



UNIVERSITI PUTRA MALAYSIA

VOTER VERIFICATION USING RUBIK'S CUBE

MAJID JAVID MOAYED

FSKTM 2009 4



VOTER VERIFICATION USING RUBIK'S CUBE

By

MAJID JAVID MOAYED

**Thesis Submitted to the School of Graduate Studies, University Putra Malaysia, in
Fulfillment of the Requirement for the Degree of Master of Science**

June 2009



DEDICATION

To

*My Father and Mother,
My wife,
My Brother and Sisters*



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of
the requirement for the degree of Master of Science

VOTER VERIFICATION USING RUBIK'S CUBE

By

MAJID JAVID MOAYED

June 2009

Chairman: Associate Professor Abdul Azim Abd. Ghani, PhD
Faculty: Computer Science and Information Technology

Electronic voting systems such as Direct Recording Electronic systems have become more prominent in election processes because of their potential in consistency of implementing security policies. Despite of this potential, most of the systems still exclusively rely on the integrity of election officers and poll workers to ensure that the election maintains the proper security and privacy. Various cryptography voting schemes have been proposed to tackle the problem of how to trust the voting machine with correct recording of votes. However, still the probability of cheating is relatively high.

This thesis proposes an electronic voting system that provides a trustable voter verification system by scrambling ballots as the cryptography method. The system selects and unselects candidates, and Rubik's cube is used for encrypting ballots and



generating receipts. The receipts can be used by voters to verify their votes in the final tally of votes.

Cheating probabilities were analyzed to evaluate the strength of the proposed system. The results of the probability analysis show that cheating probabilities in the proposed system are very low.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

PENGESAHAN PENGUNDI DENGAN MENGGUNAKAN KIUB RUBIK

Oleh

MAJID JAVID MOAYED

Ogost 2009

Pengerusi: Profesor Madya Abdul Azim Abd. Ghani, PhD

Fakulti: Sains Komputer Dan Teknologi Maklumat

Sistem pengundian elektronik seperti Sistem Perekodan Secara Terus Elektronik telah menjadi prominen dalam proses pilihanraya disebabkan oleh potensi mereka dalam melaksana secara konsisten polisi sekuriti. Walaupun berpotensi, kebanyakan sistem masih lagi secara eksklusif bergantung kepada integriti pegawai pilihanraya dan petugas pusat pengundian untuk memastikan pilihanraya menjamin sekuriti dan keadaan berahsia yang sewajarnya. Pelbagai skema pengundian kriptografi telah dicadangkan untuk menangani masalah bagaimana untuk dipercayai mesin undian dengan perekodan undi yang betul. Sungguhpun begitu, kebarangkalian penipuan masih lagi secara relatifnya tinggi.

Tesis ini mencadangkan satu sistem undi elektronik yang menyediakan sistem verifikasi pengundi yang boleh dipercayai dengan mencampuraduk undian sebagai kaedah



kriptografi. Sistem tersebut memilih dan tidak memilih calon, dan kiub Rubik digunakan untuk mengenkrip undi dan menjanakan resit. Resit ini boleh digunakan oleh pengundi untuk mengesahkan undi mereka dalam jumlah akhir undian.

Kebarangkalian penipuan dianalisis untuk menilai kekuatan sistem yang dicadang. Keputusan analisis kebarangkalian menunjukkan kebarangkalian penipuan dalam sistem cadangan adalah rendah.

ACKNOWLEDGMENTS

First and foremost I would like to express my deep gratefulness to my parent for providing me the opportunity to continue my master's program and financial support. And I'm appreciating my wife "Hooraa Sadat Mirsaanei" for her aid in my thesis and for her patience. And I'm grateful to my supervisor Associate Professor Dr. Abdul Azim Abdul Ghani, for his kind assistance, critical advice, encouragement and suggestions during the study and preparation of this thesis. Moreover, I appreciate his encouragement to provide the opportunity to attend several conferences. I truly appreciate the time he devoted in advising me and showing me the proper directions to continue this research and for his openness, honesty and sincerity.

