shared identity generation, and finally ciphering and integrity key derivation. To the best of our knowledge, the lightweight security solutions for D2D

communications in LTE-A have not been yet well studied.

5.3 D2D Authentication and Key agreement scheme based on ECC

The AKA protocol and its extensions are not well suited for D2D in LTE-A due to the HN's involvement in the authentication procedure. Instead of forwarding the authentication request to the HN, both sides of communication could negotiate their key session directly through a trusted third party. The scenario of D2D as illustrated in Figure 5.1 shows that the traffic between two UEs (UE_2 and UE_3) is not passing through the HN.

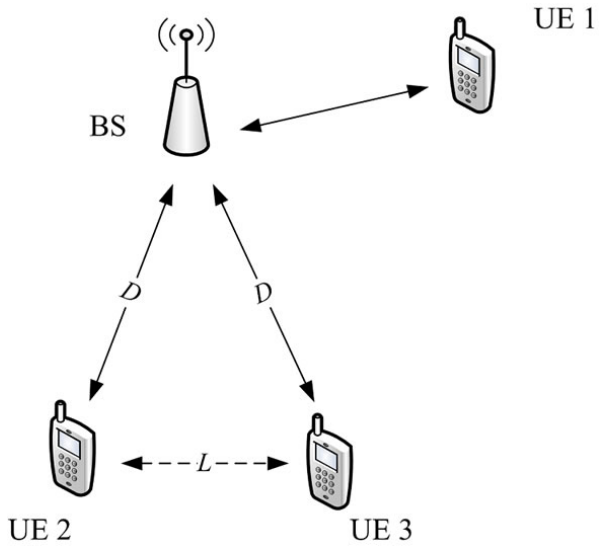


FIGURE 5.1: Scenario of LTE-A D2D communication

Hence, to authenticate the two devices with each other we prpose the use of asymmetric cryptography, and then the necessary keys are derived to be used for ensuring both data confidentiality and data integrity without passing through the core network. Accordingly, in such scenario the IBC using elliptic curves is one of the asymmetric encryption paradigms which could be applied efficiently with minimum communication and computation overheads. The concept of IBC first presented by Shamir in [63] is based on using users identity such as email address, phone numbers or still office locations as public keys. The private keys are generated using a trusted third party denoted in this paper as PKG.

Recently, the concept of IBC has attracted a lot of attentions due to its strong security performance and also its simplified authentication method compared to PKI [64]. Two approaches have been proposed for IBC: signature based and dedicated approaches. The

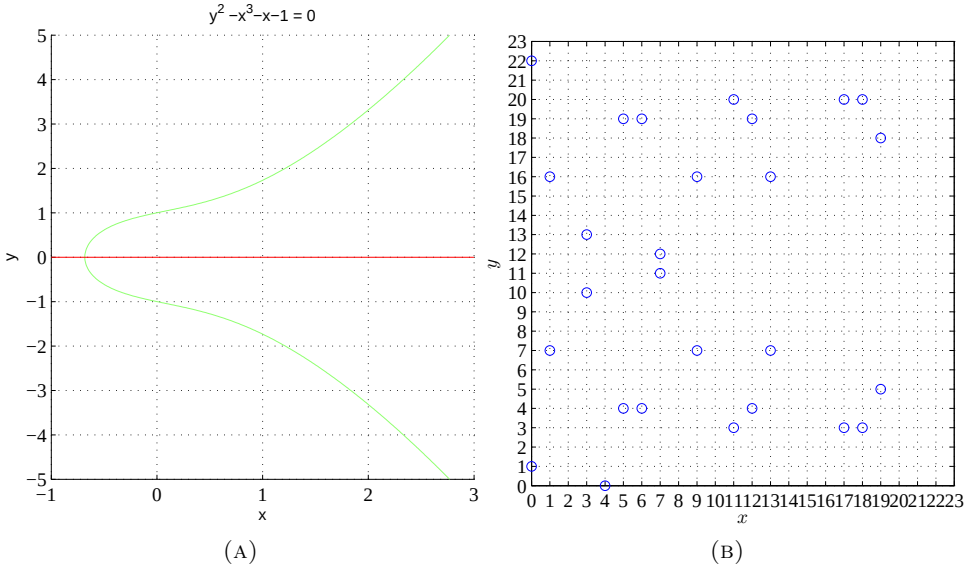
former are employing signature to authenticate the two parties of the communication and at the same time to protect the integrity of the message. The latter, instead of signing the message during authentication, first establish a symmetric session key between the two parties, and then the symmetric key is used for encryption and decryption. The majority of the protocols are based on dedicated approaches including the scheme presented in this paper. Moreover, one of the most employed cryptographic schemes for an IBC is based on ECC which generally allows the best balance in terms of speed, memory requirements and security level [65]. The major advantage of ECC compared to asymmetric schemes like RSA and Elgamal is its small key size (160 bits for ECC against 1024 bits in RSA with the same security level) [66].
An elliptic curve E_p over a prime field $\mathbb{F}_p$ can be defined as the set of all tuples $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying an equation of the following form:

$$y^2 = x^3 + ax + b \mod p \tag{5.1}$$

where a and b are the curve coefficients, that is to say two non negative integers belonging to $\mathbb{F}_p$, smaller than the prime number p and defining the curve $(E_p(a, b))$. We can notice that the curve coefficients have to fulfill the following condition:

$$4a^3 + 27b^2 \mod p \neq 0 \tag{5.2}$$

Figure 5.2 shows an example of an elliptic curve and illustrates the distribution of the elliptic group $E_{23}(1,\ 1)$.



