

Contents

Abstract	9
Zusammenfassung	11
1 Introduction	15
1.1 Contribution of this Work	16
1.2 Structure of this Work	16
2 Preliminaries	19
2.1 About Elections	19
2.1.1 Election Types	19
2.1.2 Voting Procedure	20
2.1.3 Electoral Systems	21
2.1.4 Properties of Elections	22
2.1.5 Attacks on Voting Schemes	23
2.1.6 Paper vs. Machine	24
2.1.6.1 Paper Ballots	24
2.1.6.2 Optical Scan Voting System	25
2.1.6.3 Voting Machines	25
2.1.7 Presence vs. Remote Voting	26
2.2 Terminology and Notions	27
2.2.1 Roles in an Election	27
2.2.2 Phases of an Election	27
2.2.3 Tally and Result	28
2.3 Security Notions	29
2.3.1 Correctness	29
2.3.1.1 Software Independence	29
2.3.1.2 End-to-end Security	30
2.3.2 Ballot Secrecy	30
2.3.2.1 Receipt Freeness	31
2.3.2.2 Coercion Resistance	31
2.3.3 Practical Requirements	32
2.3.3.1 Dispute Freeness	32
2.3.3.2 Robustness	32
2.3.4 Computational & Unconditional Security	32
2.4 Cryptography	33
2.4.1 Bulletin Board	33

2.4.2	Commitments	33
2.4.2.1	UHDLCs	34
2.4.2.2	Rerandomization	35
2.4.3	Zero-knowledge Proofs	35
2.4.3.1	Interactive Zero-knowledge Proofs	36
2.4.3.2	Non-interactive Zero-knowledge Proofs	36
2.4.4	Proof of a Shuffle of Known Content	36
2.4.4.1	Randomized Partial Checking	37
2.4.4.2	Efficient Proof of a Shuffle of Known Content by Groth	38
2.5	Cryptographic Voting Schemes	39
2.5.1	Farnel and Twin	39
2.5.2	Voteegrity	40
2.5.3	MarkPledge	41
2.5.4	Prêt à Voter	42
2.5.5	Punchscan	43
2.5.6	Voting Scheme by Moran and Naor	43
2.5.7	ThreeBallot	44
2.5.8	Scantegrity and Scantegrity II	45
3	Bingo Voting	47
3.1	Important Concepts	47
3.1.1	Trusted Random Number Generator	48
3.1.2	Commitments for Bingo Voting	49
3.1.3	Dummy Votes	49
3.2	Bingo Voting in a Nutshell	50
3.3	Bingo Voting Protocol	51
3.3.1	Preparation Phase	51
3.3.2	Voting Phase	52
3.3.3	Tally Phase	52
3.4	Verification	53
3.4.1	Individual Verification	54
3.4.2	Global Verification	55
4	Real-World Experiences with Bingo Voting	57
4.1	Election Details	58
4.1.1	Student Parliament Election	59
4.1.2	Other Elections	59
4.1.3	Formal Requirements	59
4.1.4	Implementation of the Voting Machine	59
4.2	Experiences	61
4.2.1	Preparation Phase	61
4.2.2	Voting Phase	62
4.2.3	Tally Phase	63
4.2.4	Conclusions from the Student Parliament Election	63
4.3	Latest Prototype	64

5	Improvements for Bingo Voting	65
5.1	Bingo Voting for Complex Elections	65
5.1.1	Abstention and Invalid Votes	66
5.1.2	Multiple Votes per Voter	67
5.1.3	Ranking Candidates	68
5.1.4	Multiple Voting Machine	69
5.2	Reducing the Length of Random Numbers	70
5.3	Presentation of Random Numbers	72
5.4	Dispute Resolution	73
5.4.1	Dispute Resolution During the Voting Phase	74
5.4.2	Dispute Resolution During the Tally Phase	75
5.5	Reducing the Size of Public Data	77
5.5.1	Decreasing Dummy Vote Size	78
5.5.2	Changing the Proof Style	78
5.5.3	Optimizing the Proof of Correct Distribution of Dummy Votes	79
5.6	Preventing the Receipt Stealing Attack	80
5.6.1	Receipt Stealing Attack	80
5.6.2	Hash Chains	82
5.6.3	Hidden Hash Chains	83
5.6.4	Relevance for Other Schemes	84
6	Analysis and Evaluation	85
6.1	Scenarios for Evaluation	86
6.2	Assumptions Required for Bingo Voting	86
6.2.1	General Assumptions	87
6.2.2	Voting Booth Assumption	88
6.2.3	Verification Assumption	88
6.2.4	Random Number Generator	89
6.2.5	Receipt Authenticity Assumption	90
6.2.6	Discrete Logarithm Assumptions	91
6.2.7	Hash Function Assumptions	91
6.3	Security Analysis of Bingo Voting	91
6.3.1	Voter Privacy	92
6.3.1.1	Receipt Freeness	93
6.3.1.2	Coercion Resistance	93
6.3.2	Correctness and Verifiability	94
6.3.2.1	Individual Verification	94
6.3.2.2	Global Verification	94
6.3.3	Dispute Freeness	95
6.3.4	Robustness and Recovery	95
6.3.5	Collisions	95
6.3.5.1	Consequences of Collisions	96
6.3.5.2	Probability of Collisions	97
6.4	Practical Considerations	99
6.4.1	A Comparison of Usability	99
6.4.1.1	Prêt à Voter	99
6.4.1.2	Punchscan	100
6.4.1.3	Voting Scheme by Moran and Naor	101

6.4.1.4	Bingo Voting	101
6.4.1.5	Comparison	101
6.4.2	Size of Public Data	102
6.4.2.1	Published Data Size of the Original Version . . .	102
6.4.2.2	Published Data Size of the Improved Version . .	104
6.4.2.3	Size Improvement	105
6.4.3	Legal Considerations	105
7	Conclusion	107
	Bibliography	109