



AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics and Communications Engineering Department

Building Smart Multipurpose Electronic Voting System

A THESIS

Submitted in partial fulfillment for the requirements
of Doctor of Philosophy Degree in Electrical Engineering

Submitted by

Enas Mohamed Mahmoud Elbarbary

M.Sc. of Electrical Engineering

(Electronics & Communications Engineering)

Ain Shams University - 2010

Supervised by

Prof. Dr. Abd El-Halim Abd-Elnabi Zekry

Faculty of Engineering

Ain Shams University

Assoc. Prof. Hussam M. Elbehery

Faculty of Information Systems and Computer Science

October 6 University

Ass. Prof. Ghada Abdelmouez M. Abdelhady

Faculty of Information Systems and Computer Science

October 6 University

Cairo - 2016



AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING

Electronics and Communications Engineering Department

Name : Enas Mohamed Mahmoud Elbarbary

Thesis : BUILDING SMART MULTIPURPOSE ELECTRONIC VOTING SYSTEM

Degree : Doctor of Philosophy in Electrical Engineering

EXAMINERS COMMITTEE

Name, Title, and Affiliation

Signature

(Examiner)

1. Prof. Dr. Talaat Abd El-Latif Elgarf

Professor in Electrical Engineering Department
10th of Ramadan Engineering Faculty

(Examiner)

2. Prof. Dr. Hoda Korashy Mohamed Ismail

Professor in Computers and Systems Engineering Department
Faculty of Engineering
Ain Shams University, Cairo

(Supervisor)

3. Prof. Dr. Abd El-Halim Abd-Elnabi Zekry

Professor in Electronics and Communications Engineering Department
Faculty of Engineering
Ain Shams University, Cairo

Date 28/4/2016

FOR MY PARENTS

*As fulfillment, favor appreciation: I would like to warmly thank **my mother** for her great support, continuous encouragement to achieve my best to finalize this research.*

*I would like to warmly thank **my father** for his great support, continuous encouragement to achieve my best to finalize this research.*

Also, without their continuous pray along the research period, this work may not be completed. Words could not express my deepest feeling to thank them.

*May **GOD** give them the best penalty to reach the highest degree in Heaven.*

Enas Elbarbary

STATEMENT

This dissertation is submitted to Ain Shams University for the Degree of Doctor of Philosophy in Electrical Engineering, Electronics and Communications Engineering.

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

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

Name : Enas Mohamed Mahmoud Elbarbary

Signature :

Date : / / 2016

ACKNOWLEDGEMENT

*The first and foremost thanks are due to **God**, the most beneficent and merciful.*

*I would like to express my sincere thanks and gratitude, deepest feeling to **Prof. Dr. Abd El-Halim Zekry**, Professor at Electronics & Communications Engineering Department, Faculty of Engineering, Ain Shams University for his sympathetic kind help, essential and valuable supervision and criticism backed by his vast experience, and strong support.*

*I would like to express my sincere thanks and gratitude to **Assoc. Prof. Hussam Elbehier**, Head of Computer Science Department, Faculty of Information Systems and Computer Science, October 6 University for his essential supervision, valuable criticism, and strong support.*

*I owe special thanks and sincere gratitude to **Ass. Prof. Ghada Abdelhady**, Computer Science Department, Faculty of Information Systems and Computer Science, October 6 University for her supervision, and strong support.*

*Finally, honorable mention goes to **my beloved family, and my close friends** for all their faith in me, the support, advice, and understanding they give me all the time.*

Enas Elbarbary

LIST OF CONTENTS

ACKNOWLEDGEMENT

LIST OF CONTENTS	I
LIST OF FIGURES	VI
LIST OF TABLES	X
LIST OF ABBREVIATIONS.....	XI
LIST OF SYMBOLS.....	XV
ABSTRACT.....	XVII

