بسم الله الرحمن الرحيم

MONA MAGHRABY

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

MONA MAGHRABY

شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

MONA MAGHRABY

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics Engineering and Electrical Communications

An Enhanced Implementation of Elliptic Curve Digital Signature Algorithm

A Thesis submitted in partial fulfilment of the requirements of the degree of

Master of Science in Electrical Engineering

Electronics Department and Electrical Communications

By

Ahmed Mohamed Samir Abo-Taleb

Bachelor of Science in Electrical Engineering

(Electronics Engineering and Electrical Communications)

Faculty of Engineering, Alexandria University, 2009

Supervised By

Prof. Salwa Hussein El Ramly

DR. Mohamed Mahmoud Youssef Shalaby

DR. Mohamed Nabil Mohamed Hassan

Cairo – (2020)

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics Department and Electrical Communications

An Enhanced Implementation of Elliptic Curve Digital Signature Algorithm

By

Ahmed Mohamed Samir Abo-Taleb

Bachelor of Science in Electrical Engineering

(Electronics Engineering and Electrical Communications)

Faculty of Engineering, Alexandria University, 2009

Examiners' Committee

Name and Affiliation	**Signature**
Associate Prof. / Hussein Abdel Atty Elsayed Ain Shams University Electronics and Communications Eng. Dept.	.....
Prof. Dr. Heba Kamal Aslan Electronic Research Institute (ERI)	.....
Prof. Dr. Salwa Hussein El-Ramly Ain Shams University Electronics and Communications Eng. Dept.	.....

Date: 22 / 04 / 2020

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics Department and Electrical Communications

An Enhanced Implementation of Elliptic Curve Digital Signature Algorithm

Submitted By: Ahmed Mohamed Samir Abo-Taleb
Degree: Master of Science in Electronics and Communication Engineering.

Supervisory Committee

Name and Affiliation	**Signature**
Prof. Dr. Salwa Hussein El-Ramly Ain Shams University Electronics and Communications Eng. Dept.	.....
DR. Mohamed Mahmoud Youssef Shalaby Air Defense Research and Dev. Center	.....
DR. Mohamed Nabil Mohamed Hassan Armed Forces Research and Dev. Center	.....

Statement

This thesis is submitted as a partial fulfilment of Master of Science in Electrical Engineering Engineering, Faculty of Engineering, Ain shams University.
The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Ahmed Mohamed Samir Abo-Taleb
Signature
……..……...…….

Date: 22 04 2020

Researcher Data

Name: Ahmed Mohamed Samir Abo-Taleb.

Date of birth: 16/ 02 / 1988.

Place of birth: Cairo.

Last academic degree: Bachelor of Science in Electrical Engineering

Field of specialization: Electronics Engineering and Electrical Communications

University issued the degree: Alexandria University.

Date of issued degree: July 2009.

Current job: Researcher in Air Defense R&D Center.

Faculty of Engineering-Ain Shams University

Electronics and Communication Engineering

Department

Thesis title "**An Enhanced Implementation of Elliptic Curve Digital Signature Algorithm**"

Submitted by: **Ahmed Mohamed Samir Abo-Taleb**

Degree: **Master of Science in Electrical Engineering**

SUMMARY

In the current modern era, there are a lot of activities that require the presence of human beings, are replaced with a digital data which represent him/her at anytime and anywhere. This digital information is called "Digital Signature". Digital signatures are very useful for signing important documents, confirming decisions and even banking transactions. The digital world is facilitating our life by making us able to accomplish difficult tasks which is quite a distance from us using such techniques. But there is some trouble we are being faced which is "Security Breach". This can be done through performing malicious activity against any two parties who are communicating with each other across a certain communication link. The old fashion of attacks against cryptographic scheme is performing a brute force attack until the attacker successfully gets the private key which is associated with a public key. This kind of attack takes more time to break the security, but the problem is that, the attackers have developed new types of attack which are indirect

and more efficient called “Side-Channel Attacks”, in which the attacking time is reduced to be some minutes.

Chapter 1: contains a thesis introduction, as well as a literature review.