(A) (B)

FIGURE 5.2: Elliptic curve equation (5.1) (a) and the distribution of Elliptic group $(E_{23}(1, 1)$ (b)

A well known protocol based on ECC is Elliptic Curve Diffie-Hellman (ECDH) [67]. It can be used to establish shared secret keys between two entities using an insecure communication channel and provides also perfect forward secrecy [68]. The original version of ECDH is vulnerable to MitM attacks because there is no authentication by the communication parties. However, the problem of authentication has been addressed and fixed in [69]. Before the ECDH key exchange can be carried out, the involved parties have to agree upon a common set of so-called domain parameters which specifies: the finite field $\mathbb{F}_p$, the elliptic curve E_p (i.e. the coefficients a and b), a base point G identifying the "start" of the curve, the order n of this subgroup, and the co-factor h which is usually equal to one in the prime field. Consequently, elliptic curve domain parameters over $\mathbb{F}_p$ are a sextuple $D = (p, a, b, G, n, h)$ which could be inserted in the UE's Universal Subscriber Identity Module (USIM)/Universal Integrated Circuit Card (UICC) as well as in the eNBs PKG.
Accordingly, the main idea of our device to device authentication and key agreement solution, based on ECDH scheme, is that each UE has a pair of public and private keys. The public key is only known by the eNB, which acts as a PKG, while the private key remains secret. Similarly, the eNB is also provided with a pair of keys; one is private and kept secret and the other is public and disclosed to the two UEs intending to initiate the D2D communication. Our scheme is divided in five phases: (A) Initialization, (B) temporary key generation, (C) identification, (D) permanent identity generation and finally (E) ciphering and integrity key generation.

5.3.1 Initialization

The device to device discovery, as shown in Figure 5.3, is outside the scope of this thesis. It is the first step of connection establishment between the two devices. The reader may refer to the works which have proposed different initializing protocols, using beacons or FHS in LTE technology as demonstrated in [70], [71].

5.3.2 Temporary key generation

The temporary key generation, as shown in Figure 5.4, is achieved separately in each of the two communication parties. The UEs of each communication pairs are responsible for generating their own public and private keys based on ECC.

More precisely, two UEs A and B have to generate secret keys d_A and d_B by selecting a random integer in $[1, n-1]$, where n is the order chosen for the ECC operations. Later, the two public keys of both UEs, Q_A and Q_B, are calculated using scalar multiplication. Scalar addition and multiplication are symbolized by $+$ and $\times$, respectively. Let G be

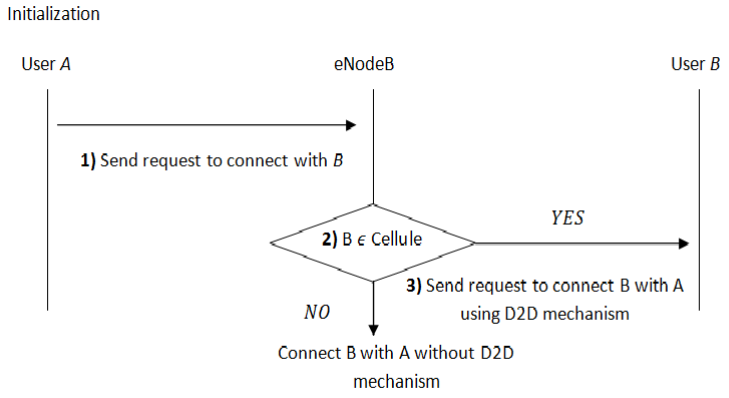


FIGURE 5.3: Initialization

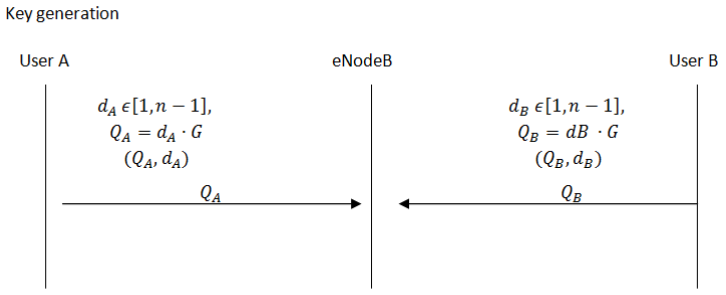


FIGURE 5.4: Temporary key generation

the curve generator which is the common domain parameter known by every registered UEs in the HN.

$$Q_A = d_A \times G \tag{5.3}$$

$$Q_B = d_B \times G \tag{5.4}$$

Each UE sends its own public key to the eNB to be handled by the PKG. Now the public keys Q_A and Q_B are known while d_A and d_B are kept secret.

5.3.3 Identification

The identification scheme is shown in Figure 5.5. In order to identify each of the two devices by the eNB, a three move protocol (commitment, challenge, response) is adopted without disclosing any information about real UEs identity.

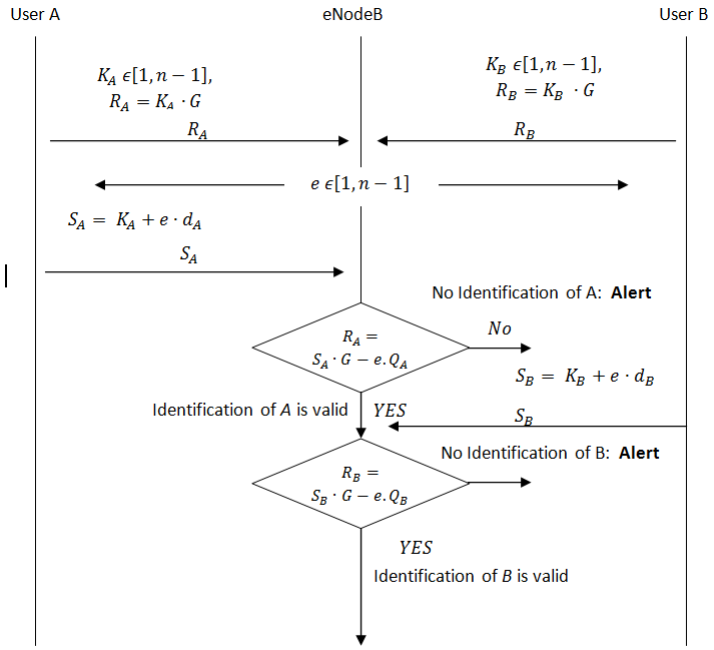


FIGURE 5.5: Identification

Here, the basic idea is that UEs A and B will select a random integer in $[1, n-1]$ (k_A and k_B, respectively) as temporary secret key to hide their real identity. Each UE will compute its own blind identity as follows:

