



**Ain Shams University**  
**Faculty of Engineering**  
**Cairo-Egypt**

Department of Electronics and Communication Engineering

# **Authentication Techniques in Mobile Communications**

by

**Zakaria Zakaria Hassan Hassan**

A Thesis

Submitted in Partial Fulfillment of the  
Requirements for the Degree of

**Master of Science**  
in Electrical Engineering

at

Faculty of Engineering - Ain Shams University

**Supervised by**

**Prof. Dr. Abdelhalim Zekry**

Professor in the Electronics and Communications Engineering Department  
Faculty of Engineering - Ain shams University

**Prof. Dr. Talaat Abdellatief Elgarf**

Professor in the Electrical and Computer Engineering Department  
Higher Technological Institute (HTI)

2014



**AIN SHAMS UNIVERSITY  
FACULTY OF ENGINEERING  
CAIRO-EGYPT**

Department of Electronics and Electrical Communications Engineering

Name: **Zakaria Zakaria Hassan Hassan Abdelwahab**

Thesis title: **"Authentication Techniques in Mobile Communications"**.

Degree: **Master of Science in Electrical Engineering** (Electronics and Electrical Communications Engineering Department).

**EXAMINERS COMMITTEE**

| <b>Name</b>                                                                                                                                          | <b>Signature</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>Prof.Dr. Salah Sayed Ibrahim Elagooz</b><br>Electronics and Electrical Communications Eng.Dept.<br>El Shorouk Academy                             | .....            |
| <b>Prof.Dr. Wagdy Refaat Anis</b><br>Electronics and Electrical Communications Eng.Dept.<br>Faculty of Engineering – Ain Shams University            | .....            |
| <b>Prof.Dr. Abdelhalim AbdulNabi Zekry</b><br>Electronics and Electrical Communications Eng.Dept.<br>Faculty of Engineering – Ain Shams University   | .....            |
| <b>Prof. Dr. Talaat Abdellatief Elgarf</b><br>Electrical and Computers Eng.Dept.<br>Higher Technological Institute (HTI) 10 <sup>th</sup> Of Ramadan | .....            |

**Date:**     /     /

# STATEMENT

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering (Electronics and Communications Engineering).

The work included in this thesis was carried out by the author at the Electronics and Communications Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

No part of this thesis was submitted for a degree or a qualification at any other University or institution.

**Name:** Zakaria Zakaria Hassan Hassan Abdelwahab

**Signature:**

**Date:** 11/8/2014

# **CURRICULUM VITAE**

**Name of Researcher** : Zakaria Zakaria Hassan Hassan Abdelwahab

**Date of Birth** : 27/9/1987

**Place of Birth** : Cairo, Egypt

**First University Degree** : B.Sc. in Electrical Engineering

**Name of University** : Higher Technological Institute, 10<sup>th</sup> of Ramadan

**Date of Degree** : August 2009

# Abstract

MILENAGE Algorithm applies the block cipher Rijndael (AES) with 128 bit key and 128 bit block size. This algorithm is used in the 3GPP authentication and key generation functions ( $f_1$ ,  $f_1^*$ ,  $f_2$ ,  $f_3$ ,  $f_4$ ,  $f_5$  and  $f_5^*$ ) for mobile communication systems (GSM/UMTS/LTE). In this thesis a modification of Milenage algorithm is proposed through a dynamic change of S-box in AES depending on secret key. To get a new secret key for every authentication process we add the random number (RAND) transmitted from the authentication center (AuC) to the contents of the fixed stored secret key (K) and thus the initialization of the AES will be different each new authentication process. For every change in secret key a new S-box is derived from the standard one by permuting its rows and columns with the help of a new designed PN sequence generator. A complete simulation of modified Milenage and PN sequence generator is done using Microcontroller (PIC18F452). Security analysis is applied using Avalanche test to compare between the original and modified Milenage. Tests proved that the modified algorithm is more secure than the original one due to the dynamic behavior of S-box with every change of the secret key and immunity against linear and differential cryptanalysis using Avalanche tests. This makes the modified Milenage more suitable for the applications of authentication techniques especially for mobile communication systems.