I would also like to express my gratitude to my co-supervisor Associate Professor Ramlan Mahmud, to whom I'm grateful for his practical experience and knowledge that made an invaluable contribution to this thesis.

I also owe thanks to all of the people who were been willing to provide assistance and give advice. Last but not the least the deepest appreciation goes to my friends Matthew Fryslie for their contentious support and encouragement. Another thank you goes to Ms. Lailan Choy for the translation of my abstract into Malay language.



I certify that an Examination Committee has met on 17 Jun 2009 to conduct the final examination of Majid Javid Moayed on his Master of Science thesis entitled "Voter Verification using Rubik's Cube" in accordance with Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the candidate be awarded the relevant degree.

Members of the Examination Committee are as follows:

Shamala K. Subramaniam, PhD

Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Ali Mamat, PhD

Associate professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Abdul Rahman Ramli, PhD

Associate professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Abdul Hanan Abdullah, PhD

Professor
Faculty of Computer Science and Information Technology
Universiti of Technology Malaysia
(External Examiner)

BUJANG KIM HUAT
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:



This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirements for the degree of Master of Science. Members of the Supervisory Committee were as follows:

Abdul Azim Abdul. Ghani, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Ramlan Mahmud, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

HASANAH MOHD GHAZALI, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date: 16 October 2009



DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

Majid Javid Moayed

Date: 16 August 2009



TABLE OF CONTENTS

	Page
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGMENTS	vii
DECLARATION	x
LIST OF TABLES	xiv
LIST OF FIGURES	xv
LIST OF ABBREVIATION	xviii
LIST OF ABBREVIATION	xviii
CHAPTER 1	1
INTRODUCTION	1
1.1 Background	1
1.2 Problem Statement	4
1.3 Research Objectives	7
1.4 Research Scope	7
1.5 Research Contributions	8
1.6 Research Methodology	9
1.7 Thesis Organization	11
CHAPTER 2	12
LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Paper-based voting systems	14
2.3 Electronic voting systems	16
2.3.1 Voter-Verified in Paper-Based Systems	16
2.3.2 Accessibility and DRE systems	18
2.3.3 DREs and voter verification	19
2.3.4 DRE's and Online solutions	21
2.4 Primary Definitions	22
2.4.1 Mix-net	22
2.4.2 <i>Paillier cryptography</i> algorithm	25
2.4.3 ElGamal cryptography algorithms	26
2.4.4 Homomorphic Crypto System	27
2.4.5 A Very Basic homomorphic encryption scheme	27
2.5 Cryptography Approach to Voter Verification	28
2.5.1 Chaum and Visual Cryptography	29
2.5.2 Neff and Votehere.NET	33
2.5.3 Forsythe Gridding Model	38
2.5.4 Roland and his ThreeBallot	42
2.6. Evaluation of existing methods	45



CHAPTER 3	50
RCV METHODOLOGY	50
3.1 Introduction	50
3.2 A simple way for selecting candidate	50
3.2.1 Selecting method in voting system	51
3.3 Rubik's Cube Game Tool	52
3.3.1 Introduction	53
3.3.2 Rubik Cube Characteristics	53
3.3.3 Rubik's Cube Terminology and Move Notation	55
3.4 RCV Method Algorithm	57
3.5 The Method's Parts	64
3.5.1 Ballot Configuration	65
3.5.2 Selecting Candidates	67
3.5.3 Ballot Security (Voting Cryptosystem)	70
3.6 Checking the Integrity of the Bulletin Board	72
3.7 Decrypting ballots and Counting	73
3.8 Summary	74
CHAPTER 4	76
SECURITY OF THE SCHEME	76
4.1 Introduction	76
4.3 Add Invalid Ballots	76
4.4 Modifying or Deleting Ballots	77
4.5 Machine Cheating	77
4.6 Voter factor and his effect	78
4.6.1 Sell Vote by Voter	79
4.6.2 Detecting Malicious Voters	80
4.6.3 Attacking the Checker	81
4.6.4 Paying for Receipts	81
4.6.5 Rubik's Cube permutation	83
4.7 Trustee factor on security	88
4.8 Voter Privacy	89
4.8.1 Receipt and Voter Privacy	90
4.9 Other factors and their effect on security	91
4.9.1 Recounts and Audits	92
4.9.2 Risk at the Printers	92
4.9.3 Risk of Copying	93
4.9.4 Risk of Several Copies	94
CHAPTER 5	95
IMPLEMENTATION AND DISCUSSION OF RESULTS	95
5.1 Introduction	95
5.2 Virtual voting booth	95
5.3 Edge and Corner Permutation	97
5.3.1 Edge Orientation	101
5.3.2 Corner Orientation	102
5.4 Comparing methods	107