CHAPTER 1 Introduction

1.1 Voting History	1
1.1.1 Voting Systems	3
1.1.1.1 Paper Ballot Voting System.....	3
1.1.1.2 Electronic Voting System	5
1.1.1.3 Online Voting System.....	8
1.2 Recent Voting Systems	11
1.2.1 Estonian Internet Voting System	11
1.2.1.1 National ID Cards	13
1.2.1.2 I-Voting Server Infrastructure.....	13
1.2.2 Design and Build A Secure E-Voting Infrastructure	15
1.2.3 Cobra: Toward Concurrent Ballot Authorization for Internet Voting	18

1.2.4 Coercion-Resistant Electronic Elections with Write-In Candidates	19
1.3 Research Goals.....	22
1.4 Research Structure.....	24

CHAPTER 2 Cryptology

2.1 Introduction	27
2.2 Cryptology	27
2.2.1 Encryption Systems	32
2.2.1.1 Symmetric Encryption	32
2.2.1.2 Asymmetric Encryption	33
2.2.1.3 Symmetric versus Asymmetric Schemes	38
2.2.1.4 Asymmetric Schemes	41
2.3 Hashing	52
2.4 Digital Signatures	55
2.4.1 Security Services	55
2.4.2 Digital Signatures Principle and Applications	57
2.4.3 Digital Signatures Algorithms.....	60
2.5 Certificates	67
2.6 Cryptanalysis	70
2.6.1 Brute-Force Attack (Exhaustive Key Search).....	75
2.6.2 MITM Attack	77
2.6.3 Types of Attacks on Signature Schemes	79
2.6.3.1 Security Considerations	82

CHAPTER 3 Suggested Cryptographic Schemes (Encryption & Authentication)

3.1 Introduction	83
3.2 Elgamal Encryption Protocol	83
3.2.1 Elgamal Encryption Protocol Attacks.....	87
3.2.1.1 Secret Exponent Computation	87
3.2.1.2 Secret Exponent Reuse.....	88
3.3 Elgamal DS Protocol	89
3.3.1 Setup (Key Generation).....	89
3.3.2 Signature Generation.....	90
3.3.3 Signature Verification	91
3.3.4 Elgamal DS Protocol Attacks	91
3.3.4.1 Ephemeral Key Reuse.....	91
3.3.4.2 Existential Forgery Attack	93
3.4 Certificates Application for STCVS	94
3.5 SHA-1 Algorithm	96

CHAPTER 4 Security Systems Performance Measurements

4.1 Introduction	98
4.2 Data Masking (using LFSR)	98
4.2.1 Data Masking versus Encryption	99
4.2.2 Fibonacci LFSR	100
4.3 Avalanche Effect	103

CHAPTER 5 Secured Transparent Computerized Voting System (STCVS)

5.1 Introduction	106
5.2 STCVS Methodology	106
5.3 STCVS Analysis	109
5.3.1 STCVS Use Case Diagram	109
5.3.2 STCVS Sequence/Process Diagrams	111
5.3.3 STCVS Flow Chart	114
5.3.4 STCVS Database	117
5.3.5 STCVS Website	118
5.3.5.1 Voting Login	118
5.3.5.2 Supervision Login	128

CHAPTER 6 Experimental Work & Results Discussion and Analysis

6.1 Introduction	133
6.2 STCVS Performance Measurements	134
6.2.1 Plaintext Masking	134
6.2.2 Avalanche Effect Results	141
6.2.2.1 Input Data Tests	142
6.2.2.2 Public Key Tests	149
6.2.3 STCVS Digital Signatures	153
6.3 STCVS Constraints	154
6.4 STCVS Performance Analysis	154