**Keywords:** Authentication vector (AV), Modified MILENAGE Algorithm for AKA Functions ( $F_1$ ,  $F_1^*$ ,  $F_2$ ,  $F_3$ ,  $F_4$ ,  $F_5$ ,  $F_5^*$ ), AES, Dynamic S-BOX and PN Sequence Generator (LFSR).

# Acknowledgements

First of all, I am grateful to the Almighty **ALLAH** for establishing me to complete this thesis.

I would like to express my sincere gratitude to **Prof. Dr. Abdelhalim Zekry** for his guidance and professional advice. His constant encouragement, valuable comments and suggestions made this thesis successful. I thank him for advising me to publish my paper at the conference (CyberSec2014) that will be held at the Faculty of Engineering-Lebanese University.

I would like to thank and appreciate **Prof. Dr. Talaat Abdellatief Elgarf** for his support, guidance, advices, suggestions, and for his unlimited assistance and helpful comments during preparing this thesis.

I am deeply and forever indebted to my parents for their love, support and encouragement throughout my entire life. I am also very grateful to my brother Yehia Zakaria and my sister Nesreen Zakaria. I would like to acknowledge my best friend Mohammed Soliman for providing me his valuable insights on practical implementation.

# Table of Contents

|                                                                                      |            |
|--------------------------------------------------------------------------------------|------------|
| <b>ABSTRACT.....</b>                                                                 | <b>I</b>   |
| <b>ACKNOWLEDGEMENTS.....</b>                                                         | <b>II</b>  |
| <b>TABLE OF CONTENTS.....</b>                                                        | <b>III</b> |
| <b>LIST OF FIGURES.....</b>                                                          | <b>VI</b>  |
| <b>LIST OF TABLES.....</b>                                                           | <b>IX</b>  |
| <b>LIST OF ABBREVIATIONS.....</b>                                                    | <b>X</b>   |
| <b>LIST OF SYMBOLS.....</b>                                                          | <b>XV</b>  |
| <b>LIST OF VARIABLES.....</b>                                                        | <b>XVI</b> |
| <b>Chapter 1 Introduction.....</b>                                                   | <b>1</b>   |
| <b>1.1 Authentication in Mobile Communication Systems.....</b>                       | <b>1</b>   |
| <b>1.2 Thesis Objectives.....</b>                                                    | <b>1</b>   |
| <b>1.3 Thesis Organization.....</b>                                                  | <b>2</b>   |
| <b>1.4 publications.....</b>                                                         | <b>2</b>   |
| <b>Chapter 2 Authentication Schemes in Mobile Communication<br/>    Systems.....</b> | <b>3</b>   |
| <b>2.1 Introduction.....</b>                                                         | <b>3</b>   |
| <b>2.2 Security Architecture of the GSM/GPRS.....</b>                                | <b>3</b>   |
| 2.2.1 Subscriber identity (IMSI) confidentiality.....                                | 4          |
| 2.2.2 Subscriber identity authentication.....                                        | 4          |
| 2.2.3 User data confidentiality on physical connections.....                         | 4          |
| 2.2.4 Connectionless user data confidentiality.....                                  | 5          |
| 2.2.5 Signaling information element confidentiality.....                             | 5          |
| <b>2.3 Security Architecture of the UMTS/LTE/Advanced-LTE.....</b>                   | <b>6</b>   |
| 2.3.1 Network access security (NAS).....                                             | 8          |
| 2.3.2 Network Domain Security (NDS).....                                             | 11         |
| 2.3.3 User domain security (UDS).....                                                | 11         |
| 2.3.4 Application Domain Security (ADS).....                                         | 12         |
| 2.3.5 Security visibility and configurability.....                                   | 13         |
| <b>2.4 Security Enhancements.....</b>                                                | <b>14</b>  |
| 2.4.1 Security Enhancements in UMTS Standard.....                                    | 14         |

