
**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 COMMITEE

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

**Date of Degree** **:** August 2009

# Abstract

MILENAGE Algorithm applies the block cipher Rijnadael (AES) with 128 bit key and 128 bit block size. This algorithm is used in the 3GPP authentication and key generation functions (f1, f1*, f2, f3, f4, f5 and f5*) 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 (F1, F1*, F2, F3, F4, F5, F5*), 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

# List of Figures

# List of Tables

# 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 |