

Table of Contents

1	Introduction.....	5
1.1	Background.....	5
1.2	History.....	6
1.3	Motivation.....	12
2	Theory.....	18
2.1	Cryptographic Elements.....	18
2.2	“A Practical Secret Voting Scheme for Large Scale Elections”.....	22
3	The E-Vox System.....	26
3.1	Assumptions.....	26
3.2	Creating a Well-Defined System.....	27
3.3	The Revised Voting Protocol.....	33
3.4	Proof of Correctness of the Revised Protocol.....	37
4	Components.....	42
4.1	Cryptographic Library.....	42
4.2	Vote Object.....	43
4.3	GenRand, the Random Number Generator.....	44
4.4	Network Connections.....	45
4.5	Registrar.....	47
4.6	Election Builder.....	47
4.7	Servers.....	49
4.8	Voting Applet.....	62
5	Testing.....	65
6	Limitations, Their Solutions, and Further Extensions.....	67
6.1	Code Improvements.....	67
6.2	Protocol.....	68
6.3	Architecture.....	74
6.4	Policy.....	77
7	Conclusion.....	79
	Appendix	80
	Bibliography	81