$$R_A = k_A \times G \tag{5.5}$$

$$R_B = k_B \times G \tag{5.6}$$

Hence, these two parameters are used to identify both UEs by the eNB. Then, the eNB selects a random integer from $e \in [1, n-1]$ and sends it to both UEs A and B to compute S_A and S_B respectively.

$$S_A = k_A + e \times d_A \tag{5.7}$$

$$S_B = k_B + e \times d_B \tag{5.8}$$

Finally, these results are sent by the UEs to the eNB, which verifies R_i ($i = A$ or B) as follow:

$$
\begin{aligned}
& S_i \times G - e \times Q_i \\
&= k_i \times G + e \times d_i \times G - e \times d_i \times G \\
&= k_i \times G \\
&= R_i
\end{aligned} \tag{5.9}
$$

Hence, UEs A and B are authenticated.

5.3.4 Shared Identity Generation (SIG)

After authentication, the SIG is executed as in Figure 5.6.

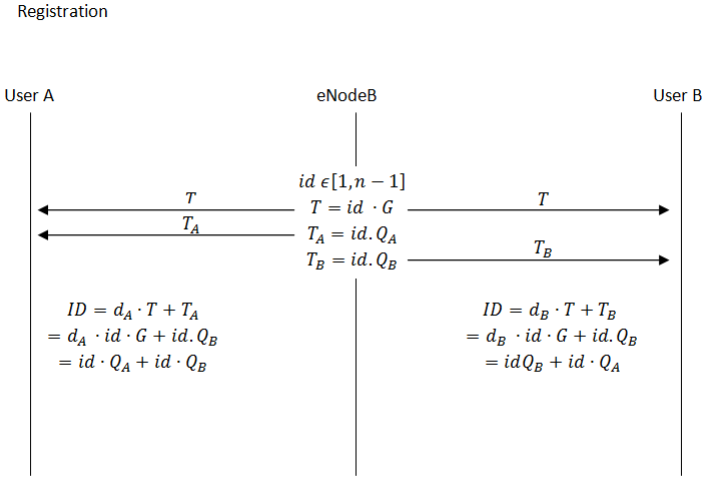


FIGURE 5.6: Shared identity Generation

Based on ECDH key agreement scheme, the eNB selects a random number $id \in [1, n-1]$ to compute a public common identifier T which is sent to both UEs.

$$T = id \times G \tag{5.10}$$

Then, the eNB computes T_A (respectively T_B) and sends it to B (respectively A).

$$T_A = id \times Q_A \tag{5.11}$$

$$T_B = id \times Q_B \tag{5.12}$$

Finally, each UE computes a private common identifier (ID) as follow:

In UE A side

$$\begin{aligned} ID &= d_A \times T + T_A \\ &= d_A \times id \times G + id \times Q_B \\ &= id \times Q_A + id \times Q_B \end{aligned} \tag{5.13}$$

In UE B side

$$\begin{aligned} ID &= d_B \times T + T_B \\ &= d_B \times id \times G + id \times Q_A \\ &= id \times Q_B + id \times Q_A \end{aligned} \tag{5.14}$$

This proves that both permanent identities are identical and could be used as common input for the permanent key derivation phase.

5.3.5 Ciphering and integrity keys generation

To provide more robustness against attacks, we propose a new scheme of dynamic key generation for KI and KE by using the secret ID as shown in the Figure 5.7. Additionally, some information $addin_A$, $addin_B$ about both users A and B are concatenated with ID to produce session key V as below:

$$V = hash(ID||addin_A||addin_B)$$

After that, V is processed into two parallel hash functions and with different input parameters (counter and variable s), that are concatenated with the session key V to produce the corresponding dynamic key. Character s is equal to I or E for integrity and ciphering services respectively.

Then, KI and KE are produced as follows:

$$KI = LSB_{128}\{hash(V||CTR_I||I)\}$$
$$KE = LSB_{128}\{hash(V||CTR_E||E)\}$$

where $LSB_n\{X\}$ returns the bit string consisting of the n least significant bits of the bit string X and $hash$ can be any secure cryptographic hash function. In addition, the counter of each security service is incremented if the user requests its corresponding security service (CTR_E for ciphering and CTR_I for Integrity).

Moreover, the session key V and dynamic key DK should be updated for several numbers of requests to provide more robustness against attacks. The cycle length for each session and dynamic key are defined as d and w packets respectively and $d \geq w$. In fact, lower w and d, produces higher security level but also require additional computation complexity.

