

# CONTENTS

<b>Introduction</b>	<b>5</b>
<b>1 Thesis Overview</b>	<b>6</b>
1.1 Motivation . . . . .	6
1.2 Goals . . . . .	6
1.3 Contribution . . . . .	7
1.3.1 Relation to Author's Other Publications . . . . .	8
1.4 Structure . . . . .	8
<b>2 Cryptography Fundamentals</b>	<b>10</b>
2.1 Notation . . . . .	10
<b>3 Existing Systems Using Proofs of Knowledge</b>	<b>12</b>
3.1 Authentication and Identification Schemes . . . . .	12
3.2 Anonymous Credentials . . . . .	13
3.3 Group Signatures, Data Collection Schemes . . . . .	13
<b>4 Novel Systems Using Proofs of Knowledge</b>	<b>16</b>
4.1 Authentication and Identification Schemes . . . . .	16
4.1.1 Introduction to PACs . . . . .	16
4.1.2 Our Contribution . . . . .	17
4.1.3 SPAC Summary . . . . .	18
4.2 Anonymous Credentials . . . . .	18
4.2.1 Introduction to ABCs . . . . .	18
4.2.2 Our Contribution . . . . .	19
4.2.3 ABC Summary . . . . .	19
4.3 Group Signatures, Data Collection Schemes . . . . .	19
4.3.1 Introduction to VANETs . . . . .	20
4.3.2 Our Contribution . . . . .	20
4.3.3 SVANET Summary . . . . .	21
<b>5 Implementation Aspects</b>	<b>22</b>
5.1 Implementation of Primitive Operations . . . . .	22
5.1.1 Pilot Results . . . . .	23
5.2 Implementation Summary . . . . .	23
<b>6 Conclusion</b>	<b>24</b>
<b>Bibliography</b>	<b>25</b>
<b>List of Abbreviations</b>	<b>30</b>