|                                                                                                                                           |           |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 2.4.2 Security Enhancements in LTE/Advanced LTE Standard.....                                                                             | 15        |
| <b>2.5 Network Architecture in Mobile Communication Systems.....</b>                                                                      | <b>16</b> |
| 2.5.1 Common GSM/GPRS/UMTS Network Architecture.....                                                                                      | 16        |
| 2.5.1.1 GSM Network Architecture.....                                                                                                     | 16        |
| 2.5.1.2 GPRS Network Architecture.....                                                                                                    | 18        |
| 2.5.1.3 UMTS Network Architecture.....                                                                                                    | 19        |
| 2.5.2 LTE/SAE and Advanced LTE/SAE Network Architecture.....                                                                              | 20        |
| <b>2.6 Authentication Schemes in Global System for Mobile Communication (GSM) / General Packet Radio Service (GPRS).....</b>              | <b>23</b> |
| 2.6.1 (GSM/ GPRS) Generation of Authentication vectors (Triplet codes) by the HLR/AUC.....                                                | 25        |
| 2.6.2 GSM/ GPRS Computation of an Authentication Vector (Authentication Triplet codes) in user Subscriber Identity Module (SIM card)..... | 26        |
| <b>2.7 Authentication Schemes in Universal Mobile Telecommunications System (UMTS).....</b>                                               | <b>26</b> |
| 2.7.1 UMTS Generation of Authentication vectors (Quintets) by the HLR/AuC.....                                                            | 28        |
| 2.7.2 UMTS Authentication and key derivation in the Universal Subscriber Identity Module (USIM).....                                      | 30        |
| <b>2.8 Authentication Schemes in Long Term Evolution (LTE) /Advanced LTE.....</b>                                                         | <b>31</b> |
| 2.8.1 Generation of EPS Authentication vectors by the HSS/AuC.....                                                                        | 33        |
| 2.8.2 EPS Authentication and key derivation in the Universal Subscriber Identity Module (USIM) and Mobile Equipment (ME).....             | 35        |
| <b>Chapter 3 AES-128 and MILENAGE algorithms.....</b>                                                                                     | <b>38</b> |
| <b>3.1 Introduction.....</b>                                                                                                              | <b>38</b> |
| <b>3.2 Rijndael (AES-128) algorithm.....</b>                                                                                              | <b>38</b> |
| <b>3.3 Encryption operations in AES-128 Algorithm.....</b>                                                                                | <b>40</b> |
| 3.3.1 an initial Round Key addition.....                                                                                                  | 40        |
| 3.3.2 Byte Substitution transformation .....                                                                                              | 41        |
| 3.3.3 Shift Rows transformation.....                                                                                                      | 43        |
| 3.3.4 Mix-Column transformation.....                                                                                                      | 43        |
| 3.3.5 Round Key Addition.....                                                                                                             | 45        |
| 3.3.6 AES Key Expansion Algorithm (Schedule Key).....                                                                                     | 46        |
| 3.3.7 A final round operation.....                                                                                                        | 49        |
| <b>3.4 MILENAGE Algorithm.....</b>                                                                                                        | <b>50</b> |
| 3.4.1 Computation of the MILENAGE Algorithm.....                                                                                          | 51        |

|                                                                                                |            |
|------------------------------------------------------------------------------------------------|------------|
| 3.4.2 Computation of MILENAGE-3G/4G Algorithms.....                                            | 52         |
| 3.4.3 Computation of MILENAGE-2G Algorithms.....                                               | 54         |
| <b>Chapter 4 Modifying Authentication Techniques in Mobile<br/>Communication Systems.....</b>  | <b>56</b>  |
| 4.1 Introduction.....                                                                          | 56         |
| 4.2 Proposed of MILENAGE Algorithm.....                                                        | 56         |
| 4.3 Upgrade of S-box (Dynamic change of S-box) using PN<br>sequence generator.....             | 57         |
| <b>Chapter 5 Simulation and Results.....</b>                                                   | <b>61</b>  |
| 5.1 Introduction.....                                                                          | 61         |
| 5.2 AES standard-128.....                                                                      | 61         |
| 5.3 Modified AES -128.....                                                                     | 62         |
| 5.4 Avalanche test in AES standard - 128.....                                                  | 64         |
| 5.5 Avalanche test in Modified AES-128.....                                                    | 67         |
| 5.6 Derivation of Authentication Vector (AV) in 3GPP<br>MILENAGE Algorithm Standard.....       | 70         |
| 5.7 Derivation of a stronger Authentication Vector (AV) in<br>Modified MILENAGE Algorithm..... | 71         |
| <b>Chapter 6 Conclusions and Future Work.....</b>                                              | <b>81</b>  |
| 6.1 Conclusions.....                                                                           | 81         |
| 6.2 Future Work.....                                                                           | 82         |
| <b>APPENDIX A.....</b>                                                                         | <b>83</b>  |
| <b>APPENDIX B.....</b>                                                                         | <b>87</b>  |
| <b>APPENDIX C.....</b>                                                                         | <b>93</b>  |
| <b>APPENDIX D.....</b>                                                                         | <b>99</b>  |
| <b>References.....</b>                                                                         | <b>106</b> |