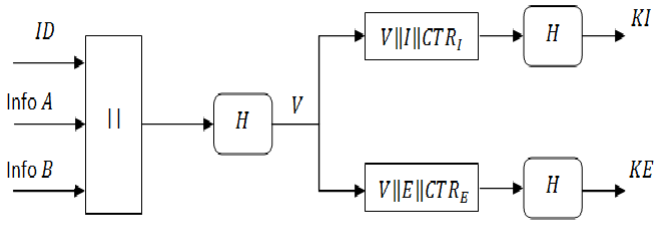


FIGURE 5.7: Cipher and Integrity Key generation

The proposed technique for updating the session and dynamic key are described as pseudo-code in Figure 5.8. The variable i is an integer value representing the number of requests (encryption or integrity). The hash function SHA_256 is used to produce a new session key V when i attains $\alpha \times d$, with $\alpha = 1,\ 2,\ \ldots$ In response, updating V leads to produce different (integrity and ciphering) dynamic keys. The dynamic key (DK) represents KI or KE. DK is updated when i attains $\beta \times w$, $\beta = 1,\ 2,\ \ldots$. These keys are used for the data integrity and confidentiality services, which are realized in the PDCP sub-layer of the LTE/LTE-A protocol stack.

5.4 Security analysis of the proposed protocol

The security of our protocol is achieved thanks to the use of ECC approach since it is unfeasible for attackers to break up the protocol and find the secret keys of the algorithms

procedure DYNAMIC_KEY_UPDATE($V, adin, i, c1, w, d$)
  if $i \bmod d = 0$ **then**
    $c1 \leftarrow c1 + 1$
    $V \leftarrow SHA\_256(V||c1||adin)$
  else
    if $i \bmod w = 0$ **then**
      $DK \leftarrow LSB_{128}\{SHA\_256(V||adin||c1||i)\}$
    end if
  end if
  return $DK, V, i, c1$
end procedure

FIGURE 5.8: Dynamic Key updates algorithm

if a suitable size of curve $E(n)$ is used. Additionally, the prime p is chosen to have sufficient points on the curve for a stronger cryptographic security. Accordingly, the attacks difficulty is related to the hardness of solving the Elliptic Curve Discrete Logarithmic Problem (ECDLP) and the best algorithm known for solving such problem requires very high computational time, which is fully exponential if the domain parameters are chosen with care. Moreover the larger the curve sizes the better the security level. However, for a complete performance evaluation, one should also consider the communication and computation overheads especially when dealing with resource-limited devices such as LTE-A terminals. In the following, several security aspects of the proposed scheme are analyzed.

5.4.1 Randomness of the produced dynamic key

The security strength of the proposed solution is depending on the produced dynamic keys; therefore the key derivation function should produce key-streams with high level of randomness. Some parameters of the LTE-terminal information are used in addition to the counter to form the Initial Vector (IV). The input block of the second iterated hash function is constructed form the Vector V, the characters I or E and the counter CTR_I or CTR_E for data integrity and confidentiality, respectively. The cipher block is renewed for each block, consequently the produced dynamic keys (KI and KE) are updated.

To show the randomness properties, the produced dynamic key-stream is analyzed using the randomness test of NIST [43]. In order to get correct statistical results one needs to provide 100 secret keys (ID) and each one produces a dynamic key-stream with 1000000 bit length. The NIST test performs 15 tests on the data sample, with a total amount of executed tests of 189. The obtained NIST results are shown in Figure 5.9, where obtained proportion values (success rate) show how many samples have passed

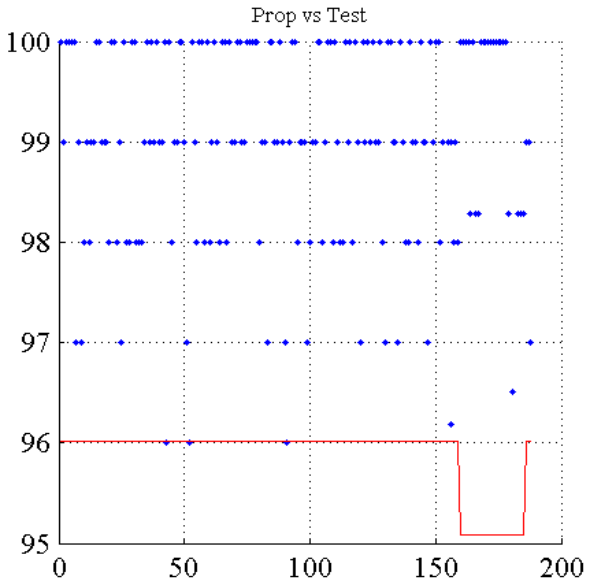


FIGURE 5.9: Proportion values of NIST tests

the given tests. The red line marks minimum proportion values in order to consider the sequence random. Random Excursions and Random Excursions Variant tests represent 26 tests with different parameters. The simulation results indicate that the produced sequences pass all the tests and consequently the randomness and uniformity of the generated dynamic key-streams are attained.

5.4.2 Identity privacy

One of the security requirements of any data exchange is the privacy of the communication parties. Indeed, using a combination of temporal private keys hide the real identity of the UEs since only the public key is diffused. Accordingly, the real identity of the UEs is preserved in the permanent secret keys and never revealed. This ensures that some threats related to the user location tracking attacks are not possible. Note that in the AKA protocol, the real identity of the UEs are revealed in two special cases: when the UE connects the HN for the first time and in the case of a MAC verification failure [72].

5.4.3 Resistance to the man in the middle attack

The MitM attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them. While the original ECDH and AKA protocol are vulnerable to the MitM attacks, our protocol has adopted an authentication procedure through the identification of the UEs by the eNB. Indeed during the UEs identification UEs the quantity $S_A = k_A + e \times d_A$ working as

an implicit signature for UE A. It is a signature in the sense that the only person who knows A's private key d_A can produce SA. Later, the eNB verifies the validity of the signature through the calculation of $S_A \times G - e \times Q_A$. In the same way, the quantity $S_B = k_B + e \times d_B$ serves as a signature for UE B and is verified by the eNB through $S_B \times G - e \times Q_B$.