CHAPTER 6	109
CONCLUSION AND FUTURE WORK	109
6.1 Conclusion	109
6.2 Future work	112
BIBLIOGRAPHY	115
APPENDICES	119
BIODATA OF STUDENT	148
LIST OF PUBLICATIONS	149



LIST OF TABLES

Table	Page
5.1: Rubik's cube Probabilities	106
6.1: Cheating probabilities in the last methods	110



LIST OF FIGURES

Figure	Page
1.1: Research methodology step by step	10
2.1: A particular permutation for a mix-net	24
2.2: The two pixel symbols separate and overlaid.	30
2.3: The letter “e” in (a) standard printing and (b) receipt printing.	31
2.4: A sample codebook, VC_{14} , for ballot 14.	34
2.5: The trial of a ballot during the decryption process.	36
2.6: An overview of the proposed voter-verification scheme.	39
2.7: A filled-out version the multi-ballot [21]	43
3.1: Kinds of selecting candidate	51
3.3: (a) is a selected and (b) is unselected, (c) and (d) are after rotation	52
3.4: A Rubik’s cube	53
3.5: Side of the Rubik’s cube	55
3.6: This picture shows horizontal motivation groups	56
3.7: This picture shows vertical motivation groups	56
3.8: This pictures show face rotation	56
3.9: RCV Variable definition	57
3.10: Voter ballot preparation	58
3.11: Selecting and unselecting candidates	58
3.12: Scrambling Rubik’s cube	59
3.13: The checking ballot	59
3.14: Generating receipt by scrambling Rubik’s cube	60



3.15: Voting cryptography	61
3.16: Booth flowchart	62
3.17: Voting decryption ballot	63
3.18: Comparing receipt algorithm	63
3.19: The voter verification steps	64
3.20: RCV methodology	65
3.21: A sample of voting system by using Rubik's cube (a ballot)	67
3.22: Selecting and unselecting candidates	68
3.23: An encrypted ballot	69
3.24: A decrypted ballot	69
3.25: Selecting three faces as the receipt	70
3.26: two different receipts	73
3.27: Scanning ballot after solving	74
4.1: Preservation of Edge Parity	85
5.1: A scrambling Rubik's cube	96
5.2: A voting receipt	96
5.3: Rubik's cube simulator software	98
5.4: Probabilities of n corners places (CP)	100
5.5. Probabilities of n edges places (EP)	100
5.6. Simulation of n corners places	100
5.7. Simulation of n edges places	100
5.8: Probabilities of n edges oriented (EO)	102
5.9: Simulation of probabilities of n edges oriented	102
5.10: Probabilities of n corners oriented (CO)	103



5.11: Simulation of probabilities of n Corners Oriented	104
A.1: Above picture shows a Rubik's cube	120
A.2: Above picture shows view side of the Rubik's cube	122
A.3: direction of the various horizontal rows	123
A.4: direction of the various vertical columns	123
A.5: direction of the entire front face	123
A.6: The picture shows view side of the Rubik's cube	124
A.7: Dividing Rubik's cube to five directions	125
A.8: Rotating Rubik's cube at five steps	126
A.9: Correcting fore corner of a face	126
A.10: Dividing Rubik's cube to five points	127
A.11: Rotating Rubik's cube to five directions	127
A.12: Changing two positions in a face	128
A.13: Rotating Some Rubik's level at two steps	129
A.14: Dividing Rubik's cube to fore points	130
A.15: Showing rotated Rubik's cube	130
A.16: Rotating some levels of Rubik's cube at two steps	131
A.17: Changing front face	132
A.18: Rotating front face	132
A.19: Rotating From the correctly- position edge side	133
A.20: After Rotating for correcting edges	133
A.21: Changing positions at front	134
A.22: Rotating levels of Rubik's cube several times	135