## List of Figures

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Figure 2.1: security architecture of both UMTS/LTE and Advanced-LTE.....         | 8  |
| Figure 2.2: Evolving NAS in mobile communication systems.....                    | 11 |
| Figure 2.3: Common GSM/GPRS/UMTS Network.....                                    | 19 |
| Figure 2.4: EPC Architecture.....                                                | 22 |
| Figure 2.5: E-UTRAN Architecture.....                                            | 22 |
| Figure 2.6: Authentication schemes in GSM /GPRS.....                             | 24 |
| Figure 2.7: Generation of Authentication Vectors (Triplet codes) in the AuC..... | 25 |
| Figure 2.8: GSM/GPRS Authentication and key derivation in the SIM-Card.....      | 26 |
| Figure 2.9: Authentication Schemes in UMTS.....                                  | 28 |
| Figure 2.10: Generation of UMTS Authentication Vectors in the AuC.....           | 30 |
| Figure 2.11: UMTS Authentication and key derivation in the USIM.....             | 31 |
| Figure 2.12: Authentication Schemes in LTE/Advanced LTE.....                     | 32 |
| Figure 2.13: Computation of local master key $K_{ASME}$ .....                    | 34 |
| Figure 2.14: Generation of EPS Authentication Vectors in the HSS.....            | 34 |
| Figure 2.15: Successful EPS AKA authentication.....                              | 35 |
| Figure 2.16: EPS Authentication and key derivation in the USIM and ME.....       | 37 |
| Figure 3.1: Overall structure of the AES-128 algorithm.....                      | 40 |

|                                                                                                                               |           |
|-------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Figure 3.2: Structure of the Sub-Bytes.....</b>                                                                            | <b>41</b> |
| <b>Figure 3.3: Example of the Sub-Bytes transformation.....</b>                                                               | <b>42</b> |
| <b>Figure 3.4: Structure of the Shift Rows.....</b>                                                                           | <b>43</b> |
| <b>Figure 3.5: Example of the Shift Rows s transformation.....</b>                                                            | <b>43</b> |
| <b>Figure 3.6: Structure of the Mix-column.....</b>                                                                           | <b>44</b> |
| <b>Figure 3.7 Example of the Mix- Columns transformation.....</b>                                                             | <b>45</b> |
| <b>Figure 3.8 Structure of the Add Round Key.....</b>                                                                         | <b>45</b> |
| <b>Figure 3.9 Example of the Add Round Key transformation.....</b>                                                            | <b>45</b> |
| <b>Figure 3.10: AES Key Expansion.....</b>                                                                                    | <b>46</b> |
| <b>Figure 3.11: Rotated the last Row.....</b>                                                                                 | <b>47</b> |
| <b>Figure 3.12: Sub-byte the Row by using S-box Look up Table.....</b>                                                        | <b>47</b> |
| <b>Figure 3.13: Look Up Table of the Rcon.....</b>                                                                            | <b>48</b> |
| <b>Figure 3.14: Operation XOR between first Row of Key and last Row<br/>after the Modification and First Row of Rcon.....</b> | <b>48</b> |
| <b>Figure 3.15: XOR-ing between Modified Row and Second Row of<br/>Master Key.....</b>                                        | <b>48</b> |
| <b>Figure 3.16: Example of AES-128 Key Expansion.....</b>                                                                     | <b>48</b> |
| <b>Figure 3.17: AES encryption round.....</b>                                                                                 | <b>49</b> |
| <b>Figure 3.18: Computation of the MILENAGE Algorithm functions.....</b>                                                      | <b>54</b> |
| <b>Figure 4.1: Modification of MILENAGE Algorithm.....</b>                                                                    | <b>57</b> |
| <b>Figure 4.2: PN random sequence generator.....</b>                                                                          | <b>58</b> |
| <b>Figure 5.1: Avalanche effects of AES standard due to change one<br/>bit in plaintext.....</b>                              | <b>65</b> |