5.4.4 Resistance to impersonation attacks

In the impersonation attack, an adversary may pretend to be another UE or even an eNB to deceive the users. Indeed, another goal of the identification procedure is the resistance of the protocol against impersonation under active attacks. Moreover, the authentication procedure is depending on Zero information about the real identity of the UE and adversary should provide both public and temporary secret keys in order to be identified by the eNB. Therefore, the adversary again is facing the ECDLP to guess the secret keys and consequently an exponential-time algorithm is required to obtain the temporary secret key.

5.5 Conclusion and Discussion

In this chapter, we have proposed a novel authentication and key generation scheme for D2D communications in LTE-A networks. Our scheme employs the public key cryptography for authentication and derives symmetric keys using one-way hash functions for both data encryption and integrity protection. We have adopted the concept of ECC due to its use of small key size compared to other public key cryptography schemes such as RSA, which consequently leads in to less computation and communication complexity. Moreover, the proposed scheme uses EDCH for key agreement between the two UEs intending to establish a D2D communication without involving the home network in the procedure. In order to secure the EDCH, the solution implements identification using signatures to authenticate the two devices with the PKG of the eNB. Security analysis and simulation results have demonstrated the randomness of the generated keys, which makes it difficult for the attackers predicting the keys. Additionally, the authentication scheme has been analyzed in terms of its strength against different attacks and it has been shown that our scheme is achieving identity privacy and is immune against MitM and impersonation attacks. In conclusion the proposed protocol could be efficiently employed in the authentication procedure between two UEs involving in D2D communications under LTE/LTE-A network coverage.

Chapter 6

Conclusion and future works

6.1 Conclusions

In this thesis, we addressed two main challenges related to the security services of LTE/LTE-A networks: we proposed lightweight encryption and integrity algorithms in order to achieve data confidentiality and data integrity, and a novel authentication and key agreement protocol for Device to Device communications. For a better understanding of the required functionalities of security services as well as paradigms employed to realize these services, we first introduced a detailed description of LTE/LTE-A networks security architecture. Our thorough analysis of this architecture as it was suggested and drafted by the 3GPP had allowed us discover where, when and how the requested security services are achieved.

The 3GPP committee has defined five security levels for the LTE/LTE-A networks namely: network access security, network domain security, user domain security, application domain security and non 3GPP domain security. We have primarily focused on the security features and services at network access security level in our thesis.

Data confidentiality is an important security service which has to be provided in LTE/LTE-A networks. To protect user and mobile operator's information privacy and confidentiality, encryption is a common method to achieve this goal. So far the 3GPP standardized three encryption algorithms to be employed in LTE/LTE-A networks, namely EEA1, EEA2 and EEA3 which their designs are based on Snow 3G, AES and ZUC, respectively. However, the state of art related to these standardized solutions clearly revealed considerable drawbacks in terms of computational complexity as well as security flaws. To

deal with limitations we proposed a novel robust and lightweight encryption algorithm, named ERCA which showed less computational complexity and consequently better energy consumption.

ERCA algorithm is basically designed based on substitution diffusion structure. Unlike the standardized algorithms which are mostly based on Shannon's theory for encryption algorithms in which it is recommended applying confusion and diffusion for several rounds to attain strong security strength, our purposed solution reduces the complexity to one round. The novel proposed stream cipher is composed from a round function consisting of an addition, a substitution and a diffusion layer. ERCA has been subjected to most necessary statistical and analytical tests to verify its security strength and simulation results have demonstrated clearly that it possesses most of the requested cryptographic properties to be considered as a robust and secure cipher algorithm. In terms of complexity we compared ERCA to EIA2 algorithm since it is using a similar structure and its core algorithm (AES) is considered as the most secure standardized solution. Moreover, the simulation results in terms of execution time have demonstrated that our proposal is at least 4.5 times faster than AES (EIA2).

Integrity protection is another important security service specifically in LTE/LTE-A networks to assure the accuracy and consistency of the control plane data. The integrity protection is achieved using MACs and the 3GPP has proposed three set of algorithms EIA1, EIA2 and EIA3 which employ the same core ciphers already used in confidentiality algorithms for generating the MAC. Similarly, before presenting our alternative DI solution, we first highlighted the main limitations and flaws of the standardized reference solutions.

ERADI algorithm was our second contribution in this dissertation. Unlike the standardized solution where the same cipher algorithm is used in both encryption and integrity protection only due to re-usability purposes, in this thesis we used a different modified version of the cipher in the core of the proposed ERADI by adding a chaining layer to the original algorithm employed in data confidentiality. Adding a chaining layer had allowed us to have better bit dependency with a negligible overhead to the cipher algorithm complexity. The performance of ERADI has been evaluated using well-known statistical and analytical tests in terms of robustness and security. The obtained results showed its effectiveness in generating credible MAC to be employed in integrity protection in LTE/LTE-A networks. Moreover, to quantify the gain in complexity, a comparison has been realized with EIA2 algorithm which is based on AES. The results showed better

performance of ERADI algorithm which was at least about 4.5 times faster than EIA2.

Authentication of subscribers is considered as one of the most important security features of mobile networks. We first explained how a UE is authenticated with the core network using EPS-AKA protocol which, besides authentication, is also in charge of deriving necessary key sessions employed in both traffic encryption and integrity protection in different security levels. AS neither EPS-AKA nor other enhanced authentication protocols proposed in the literature considered D2D communications paradigm, we proposed a novel authentication protocol able to support such communication scenarios.

