

# Contents

<b>List of Tables</b>	<b>x</b>
<b>List of Figures</b>	<b>xii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background and Motivation . . . . .	1
1.2 Problem . . . . .	2
1.3 Hypothesis . . . . .	4
1.4 Objectives . . . . .	4
1.4.1 General objective . . . . .	4
1.4.2 Specific objectives . . . . .	4
1.5 Methodology . . . . .	5
1.6 Contributions . . . . .	6
1.7 Related Work . . . . .	7
1.7.1 Callisto . . . . .	7
1.7.2 Who Too . . . . .	7
1.7.3 Secure Allegations Escrow (SAE) . . . . .	8
1.8 Structure . . . . .	8
<b>2 Cryptographic Tools</b>	<b>9</b>
2.1 Preliminaries . . . . .	9
2.1.1 Notation . . . . .	9
2.1.2 Probabilistic Polynomial Time (PPT) Algorithm . . . . .	9
2.1.3 Bilinear pairings . . . . .	10
2.1.4 Computational Assumptions . . . . .	10
2.1.5 Communication channels . . . . .	11
2.1.6 Security Requirements and Threat Model . . . . .	11
2.2 Building Blocks . . . . .	12
2.2.1 Pseudo-Random Functions: . . . . .	12
2.2.2 Hash Function . . . . .	12
2.2.3 Message Authentication Code (MAC) . . . . .	13
2.2.4 ElGamal Encryption . . . . .	14
2.2.5 Zero-knowledge proofs . . . . .	16
2.2.6 Threshold Operations . . . . .	17
2.2.7 Distributed Group Signatures . . . . .	19
2.2.8 Privacy-Preserving Multisets . . . . .	20

<b>3</b>	<b>A First Review of WhoToo</b>	<b>22</b>
3.1	Protocol Overviews . . . . .	22
3.1.1	WhoToo: An Introduction . . . . .	22
3.1.2	WhoToo <sup>+</sup> Overview . . . . .	24
3.2	Two Issues in WhoToo . . . . .	25
3.2.1	Securely Evaluating Quorum in WhoToo . . . . .	25
3.2.2	Identifying Duplicated Accusations . . . . .	27
<b>4</b>	<b>Improving WhoToo</b>	<b>29</b>
4.1	Duplicate Revision . . . . .	29
4.1.1	Distributed Input Pseudorandom Functions (DIPRF): . . . . .	29
4.1.2	Avoiding mismatched accusations: . . . . .	32
4.2	Matching accusations . . . . .	32
<b>5</b>	<b>Variants and Extensions</b>	<b>37</b>
5.1	Discarded ideas . . . . .	37
5.2	Flexible quorum . . . . .	38
5.3	Role . . . . .	39
5.4	Unknown perpetrator . . . . .	39
5.5	Additional Public Information . . . . .	39
5.5.1	Contact for further investigation . . . . .	39
5.5.2	Repetition counter . . . . .	40
5.6	Updates . . . . .	40
<b>6</b>	<b>Description and Security of the New Protocol</b>	<b>41</b>
6.1	WhoToo <sup>+</sup> Description . . . . .	41
6.2	Security Analysis . . . . .	45
<b>7</b>	<b>Implementation and Efficiency</b>	<b>52</b>
7.1	Prototype . . . . .	52
7.2	Efficiency Analysis and Discussion . . . . .	53
7.2.1	Theoretical Efficiency . . . . .	53
7.2.2	Experimental Efficiency . . . . .	55
<b>8</b>	<b>Concluding Remarks and Future Work</b>	<b>62</b>
8.1	Concluding Remarks . . . . .	62
8.2	Future Work . . . . .	62
<b>9</b>	<b>Bibliography</b>	<b>64</b>
<b>10</b>	<b>Appendix</b>	<b>69</b>
10.1	Focus Groups' Guideline . . . . .	69