Chapter 2: discusses cryptography background, types of cryptographic schemes, finite fields, Side-Channel Attacks, and NIST statistical tests.

Chapter 3: discusses types of Side-Channel Attacks, Cache-Based Side-Channel Attacks, proposed hashing method that can counteract last-level cache memory side-channel attack.

Chapter 4: Digital Signature Background, Recommended Elliptic Curve Domain Parameters, proposed random private-key construction model, and proposed generation model of the public key.

Chapter 5: experimental results, measurement tools, and software.

Chapter 6: contains conclusions and recommendations for future work.

Faculty of Engineering-Ain Shams University

Electronics and Communication Engineering

Department

Thesis title "**An Enhanced Implementation of Elliptic Curve Digital Signature Algorithm**"

Submitted by: **Ahmed Mohamed Samir**

Degree: **Master of Science in Electrical Engineering**

Abstract

This thesis presents a resistive implementation of elliptic curve digital signature algorithm against last level cache memory side channel attack which contains the following 3 models to fulfill a satisfied tradeoff between security and processing time as well:

1. Secured hashing model: using the standard version of KECCAK hashing algorithm which is recommended by NIST and implemented in a way similar to secured password hashing technique which is also recommended by NIST in 2015.
2. Generic random private key generation model: to generate variable length of private key which is created randomly from other random processes (Random of Random).
3. Secured Public Key generation model: based on random truth table generation for PK bit sequence in order to perform scalar multiplication differently to reduce the possibility of a successful attack.

For implementation, we made a comparison between two different programming languages which are Python3.0 and C#.Net in order to choose a suitable one to

work with. The security requirements in the implementation relies on two different techniques:

1. Confusion.
2. Eviction.

The previous techniques are accomplished using the following:

1. A shuffling algorithm (Fisher-Yates Algorithm).
2. Volatile memory objects to hold critical data and to prevent it from existing in SRAM much longer.
3. Thread locking techniques to protect the volatile objects from being accessed by any malicious thread.

Key words: Sponge Construction; KECCAK; Password hashing; Side Channel; Elliptic Curve Cryptography; Digital Signatures;

Acknowledgment

Ahmed Mohamed Samir Abo-Taleb.

Faculty of Engineering.

Electronics and Communication Engineering Department.

Ain Shams University.

Cairo, Egypt.

22 / 04 / 2020

First of all, thanks to ALLAH for everything in my life.

Then, my grateful thanks and my gratitude to my Dr. Salwa Hussein El-Ramly, Professor of Communications, Faculty of Engineering, Ain shams University on the fruitful effort in supervising this work and on follow-up, guidance and provide me with fruitful advice and also on the ongoing support and revision of ideas during the research period.

I would like to express my highest gratitude to Dr. Mohamed Mahmoud Youssef Shalaby, for making this experience possible and for all the lessons learned from him, valuable comments and suggestions made this thesis very successful.

I would like to express my thanks and appreciation to Dr. Mohamed Nabil Mohamed Hassan encouragement, and advice to me during the period of supervision and preparation of the scientific thesis for this work.

At the end, I would like to thank my family specially “my parents” to support me with all the effort to finish this work.

April 2020

List of Publications

- A. S. Abo-Taleb, M. Nabil, M. Shalaby, and S. Elramly, “An Enhanced SHA3-based Hashing Method: A Side-channel Attack Countermeasure,” in Proceedings of the 8th International Conference on Software and Information Engineering, Cairo, 2019 Index of Ei Compandex and Scopus, pp. 145–150. https://doi.org/10.1145/3328833.3328879

- A. S. Abo-Taleb, M. Shalaby, M. Nabil, and S. Elramly, “A Side-Channel Attack Resistive ECDSA,” in International Conference on Advanced Information Systems and Engineering, Cairo, 2019. Indexed by: Conference Proceedings Citation Index – Science (CPCI-S) (Thomson Reuters, Web of Science), Scopus, Ei Compendex, Inspec(IET), “A Side-Channel Attack Resistive ECDSA”, Journal of Physics. doi:10.1088/1742-6596/1454/1/012003

Table of Contents