Finally, the last contribution of our thesis was proposing an authentication and key derivation protocol for D2D communications under LTE/LTE-A environment since D2D communications would also contribute to the energy savings in such networks. As the best of our knowledge, security in D2D and particularly authentication between the two communicating devices has not been well addressed since the D2D paradigm is quite a new feature in LTE/LTE-A networks. Different from the original EPS-AKA protocol which is based on symmetric cryptography, our proposed scheme uses public key cryptography for authentication and at the same time derives symmetric keys using one-way hash functions. Indeed, we have employed the concept of ECC due to its use of small key size compared to other public key cryptography schemes such as RSA, which in return achieves reduced computation and communication complexities. The authentication scheme has been analyzed in terms of its security strength against several different attacks to assess its appropriateness for such scenarios. We have demonstrated analytically the strength of the proposed scheme in achieving identity privacy and resisting MitM and impersonation attacks. Furthermore, we have also subjected the generated keys from our scheme to the statistical analysis which in turn showed clearly their randomness.

6.2 Future works and perspective

The works developed in this thesis open new directions for research to extend some of the proposals or consider further new complementary developments, we present in the following some possible directions.

- A theoretical analysis of the ERCA encryption algorithm would be interesting to elaborate such as a theoretical analysis which would assay the permutation and

substitutions functions and prove mathematically that ERCA algorithm is less complex compared to AES.

- Further complexity and performance comparisons of the proposed mechanisms with non standardized stream cipher and block cipher algorithms would be a significant extension of our work.

- An alternative method for authentication protocols already proposed for D2D communications is using pairing in ECC instead of scalar multiplication and additions. Using pairing should allow more security and less computation complexity compared to scalar addition and multiplication. Another interesting development should consider such approaches and compare it to our solution.

- An extension of the D2D communication protocol is possible when considering that the two devices involved in D2D communications do not belong to the same cell. The potential extension could use other entities than the third trusted party during the authentication procedure. However, such solutions would introduce more complexity since the communication security in such cases is more vulnerable to security attacks and threats.

Appendix A

List of publications

The main results and findings of this thesis have been published prior to the defense in two international conferences and another paper has been already accepted in other international conference.

Conferences

1-Soran Hussein, Hassan Noura, Steven Martin, Lila Boukhatem, and Khaldoun Al Agha. 2013. ERCA: Efficient and Robust Cipher Algorithm for LTE Data Confidentiality. In Proceedings of the 16th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems (MSWiM '13). ACM, New York, NY, USA, 299-30.

2–Soran Hussein, Hassan Noura, Steven Martin, Lila Boukhatem. Device to Device Lightweight Authentication and Key Agreement Protocol for LTE-A Networks. In Proceedings of the IEEE 23rd International Conference onComputer Communication and Networks (ICCCN), , vol., no., pp.1,7, 4-7 Aug. 2014.

3-Hassan Noura, Soran Hussein ,Steven Martin, Lila Boukhatem, and Khaldoun Al Agha.-ERDIA: An Efficient and Robust Data Integrity Algorithm for Mobile and Wireless Networks. Accepted in 2015 IEEE Wireless Communications and Networking Conference WCNC 2015.

Bibliography

[1] C. B. Sankaran. Network access security in next-generation 3gpp systems: a tutorial. *Comm. Mag.*, 47(2):84–91, feb 2009. ISSN 0163-6804. doi: 10.1109/MCOM.2009.4785384. URL `http://dx.doi.org/10.1109/MCOM.2009.4785384`.

[2] Ajay R Mishra. *Fundamentals of cellular network planning and optimisation: 2G/2.5 G/3G... evolution to 4G*. John Wiley & Sons, 2004.

[3] 3GPP Technical Specification Group Services and Systems Aspects. System Architecture Evolution (SAE); Security Architecture (Release 11). Tech. Rep. 3G TS 33.401 v11.6.0,3 rd Generation Partnership Project., 2012.

[4] Luis Suarez, Loutfi Nuaymi, and Jean-Marie Bonnin. An overview and classification of research approaches in green wireless networks. *EURASIP Journal on Wireless Communications and Networking*, 2012(1):142, 2012. doi: 10.1186/1687-1499-2012-142. URL `http://dx.doi.org/10.1186/1687-1499-2012-142`.

[5] Yan Chen, Shunqing Zhang, Shugong Xu, and G.Y. Li. Fundamental trade-offs on green wireless networks. *Communications Magazine, IEEE*, 49(6):30–37, June 2011.

[6] A Asadi, Q. Wang, and V. Mancuso. A Survey on Device-to-Device Communication in Cellular Networks. *Communications Surveys Tutorials, IEEE*, PP(99):1–1, 2014.

[7] X. Lin, J.G. Andrews, A Ghosh, and R. Ratasuk. An overview of 3gpp device-to-device proximity services. *Communications Magazine, IEEE*, 52(4):40–48, April 2014. ISSN 0163-6804. doi: 10.1109/MCOM.2014.6807945.

[8] Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, and Valtteri Niemi. *LTE security*, volume 1. John Wiley & Sons, 2012.

[9] Evolved Universal Terrestrial Radio Access (E UTRA); Packet Data Convergence Protocol (PDCP) Specification. Tech. Rep 3GPP TS 36.323. , March 2009.

[10] ETSI Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification (3GPP TS 35.201 version 7.0.0 Release 7)) Juin 2007, .

[11] ETSI/SAG: Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 and 128-EIA3. document 1: 128-EEA3 and 128-EIA3 specification. Version 1.5. Tech. rep., ETSI , January 2011.

[12] Claude E. Shannon. Communication Theory of Secrecy Systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[13] ETSI Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System(UMTS); LTE; 3GPP System Architecture Evolution (SAE); (3GPP TS 33.401 version 11.7.0 Release 11)) July 2013, .

[14] Hyeran Mun, Kyusuk Han, and Kwangjo Kim. 3g-wlan interworking: security analysis and new authentication and key agreement based on EAP-AKA. In *Wireless Telecommunications Symposium, 2009. WTS 2009*, pages 1–8. IEEE, 2009.