LIST OF ABBREVIATION

VVPAT	Voter verified paper audit trail
VVAATT	voter verified audio audit transcript
DRE	Direct Recording Electronic
SBE	State Board of Elections
RFID	Radio Frequency Identification
RPC	Random Partial Checking
GUID	Global Unique Identification
RCV	Rubik's Cube Voting system
E	Encrypt
D	Decrypt
U	Upper Rubik's cube Face
D	Downer Rubik's cube Face
L	Left Rubik's cube Face
R	Right Rubik's cube Face
F	Front Rubik's cube Face
B	Behind Rubik's cube Face



CHAPTER 1

INTRODUCTION

1.1 Background

Public elections are the basis of democratic societies. Selecting leaders and representatives by voting is the most important aim of this kind of government. Eligible voters must be sure that their votes are effective in their function. It is clear that in every election, one person or group wins and other candidates or groups are losers. Hence, after counting votes, there are often some complaints about voting regularity. Losers accuse the winning candidate or group to cheat on the votes.

In the 2000 U.S. presidential election, there was a great controversy because George W. Bush lost the popular vote but won the Electoral College, including a win in Florida by a margin of only 500 votes [24]. Numerous complaints were aired: the “butterfly ballot” in Broward County was misled, the punch card system failed to record a number of votes, and more than 50,000 absentee ballots went missing [25]. This debacle served as a public wake-up call that elections were far from perfect.

As it was doubtful, researchers tried to find a safer way for voting. A Direct Recording Elections (DRE) system was used instead of the paper-base voting system. The DRE system has more benefits than the paper-based system. The DRE system can count ballots faster and more carefully than the paper-based system. Moreover, its expenditure is lower than paper-based system's. The DRE system must have some characteristics



which are necessary in voting systems. Privacy, verification, flexibility, usability, accuracy, and sturdiness are basic requirements of the voting systems.

Voters must be assured that their identifications are secure during the voting process. Then, DRE has to ensure that a voter's final ballot remains secret. Confidence of voting trusty is gained by two ways. First, according of receipt voter must be sure that his ballot did not change and it was counted as intended. Second, voter would not be able to prove the contents of his ballot to anyone according of his receipt and his evidences. Because, voters can sell their votes and voting principle- selecting candidate without any forces and cheating- will be damaged. Voters' identifications and candidate choices must both remain hidden in the voting system.

Today it is common expectation that voters can trace their vote during voting process. Voters have to be able to prove to themselves that their vote was cast as intended and that it was counted exactly. Hence, everyone needs a way to prove that the final tally is accurate. A voter must feel his vote is effective in final result of the election. Comparing between original ballot containers with candidate selected by voter, prevents cheating in voting systems. The reason is that, any changing in ballot for altering voting result will be detected and appeared. It has two advantages: first, voters can be sure their vote did not change. Second, anybody will not cheat by changing ballots. Voter will be satisfied that his vote is counted exactly but he can not prove ballot container to coercers¹. Voter can claim who is his candidate selected but it is impossible to prove it.

¹ Who wants to buy vote from voter



Final tally is summation of the all votes cast, and all correct votes have to be counted in the final summation. Therefore, ballot checking system has an important role in revealing wrong ballots and preventing incorrect ballots from being dropped in the box. Encrypting ballots after they are submitted by voter until counting day will guarantee voting security. The voting system must also be robust, meaning that is it should be stable enough so that a small group of people cannot disrupt the election.