6.5 Interfaces	155
6.5.1 Software Interface	155
6.5.2 Communication Interface.....	156

CHAPTER 7 Conclusion & Future Work Suggestions

7.1 Conclusion	157
7.2 Future Work Suggestions	162

REFERENCES	164
-------------------------	------------

Arabic Summary

LIST OF FIGURES

Figure 1.1	Paper Ballot Voting System	4
Figure 1.2	Electronic Voting System	6
Figure 1.3	(a) Punched Cards (b) Optical scan (c) DRE Voting Systems	7
Figure 1.4	Online Voting System	9
Figure 1.5	Estonian I-Voting System.....	12
Figure 1.6	Each Party Counts the Votes on each Server	17
Figure 1.7	How to Vote for a Write-in Candidate.....	20
Figure 2.1	Overview of the Cryptology Field	28
Figure 2.2	Analogy for Symmetric Encryption (a Safe with one Lock)	33
Figure 2.3	Analogy for Public-key Encryption (a Safe with a Public Lock for depositing a Message and a Secret Lock for retrieving the Message).....	34
Figure 2.4	Basic Protocol for Public-key Encryption	35
Figure 2.5	Principle of Digital Signatures (Signing and Verifying a Message)	58
Figure 2.6	Communication over an Unsecured Channel	70

Figure 2.7	Symmetric-Key Cryptosystem	72
Figure 4.1	Data Masking versus Encryption.....	99
Figure 4.2	16-bit Fibonacci LFSR.....	102
Figure 4.3	Avalanche Effect Example	104
Figure 5.1	STCVS Block Diagram	107
Figure 5.2	STCVS Use Case Diagram	110
Figure 5.3	STCVS Sequence Diagram	111
Figure 5.4	STCVS Process Diagram	113
Figure 5.5	STCVS Flow Chart	116
Figure 5.6	STCVS Login Webpage	119
Figure 5.7	Voter Authentication Message (1).....	120
Figure 5.8	Voter Authentication Message (2).....	120
Figure 5.9	Voter Authentication Message (3).....	121
Figure 5.10	STCVS Voting Webpage	122
Figure 5.11	STCVS Feedback E-mail(Acknowledgement)	123
Figure 5.12	STCVS Login Error Message (1)	124
Figure 5.13	STCVS Login Error Message (2)	125

Figure 5.14	STCVS Login Error Message (3)	125
Figure 5.15	STCVS Login Error Message (4)	126
Figure 5.16	STCVS Voting Error Message (1).....	126
Figure 5.17	STCVS Voting Error Message (2).....	127
Figure 5.18	STCVS Voting Error Message (3).....	128
Figure 5.19	STCVS SuperVision Login Webpage	129
Figure 5.20	Presidential / Parliamentary / Local Elections Charts.....	131
Figure 6.1	6-Bit NLFSR	135
Figure 6.2	6-Bit LFSR	135
Figure 6.3	Input Data Masking Effect Analysis (First Pattern)	137
Figure 6.4	Input Data Masking Effect Analysis (Second Pattern)	139
Figure 6.5	Input Data Masking Effect Analysis (Third Pattern)	141
Figure 6.6	Input Data Avalanche Effect Analysis (First Pattern)	144
Figure 6.7	Input Data Avalanche Effect Analysis (Second Pattern)	146

Figure 6.8 Input Data Avalanche Effect Analysis (Third Pattern) 148

Figure 6.9 Public Key Avalanche Effect Analysis (First Pattern) 151

Figure 6.10 Public Key Avalanche Effect Analysis (Second Pattern) 153

LIST OF TABLES

Table 1.1	Voting Systems Advantages / Disadvantages	11
Table 1.2	Used Laptop Specifications	24
Table 2.1	Applications for Public-key Cryptosystems	37
Table 5.1	STCVS Database	117
Table 5.2	STCVS Records	130
Table 6.1	Input Data Masking Effect (First Pattern)	136
Table 6.2	Input Data Masking Effect (Second Pattern)	138
Table 6.3	Input Data Masking Effect (Third Pattern)	140
Table 6.4	Input Data Avalanche Effect (First Pattern).....	143
Table 6.5	Input Data Avalanche Effect (Second Pattern)	145
Table 6.6	Input Data Avalanche Effect (Third Pattern)	147
Table 6.7	Public Key Avalanche Effect (First Pattern).....	150
Table 6.8	Public Key Avalanche Effect (Second Pattern)	152