[15] Li Xiehua and Wang Yongjun. Security enhanced authentication and key agreement protocol for LTE/SAE network. In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, pages 1–4. IEEE, 2011.

[16] J Bou Abdo, Hakima Chaouchi, and Mohammad Aoude. Ensured confidentiality authentication and key agreement protocol for eps. In *Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on*, pages 73–77. IEEE, 2012.

[17] GM Koien. Mutual entity authentication for lte. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pages 689–694. IEEE, 2011.

[18] Muhammad Al-Humaigani, Derrek B Dunn, and D Brown. Security transition roadmap to 4g and future generations wireless networks. In *System Theory, 2009. SSST 2009. 41st Southeastern Symposium on*, pages 94–97. IEEE, 2009.

[19] Feng Hao and Peter Ryan. J-pake: authenticated key exchange without pki. In *Transactions on computational science XI*, pages 192–206. Springer, 2010.

[20] Zhiyuan Shi, Zhiliang Ji, Zhibin Gao, and Lianfen Huang. Layered security approach in lte and simulation. In *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*, pages 171–173. IEEE, 2009.

[21] Shadi Traboulsi, Mohamad Sbeiti, Felix Bruns, Sebastian Hessel, and Attila Bilgic. An optimized parallel and energy-efficient implementation of snow 3g for lte mobile devices. In *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pages 535–538. IEEE, 2010.

[22] Blandine Debraize and Irene Marquez Corbella. Fault analysis of the stream cipher snow 3g. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 103–110. IEEE, 2009.

[23] Anastasios N Bikos and Nicolas Sklavos. Lte/sae security issues on 4g wireless networks. *Security & Privacy, IEEE*, 11(2):55–62, 2013.

[24] Frederic P. 'Miller, Agnes F. Vandome, and John= McBrewster. *'Advanced Encryption Standard=*. Alpha Press, 2009. ISBN 6130268297, 9786130268299.

[25] Morris Dworkin. Nist special publication 800-38d. *NIST special publication*, 800: 38D, 2007.

[26] Teng Wu and Guang Gong. The weakness of integrity protection for lte. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 79–88. ACM, 2013.

[27] P. Szalachowski, B. Ksiezopolski, and Z. Kotulski. CMAC, CCM and GCM/GMAC: advanced modes of operation of symmetric block ciphers in wireless sensor networks. *Information Processing Letters*, 110(7):247 – 251, 2010. ISSN 0020-0190.

[28] Johann Van Der Merwe, Dawoud Dawoud, and Stephen McDonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Comput. Surv.*, 39(1), April 2007. ISSN 0360-0300. doi: 10.1145/1216370.1216371. URL `http://doi.acm.org/10.1145/1216370.1216371`.

[29] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway. A survey of key management schemes in wireless sensor networks. *Computer Communications*, 30(11–12):2314 – 2341, 2007. ISSN 0140-3664. doi: http://dx.doi.org/10.1016/j.comcom.2007.04.009. URL `http://www.sciencedirect.com/science/article/pii/S0140366407001752`. Special issue on security on wireless ad hoc and sensor networks.

[30] Yingfang Fu, Jingsha He, Rong Wang, and Guorui Li. Mutual authentication in wireless mesh networks. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 1690–1694, May 2008. doi: 10.1109/ICC.2008.326.

[31] Brent A Miller and Chatschik Bisdikian. *Bluetooth revealed: the insider's guide to an open specification for global wireless communication*. Prentice Hall PTR, 2001.

[32] S. Busanelli, G. Ferrari, and L. Veltri. Short-lived key management for secure communications in vanets. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 613–618, Aug 2011. doi: 10.1109/ITST.2011.6060129.

[33] Thomas Fuhr, Henri Gilbert, Jean-René Reinhard, and Marion Videau. Analysis of the initial and modified versions of the candidate 3gpp integrity algorithm 128-eia3. In *Selected Areas in Cryptography*, pages 230–242. Springer, 2012.

[34] Carlos M. Gutierrez. Recommendation for block cipher modes of operation:, 2007.

[35] Morris Dworkin. Recommendation for block cipher modes of operation. methods and techniques. Technical report, DTIC Document, 2001.

[36] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[37] Digital cellular telecommunications system (phase 2+); Universal Mobile Telecommunications System (UMTS); mobile application part (MAP) specification (3GPP TS 29.002 version 11.5.0 Release 11) , February 2013.

[38] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin. The RC6 TM Block Cipher. In *in First Advanced Encryption Standard (AES) Conference*, page 16, 1998.

[39] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 386–397, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc. ISBN 3-540-57600-2. URL `http://dl.acm.org/citation.cfm?id=188307.188366`.

[40] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Journal of Cryptology*, Vol. 4, No. 1 1991, pp. 3-72.

[41] A. F. Webster and Stafford E. Tavares. On the design of s-boxes. In *Advances in Cryptology*, CRYPTO '85, pages 523–534, London,UK, 1986. Springer-Verlag. ISBN 3-540-16463-4. URL `http://dl.acm.org/citation.cfm?id=646751.704578`.

[42] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 55–64, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc. ISBN 3-540-57600-2. URL `http://dl.acm.org/citation.cfm?id=188307.188323`.

[43] Andrew Rukhin, Juan Soto, James Nechvatal, Elaine Barker, Stefan Leigh, Mark Levenson, David Banks, Alan Heckert, James Dray, San Vo, Andrew Rukhin, Juan Soto, Miles Smid, Stefan Leigh, Mark Vangel, Alan Heckert, James Dray, and Lawrence E Bassham Iii. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2001.