**Figure 5.2 Avalanche effects of AES standard due to change one  
bit in Secret Key.....66**

**Figure 5.3: Avalanche effects of Modified AES due to change one  
bit in Plain-Text.....68**

**Figure 5.4: Avalanche effects of Modified AES due to change one  
bit Secret Key.....69**

## List of Tables

|                                                                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Table 3.1: AES S-Boxes.....                                                                                                                                                  | 42 |
| Table 3.2: The values of RC[j] in hexadecimal.....                                                                                                                           | 47 |
| Table 4.1: AES standard S-BOX.....                                                                                                                                           | 58 |
| Table 4.2: For COLUMNS Dynamic S-box after arrangement<br>= [09AE48DBC37F5612].....                                                                                          | 59 |
| Table 4.3: Final Dynamic S-box ROWs after arrangement<br>= [B9DE60C327458F1A].....                                                                                           | 60 |
| Table 5.1: AES Standard - 128.....                                                                                                                                           | 61 |
| Table 5.2: Modified AES (Dynamic S-box) - 128.....                                                                                                                           | 63 |
| Table 5.3: Samples results of Cipher text and Avalanche test due to<br>change one bit in plain text in standard AES-128.....                                                 | 64 |
| Table 5.4 Samples results of Cipher text and Avalanche test due to<br>change one bit in secret key of AES -128 standard.....                                                 | 65 |
| Table 5.5: Samples results of Cipher text and Avalanche test due to<br>change one bit in plain text of Modified AES-128.....                                                 | 67 |
| Table 5.6: Samples results of Cipher text and Avalanche test due to<br>change one bit in Secret Key of Modified AES-128.....                                                 | 68 |
| Table 5.7 Result Outputs of Test Set in 3GPP Milenage Algorithm<br>standard to derivation Authentication Vector.....                                                         | 70 |
| Table 5.8: Result Outputs of Modified MILENAGE Algorithm to derive<br>a stronger Authentication Vector (AV) than outputs of<br>standard Milenage Algorithm (AV) in 3GPP..... | 72 |
| Table 6.1: Average value of avalanche tests for (plain text - secret key)<br>in AES-128 and Modified AES-128.....                                                            | 81 |

# List of Abbreviations

|      |                                         |
|------|-----------------------------------------|
| 2G   | Second Generation                       |
| 3G   | Third Generation                        |
| 4G   | Fourth Generation                       |
| 3GPP | Third Generation Partnership Project    |
| A3   | GSM authentication function             |
| A8   | GSM key generation function             |
| AES  | Advanced Encryption Standard            |
| ADS  | Application Domain Security             |
| AF   | Authentication Framework                |
| AK   | Anonymity Key                           |
| AKA  | Authentication and Key Agreement        |
| AMF  | Authentication and key Management Field |
| AN   | Access Network                          |
| ASME | Access Security Management Entity       |
| AuC  | Authentication Centre                   |
| AUTN | Authentication Token                    |
| AV   | Authentication Vector                   |
| BSC  | Base Station Controller                 |
| BSS  | Base Station Subsystem                  |

|         |                                                    |
|---------|----------------------------------------------------|
| BTS     | Base Transceiver Station                           |
| CK      | Cipher (Confidentiality) Key in 3G/4G              |
| CN      | Core Network                                       |
| CS      | Circuit Switched                                   |
| CCU     | Channel Codec Unit                                 |
| DES     | Data Encryption Standard                           |
| EIR     | Equipment Identity Register                        |
| EPS     | Evolved Packet System                              |
| EPS-AV  | EPS authentication vector                          |
| ETSI    | European Telecommunications Institute              |
| E-UTRAN | Evolved Universal Terrestrial Radio Access Network |
| FIPS    | Federal Information Processing Standard            |
| FFC     | Forward Error Correction                           |
| GPRS    | General Packet Radio Service                       |
| GSM     | Global System for Mobile Communications            |
| HE      | Home Environment                                   |
| HLR     | Home Location Register                             |
| HSS     | Home Subscriber Server                             |
| HON     | Handover Number                                    |
| ICC     | Integrated Circuit Card                            |
| IP      | Internet Protocol                                  |