Ain Shams University

Faculty of Engineering

Engineering Physics and Mathematics Department

Applications of Error Detection as a Fault Tolerance Mechanism for Cryptographic Algorithms

By

Naglaa Fawzy Abd El-Fatah Saudy

M.Sc. Engineering Mathematics, Cairo University, 2008

A Thesis Submitted in Partial Fulfillment of the Requirement for the Degree of

Doctor of Philosophy in Engineering Mathematics

Supervised by

Prof. Dr. / Reda Amin Elbarkoky

Faculty of Engineering, Ain Shams University

Prof. Dr. / Ihab Ali

Faculty of Engineering, Helwan University

Cairo 2019

Ain Shams University

Faculty of Engineering

Department of Engineering Physics and Mathematics

Applications of Error Detection as a Fault Tolerance Mechanism for Cryptographic Algorithms

A Thesis submitted in the Partial Fulfillment for the Requirement of the Degree of Doctor of Philosophy of Engineering Mathematics

By

Naglaa Fawzy Abd El-Fatah Saudy

M.Sc. Engineering Mathematics, Cairo University, 2008

Examiners Committee

Title, Name & Affiliation	Signature
Prof. Dr. / **Aly Nasr Elwakeil** Faculty of Engineering, Banha University	……..
Prof. Dr. / **Ayman Mohammad Bahaa Eldin** Faculty of Engineering, Ain Shams University	……..
Prof. Dr. / **Reda Amin Elbarkoky** Faculty of Engineering, Ain Shams University	……..
Prof. Dr. / **Ihab AbdelWahab AbdelGawad** Faculty of Engineering, Helwan University	……..

Date: / / ٢٠١9

STATEMENT

This thesis is submitted as partial fulfillment of Ph.D. degree in Engineering Mathematics, 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 qualification at any other scientific entity.

Naglaa Fawzy Abd El-Fatah Saudy

ACKNOWLEDGEMENT

First of all, thanks and indebtedness are due to **ALLAH** who made this work possible.

I would like to express my deep thanks and gratitude to Prof. Dr. / Reda Amin Elbarkoky, Professor of Engineering Mathematics, Faculty of Engineering, Ain-Shams University, for his supervision, continuous useful discussion, encouragement and motivation.

I would like to express my deep thanks and gratitude to Prof. Dr. / Ihab Ali, Communication department Faculty of Engineering Helwan University, not only for suggesting the subject of this research work, but also for his close supervision, valuable guidance, help, encouragement, and kind criticism.

I owe great thanks and sincere love to my family who supported me during difficult and hard times.

Naglaa Fawzy Abd El-Fatah Saudy

Table of Contents

List of Figures

Chapter 4: Error Analysis and Detection Procedures for Elliptic Curve Cryptographic Algorithm

Chapter 5: Error Analysis and Detection Procedures for Elliptic Curve Digital Signature Algorithm

ABBREVIATIONS

ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
GQ	Guillou-Quisquater
DES	Data Encryption Standard
AES	Advanced Encryption Standard
GF	Galois Fields
RSA	Rivest, Shamir, Adleman
DSA	Digital Signatures Algorithms
ECDLP	Elliptic Curve Discrete Logarithm Problem
DFA	Differential Fault Attack
RAM	Random Access Memory
EDC	Error Detection /Correction
TMR	Trust Management Root
ABFT	Algorithm Based Fault Tolerant Cryptography
LD	Lopez Dahab
CRT	Chinese Remainder Theorem
MLE	Montgomery Ladder Exponentiation
CED	Concurrent Error Detection
SPA	Simple Power Analysis
DPA	Differential Power Analysis
BSA	Borrow Save Adders
RNG	Random Number Generator
FS	Fiat and Shamir

Thesis Summary

Traditional mathematical cryptanalysis uncovers weakness in cryptographic algorithms. A small amount of side-channel information is sufficient to compromise common cryptographic algorithms. We added new modifications to some cryptographic techniques to improve their security and reliability in realistic environment

In this study, we introduced security improvement to various cryptography methods to protect cryptography against fault attack.

In case study 1, we presented applying nonlinear fault discovery codes to defend elliptic curve point addition and doubling processes in contradiction to fault attacks for non-supersingular, supersingular, and Lopez-Dahab These ciphers provide practically perfect fault discovery capacity (beside from an exponentially small probability) at reasonable overhead. We presented error discovery structure by utilizing a fault discovery cipher. This error discovery structure has appeared to have over 99% error discovery coverage.

In case study 2, we presented applying nonlinear fault discovery codes to defend protect ECDSA operations contrary to error assaults.

In case study 3, we also presented applying the same methodology to defend Guillou-Quisquater authentication structure (GQ) contrary to error injection assaults.

In case study 4, we introduced a modification on supersingular isogeny cryptosystems operations by applying nonlinear error discovery ciphers to defend supersingular isogeny cryptosystems processes contrary to error assaults.

Key Words: Cryptography, Fault Attack, and Elliptic Curve Cryptography.

CHAPTER ONE
INTRODUCTION

1.1 Problem Statement

With the emergence of new applications and the increased reliance on networks to offer new services, the need for improved security paradigms in an emerging market is being pushed to the forefront. Recently, because of the large fatalities from prohibited information get to, information security has turned into an essential topic for public, private and protection associations. So as to shield important information or data from illicit access, illegal changes, and reproduction, several types of cryptographic strategies are being utilized. Broad and diverse field of mathematics, including number theory, abstract algebra, (groups, rings, fields), probability, optimization, and information theory are utilized in the specialty of cryptography. Despite all the technological advances in security for modern communications and commerce, the cornerstone of our digital age still depends on the current incarnation of the early art of codes and ciphers as its first line of defense. The inception of current cryptography contains a great agreement of attractive mathematics, some of which have been adapted for cryptographic uses, yet a lot of which is in use exactly as from the classical mathematical rule.