[44] Thirteen Ways to Look at the Correlation Coefficient. *The American Statistician*, 42(1):59–66, 1988. doi: 10.2307/2685263.

[45] C.B. Bates and NAVAL WEAPONS LAB DAHLGREN VA. *The Chi-square Test of Goodness of Fit for a Bivariate Normal Distribution.* Defense Technical Information Center, 1966.

[46] A. Kanso and M. Ghebleh. A fast and efficient chaos-based keyed hash function. *Communications in Nonlinear Science and Numerical Simulation*, 18(1):109 – 123, 2013. ISSN 1007-5704.

[47] Ivan Damgård. A design principle for hash functions. In *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '89, pages 416–427, London, UK, UK, 1990. Springer-Verlag. ISBN 3-540-97317-6.

[48] Ralph C. Merkle. One way hash functions and des. In *CRYPTO*, pages 428–446, 1989.

[49] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology—CRYPTO'96*, pages 1–15. Springer, 1996.

[50] Erez Petrank and Charles Rackoff. Cbc mac for real-time data sources. *Journal of Cryptology*, 13(3):315–338, 2000.

[51] John Black and Phillip Rogaway. Cbc macs for arbitrary-length messages: The three-key constructions. In *Advances in Cryptology—CRYPTO 2000*, pages 197–215. Springer, 2000.

[52] Tetsu Iwata and Kaoru Kurosawa. Omac: One-key cbc mac. In *Fast Software Encryption*, pages 129–153. Springer, 2003.

[53] Kaoru Kurosawa and Tetsu Iwata. Tmac: Two-key cbc mac. In *Topics in Cryptology—CT-RSA 2003*, pages 33–49. Springer, 2003.

[54] Mihir Bellare, Roch Guérin, and Phillip Rogaway. *XOR MACs: New methods for message authentication using finite pseudorandom functions.* Springer, 1995.

[55] ETSI Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System(UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102 version 11.5.0 Release 11) February, 2013, .

[56] Xiaoyun Wang and Hongbo Yu. How to break md5 and other hash functions. In *In EUROCRYPT*. Springer-Verlag, 2005.

[57] Astely, D. and Dahlman, E. and Fodor, G. and Parkvall, S. and Sachs, J. LTE release 12 and beyond [Accepted From Open Call]. *Communications Magazine, IEEE*, 51(7):154–160, July 2013. ISSN 0163-6804. doi: 10.1109/MCOM.2013.6553692.

[58] E Silva, A Dos Santos, Luiz Carlos P Albini, and Michele N Lima. Identity-based key management in mobile ad hoc networks: techniques and applications. *Wireless Communications, IEEE*, 15(5):46–52, 2008.

[59] Ananya Gupta, Anindo Mukherjee, Bin Xie, and Dharma P. Agrawal. Decentralized key generation scheme for cellular-based heterogeneous wireless ad hoc networks. *J. Parallel Distrib. Comput.*, 67(9):981–991, September 2007. ISSN 0743-7315. doi: 10.1016/j.jpdc.2007.05.009. URL `http://dx.doi.org/10.1016/j.jpdc.2007.05.009`.

[60] Bing He, S. Joshi, D.P. Agrawal, and Dongmei Sun. An efficient authenticated key establishment scheme for wireless mesh networks. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5, Dec 2010. doi: 10.1109/GLOCOM.2010.5683733.

[61] Manel Boujelben, Habib Youssef, Rania Mzid, and Mohamed Abid. Ikm–an identity based key management scheme for heterogeneous sensor networks. *Journal of Communications*, 6(2), 2011.

[62] NIST, Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2006.

[63] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc. ISBN 0-387-15658-5. URL `http://dl.acm.org/citation.cfm?id=19478.19483`.

[64] Marko Hölbl, Tatjana Welzer, and Bostjan Brumen. An improved two-party identity-based authenticated key agreement protocol using pairings. *J. Comput. Syst. Sci.*, 78(1):142–150, 2012.

[65] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177): 203–209, 1987.

[66] Jenny Torres Olmedo. *A Secure and Reliable Identity Management Architecture for Future Internet*. PhD thesis, Université Pierre et Marie Curie-Paris 6, 2013.

[67] Marco Holbl. *Development of Identity Based Authenticated Key Agreement Protocol*. PhD thesis, University of Maribor, 2009.

[68] JoséLuis Gómez Pardo. Introduction to Public-Key Cryptography: The Diffie–Hellman Protocol. In *Introduction to Cryptography with Maple*, pages 399–417. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-32165-8. doi: 10.1007/978-3-642-32166-5_7. URL `http://dx.doi.org/10.1007/978-3-642-32166-57`.

[69] Hugo Krawczyk. Sigma: The 'sign-and-mac' approach to authenticated diffie-hellman and its use in the ike-protocols. In *CRYPTO*, pages 400–425, 2003.

[70] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Mikloas, and Z. Turanyi. Design aspects of network assisted device-to-device communications. *Communications Magazine, IEEE*, 50(3):170–177, March 2012. ISSN 0163-6804. doi: 10.1109/MCOM.2012.6163598.

[71] Lei Lei, Zhangdui Zhong, Chuang Lin, and Xuemin Shen. Operator controlled device-to-device communications in LTE-advanced networks. *Wireless Communications, IEEE*, 19(3):96–104, June 2012. ISSN 1536-1284. doi: 10.1109/MWC.2012.6231164.

[72] Cao, Jin and Ma, Maode and Li, Hui and Zhang, Yueyu and Luo, Zhenxing. A Survey on Security Aspects for LTE and LTE-A Networks. *Communications Surveys Tutorials, IEEE*, 16(1):283–302, Jan 2014. ISSN 1553-877X. doi: 10.1109/SURV.2013.041513.00174.