

# Contents

<b>Agradecimientos</b>	<b>i</b>
<b>Abstract</b>	<b>iii</b>
<b>Resumen</b>	<b>v</b>
<b>Resum</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Distributed Cryptography . . . . .	3
1.2 Electronic Voting . . . . .	4
1.3 Anonymous Identification & Access . . . . .	5
1.4 Thesis Organization . . . . .	6
<b>2 Cryptography</b>	<b>9</b>
2.1 Algebra . . . . .	10
2.1.1 Groups and Fields . . . . .	10
2.1.2 Fields . . . . .	12
2.1.3 Polynomials . . . . .	13
2.1.4 Elliptic Curves . . . . .	14
2.2 Secret Sharing . . . . .	16
2.2.1 Verifiable Secret Sharing . . . . .	16
2.3 Public-Key Cryptography . . . . .	17
2.3.1 Diffie-Hellman . . . . .	18
2.3.2 RSA . . . . .	19
2.3.3 Commitment Schemes . . . . .	20

2.4	Zero-Knowledge . . . . .	21
2.4.1	Schnorr Zero Knowledge Identification . . . . .	22
2.4.2	Non-interactivity and the Fiat Shamir Heuristic . . . . .	23
2.5	Complexity & Computability . . . . .	24
2.5.1	Discrete Logarithm Problem . . . . .	25
2.5.2	Cryptographic Assumptions . . . . .	26
2.5.3	Perfect Secrecy . . . . .	27
2.6	Digital Signatures . . . . .	28
2.6.1	Blind Signatures . . . . .	29
2.6.2	Ring Signatures . . . . .	30
<b>3</b>	<b>Blockchain</b>	<b>31</b>
3.1	Blockchain Basics & Bitcoin . . . . .	31
3.1.1	Blockchain Trilemma . . . . .	33
3.1.2	Block Finality . . . . .	34
3.1.3	Addresses . . . . .	35
3.2	Ethereum . . . . .	36
3.2.1	Gas Fees . . . . .	37
3.2.2	Events . . . . .	38
3.3	Monero . . . . .	38
3.3.1	One Time Public Keys . . . . .	39
3.3.2	Ring Signature Confidential Transactions . . . . .	40
3.4	Other Blockchains and Applications . . . . .	41
3.4.1	Other blockchains . . . . .	41
3.4.2	Applications . . . . .	43
3.5	Risks . . . . .	44
<b>4</b>	<b>Electronic Voting</b>	<b>45</b>
4.1	State of the Art . . . . .	50
4.1.1	Blind Signatures . . . . .	50
4.1.2	Ring Signatures . . . . .	52
4.1.3	Homomorphic Cryptography . . . . .	53
4.1.4	Zero-Knowledge Proofs . . . . .	55
4.1.5	Blockchain . . . . .	56
4.2	TAVS: A two Authorities Voting scheme . . . . .	63
4.2.1	Description of our Proposal . . . . .	65
4.2.2	Properties of the voting scheme . . . . .	74
4.2.3	Time complexity analysis . . . . .	76

4.3	Distributed Trust, a Blockchain Election Scheme . . . . .	84
4.3.1	Description of our Proposal . . . . .	85
4.3.2	Properties of the voting scheme . . . . .	93
4.3.3	Time complexity analysis . . . . .	96
4.4	SUVS: Secure Unencrypted Voting Scheme . . . . .	100
4.4.1	Description of our Proposal . . . . .	101
4.4.2	Properties of the voting scheme . . . . .	111
4.4.3	Time complexity analysis . . . . .	115
4.5	Review of the 3 Voting Protocols . . . . .	118
4.6	Conclusions . . . . .	119
4.6.1	Future Work . . . . .	120
<b>5</b>	<b>Identification and Distributed Access</b>	<b>121</b>
5.1	State of the Art . . . . .	122
5.2	Anonymous Access . . . . .	125
5.3	Centralized Registration, Anonymous Access . . . . .	127
5.3.1	Trusted Registration, Anonymous Access . . . . .	128
5.4	Distributed Registration, Anonymous Access . . . . .	132
5.4.1	Trusted distributed registration, anonymous access . . . . .	133
5.4.2	Anonymous registration, anonymous access . . . . .	137
5.5	Security Analysis . . . . .	142
5.5.1	TRA2 Analysis . . . . .	142
5.5.2	TDRA2 and ARA2 Analysis . . . . .	144
5.6	Time Complexity Analysis . . . . .	147
5.6.1	TRA2 and TDRA2 time complexity analysis . . . . .	148
5.6.2	ARA2 time complexity analysis . . . . .	148
5.7	Applications . . . . .	149
5.7.1	Blockchain Airdrop System . . . . .	149
5.7.2	Electronic Voting Scheme . . . . .	150
5.8	Conclusions . . . . .	151
5.8.1	Future Work . . . . .	152
<b>6</b>	<b>Conclusions</b>	<b>153</b>
6.1	PhD Key Results . . . . .	154
6.1.1	Electronic Voting . . . . .	155
6.1.2	Anonymous Identification . . . . .	155