In the 2000 year U.S. presidential election and since then there has been a push to integrate security into voting systems and thereby eliminate the reliance on third parties. In particular, many critics have focused on the problem of how to trust the voting machine with the correct recording of the votes [16]. Of the three common types of cryptography voting schemes, mix-nets and homomorphic have been proposed for addressing this problem. Chaum [10, 13] has proposed using visual cryptography to allow the voter to verify that the ballot has encrypted by choosing one of the encrypted layers. Neff [14] has proposed using receipts with codes corresponding to particular candidates. Forsythe [16] proposed a method by using homomorphic encryption voting systems, which have the advantage of maintaining greater privacy by never revealing the contents of individual ballots [16].

In some² of the previous methods, the probability of cheating is relatively high [16], whereas in some of the methods, voter verification comparing voter receipt with public site is relatively difficult. The reason is that, sometimes these methods require knowledge of mathematic formula [16] and then the common voter may face difficulty

² mix-nets and homomorphic



in understanding mathematic formula. Comparing long complexity text or tiny pixels for decryption or encryption [13] in order to verify the vote is another problem. Ignorance of the verification process or difficulty in voter verification has caused voter confusion [13, 16].

The aim of this thesis is to present a new method which incorporates cryptography and vote security with voter verification. The bases of this method are Rubik's Cube game tools. Simple rules are used for selecting candidate and Rubik's cube is used for mixing candidate for encrypting ballot. Calculation of probability of cheating shows that RCV method is more secure and for using famous game tools is exoteric enough to be understood by everyone.

1.2 Problem Statement

Election type and its requirements depend on the country and its policy but all of them follow some common properties. Every country uses a voting type which is according to some situations, but they have a common aim which is democracy creation. One voting system must have some properties which are election base. All of these properties have to be used in a voting system.

Electronic voting systems and paper-based voting system have some common points. Both of the systems accompany security, during voting days from voter registration day to day of final results publication. Each system must seriously consider exactly purpose about security issues. These properties are:

- Each eligible voter must be able to vote and he cannot vote more than one time in a voting period.
- A voter must be confident that his final ballot will be secret and nobody can access to his vote.
- For preventing from vote selling, a voter never should be able to disclose content of his ballot.
- Voting machine, hardwares, or officials can not change content of ballots.
- Final result must be the sum of all the correct votes.
- Voter must be able to prove to himself that his vote is counted as intended and it has not changed during voting process.
- Voting system must be robust; it means that a small group of people cannot disrupt the election.
- Partial totals should not be known early.

In the voting systems, some of these properties may be violated. There are lots of researches discussing the problems of violated properties. Voting receipt can cover more than one of them. Using ballot as a receipt prevents from some cheating problems on these properties.

Except the first property that depends on voting registration system, others will be discussed in this research. These properties are related to the election security.

Electronic voting system which called Direct Recording Electronic (DRE) system, have recently become more prominent in research institutes and some countries. One of the major advantages of DRE systems is the potential of the consistent implementation of the security policies. A machine performs only what it is programmed to do, whereas human behavior is situation-dependent and may bias the election system. Despite this potential, most of DRE systems still exclusively rely on the integrity of election officers and training poll workers to ensure that the election maintains the proper security and privacy. In order to believe that the votes are properly recorded and tallied, the voters must trust the election officials, the technicians setting up the machines, the programmers writing the software, and the engineers designing the hardware. They need to trust that the machines are stored in a way that prevents from tampering, and have been properly monitored since being removed from storage. They need to trust that the machines will be securely delivered to the counting location after the polls close.

Cheating probability in the previous methods is high that makes these methods unreliable [13, 14, 16, 21]. The cheating probability of Chaum method is $1/2$, Roland method's is $1/3$ and Forsythe method's is $1/d$ in which d is the number of grid rows in the method.

Among the previous voting methods, David Chaum has proposed [10, 13] visual cryptography to allow the voter to verify that the ballot encrypts the intended choices. Joy Marie Forsythe [16] proposed homomorphic cryptography to generate receipt. Chaum and Forsythe methods need to compare tiny pixels, long complexity strings or mathematic knowledge. Therefore, they are difficult for a common user.