1.2 Thesis Objectives

Traditional mathematical cryptanalysis uncovers the weakness in cryptographic algorithms. Typical side channels contain time expended by the operators utilized in the execution power dispersed by the execution, radiation exuding from the device, and the faulty outcome yielded by the usage. A little measure of side-channel data is enough to

operating basic cryptographic procedures. We will add new modifications to some cryptographic techniques to improve their security and reliability of them in realistic environments.

1.3 Thesis Contributions

In this thesis, a fault detection scheme is introduced with the ability to perform with increased protection and reliability of the Elliptic Curve Cryptography (ECC) in realistic environments at a competitive price point. The ECC functions in actual networks, which, by definition, all contain their particular sets of temporary errors. Thus, having the capacity to deal with errors that occur during the ECC performance analysis has become a must. Fall of errors in encrypted/decrypted data delivery with the transmission can create the situation of erroneous data occurring. In addition, without fault detection, in the context of encryption as well as decryption process can create the unprotected system due to random faults, and this system is vulnerable to attack from anyone who wishes to unscrupulously insert faults as a strategy to uncover the secret key.

We are striving to overcome these system weaknesses by introducing the application of nonlinear fault detection codes as it allows safeguarding the elliptic curve point while adding and doubling the operations from the fault attacks. The fundamental thought of the non-linear error detection allows making two calculation paths that remains non-linear to each other. The use of these codes ensures almost perfect error discovery capacity (with the exception of an exponentially small probability) with a reasonably priced upfront cost. Applying fault detection to ECC Public key cryptosystem offered a failsafe fault detection scheme using an error detecting code with a proven rate of 99% fault detection coverage.

In this thesis, we present the first fault detection construction to expand the defense and dependability of the Elliptic Curve Digital Signature Algorithm (ECDSA) under applied concerns. As the ECDSA will work in physical schemes, which have their particular procedure of temporary errors, having the capacity to deal with faults that occur while observing the ECDSA implementation transforms into an unquestionable necessity.

We introduce applying nonlinear fault detection codes to defend Guillou-Quisquater authentication structure (GQ) in contradiction of fault infusion attacks. These codes provide practically perfect fault discoverability (aside from an exponentially small probability) at reasonable overhead. We introduce error discovery scheme by utilizing the nonlinear fault discovery code. This error discovery structure has appeared to have over 99% error discovery coverage.

We introduce a modification on supersingular isogeny cryptosystems operations to protect against fault attacks by applying nonlinear fault detection codes. This will be achieved by calculating the image of a point under the secret isogeny utilizing the systematic non-linear (n, k, r)-code which utilizes redundancy for error detection. Non-linear error detection works by creating two calculation paths that are non-linear in alignment. The initial step in accomplishing this includes encrypting the supersingular isogeny in an operation by utilizing the nonlinear code. The first non-linear path is the original non redundant datapath. The second path, which is known as the ‘predictor' piece, goes in parallel to the non-redundant path and basically guesses the checksum of the consequences of the first calculation. These codes give almost perfect error detection capacity at a sensible overhead.

1.4 Thesis Outlines

The rest of the thesis is prepared as follows. **Chapter 2:** outlines the basic definitions and formulations. In addition, it provides an introduction to the mathematical ideas underlying that theory of cryptography.

Chapter 3: reviews the literature review on ECC Algorithm and Study different techniques of Side channel attacks, Countermeasures against these attacks for different cryptography methods, and explains the robust nonlinear residue codes techniques used in this thesis.

Chapter 4: presents designs and implements of an efficient nonlinear error detection as a Fault Tolerance Mechanism for ECC Algorithms.

Chapter 5: introduces a nonlinear fault detection scheme to improve the security and dependability of Elliptic Curve Digital Signature Algorithm (ECDSA).

Chapter 6: introduces a nonlinear fault detection scheme to improve the security and reliability of Guillou-Quisquater authentication scheme (GQ).

Chapter 7: introduces a modification on supersingular isogeny cryptosystems operations to protect against fault attacks by applying nonlinear fault detection codes.

Chapter 8: summarizes the conclusion and gives future work recommendations.

CHAPTER TWO

A REVIEW OF MATHEMATICAL CRYPTOGRAPHY

This chapter introduces the mathematical concepts essential to the theory of cryptography. Broad and diverse field of mathematics, containing number theory, abstract algebra, (groups, rings, fields), probability, optimization, elliptic curve, isogeny, and information theory are utilized in the specialty of cryptography. Each required mathematical topic will be introduced in the necessary depth to prove its relevance [1, 2].

2.1 Cryptography

Despite all the technological advances in security for modern communications and commerce, the cornerstone of our digital age still depends on the current manifestation of the early art of codes and ciphers as its first line of defense. The inception of modern cryptography contains a lot of attractive mathematics, some of which have been adopted for cryptographic uses, yet a lot of which is in use exactly as from the classical mathematical rule [3, 4].

For a large number of years, all codes and ciphers depended on the supposition that two individuals are trying to interconnect. Let's assume them to be Bob and Alice, use a secret key that their enemy, Eve, doesn't own. If Bob employs the undisclosed key to encode their correspondence, then Alice must utilize the same key to decode their messages. Thus it has become impossible for Eve or anyone not privy to the secret key, to decrypt the private correspondence. However, there is a drawback; Bob