<b>A</b>	<b>A Solidity implementation of TAVS</b>	<b>185</b>
A.1	From ECC to RSA . . . . .	186
A.1.1	Code Organization . . . . .	187
A.2	Tests . . . . .	189
A.3	Properties . . . . .	190
A.4	How to create your own election . . . . .	192
A.5	Gas analysis: Costs of having an election . . . . .	195
<b>B</b>	<b>A Benchmark for Ring Signatures</b>	<b>197</b>
<b>C</b>	<b>Distributed Trust Technical Specification</b>	<b>201</b>
C.0.1	Blockchain data structures . . . . .	201
C.0.2	Methods . . . . .	205
<b>D</b>	<b>How to Grant Anonymous Access Implementation</b>	<b>213</b>

# List of Figures

2.1	Elliptic curve examples . . . . .	15
2.2	Schnorr’s Zero-Knowledge Proof. . . . .	24
3.1	Blockchain Trilemma Problem . . . . .	34
4.1	TAVS: Pre-ballot structure . . . . .	68
4.2	TAVS: Certified ballot structure . . . . .	70
4.3	TAVS: Submission of ballot . . . . .	71
4.4	TAVS: Time interaction diagram . . . . .	72
4.5	Distributed Trust: Generating keys . . . . .	87
4.6	Distributed Trust: Registration process . . . . .	89
4.7	Distributed Trust: Casting a ballot . . . . .	90
4.8	Distributed Trust: Processing of a vote . . . . .	91
4.9	Distributed Trust: Recovering secret component of the key . . . . .	93
4.10	SUVS: Time interaction diagram . . . . .	109
5.1	Accessing a guarded resource . . . . .	130
5.2	Dealers communicating to guards . . . . .	134
5.3	Anonymous identifying to dealers . . . . .	135
A.1	STAVS: Time interaction diagram . . . . .	187
B.1	Ring signature performance times . . . . .	199
C.1	General view of blockchain data structures . . . . .	206
C.2	Distributed Trust time interaction diagram . . . . .	211

D.1	TRA2 experimental times . . . . .	215
D.2	TDRA2 experimental times . . . . .	216
D.3	ARA2 experimental times . . . . .	216

# List of Tables

4.1	TAVS: Elector and system complexity . . . . .	80
4.2	Distributed Trust: Elector and system complexity . . . . .	100
4.3	SUVS: Elector and system complexity . . . . .	118
A.1	STAVS: Costs of running an Election . . . . .	195
A.2	STAVS: Costs of calling <code>computeWinner</code> method . . . . .	196
C.1	Transaction structure in Distributed Trust . . . . .	202
C.2	Transaction's inputs and outputs structure . . . . .	202
C.3	Block structure . . . . .	203
C.4	First block structure . . . . .	204
C.5	Second block structure . . . . .	204
C.6	Last block structure . . . . .	205



# List of Algorithms

1	RSA key generation . . . . .	19
2	RSA encryption . . . . .	19
3	RSA decryption . . . . .	20
4	Schnorr’s Zero-Knowledge identification protocol. . . . .	23
5	Non-interactive Schnorr’s identification protocol . . . . .	25
6	Ring Confidential Transaction Generation . . . . .	41
7	Ring Confidential Transaction Verification . . . . .	42
8	TAVS: Pre-ballot generation . . . . .	67
9	TAVS: Pre-ballot certification . . . . .	69
10	TAVS: Ballot casting . . . . .	73
11	SUVS: Ballot crafting . . . . .	104
12	SUVS: Ballot certification . . . . .	106
13	SUVS: Casting a vote . . . . .	107
14	SUVS: Tallying votes . . . . .	109
15	TRA2 Algorithm . . . . .	131
16	TDRA2 Algorithm . . . . .	136
17	ARA2 Algorithm . . . . .	139
18	Distributed Trust: Voting process . . . . .	207
19	Distributed Trust: Validating a transaction . . . . .	208
20	Distributed Trust: Generating a block . . . . .	209
21	Distributed Trust: Validating a block . . . . .	210
22	Distributed Trust: Adding a block . . . . .	211