

# Table of Contents

<b>Declaration</b>	<b>I</b>
<b>Certificate</b>	<b>III</b>
<b>Abstract</b>	<b>V</b>
<b>Acknowledgments</b>	<b>IX</b>
<b>Table of Contents</b>	<b>XI</b>
<b>List of Figures</b>	<b>XV</b>
<b>List of Tables</b>	<b>XVII</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.1.1 Need of Internet of Vehicles . . . . .	3
1.1.2 Security Requirements in Internet of Vehicles . . . . .	4
1.2 Research Motivation . . . . .	7
1.3 Research Objectives . . . . .	9
1.4 Summary of Contributions . . . . .	11
1.4.1 Tamper-Proof Device Based Solutions . . . . .	11
1.4.2 Physical Unclonable Function Based Solutions . . . . .	13
1.5 Preliminaries . . . . .	14
1.5.1 Hardware Security Modules . . . . .	14
1.5.2 Simulation Tools . . . . .	17
1.5.3 Models for Security Analysis . . . . .	19
1.6 Thesis Structure . . . . .	21
<b>2 Related Work</b>	<b>23</b>
2.1 Based on Tamper-Proof Device . . . . .	24
2.1.1 Authentication Schemes . . . . .	24
2.1.2 Batch Verification Methods . . . . .	26
2.1.3 Secure Data Handling . . . . .	29
2.2 Based on Physical Unclonable Functions . . . . .	32
2.2.1 Authentication Schemes . . . . .	32
2.2.2 Secure Data Handling . . . . .	35

<b>3</b>	<b>Lightweight Authentication and Verification using Tamper-Proof Devices</b>	<b>41</b>
3.1	Conditional Privacy Preservation and Lightweight Authentication . . . . .	42
3.1.1	Network and Adversary Model . . . . .	44
3.1.2	Proposed Scheme: NoMAS . . . . .	46
3.1.3	Security Analysis . . . . .	51
3.1.4	Performance Analysis and Simulation Results . . . . .	57
3.1.5	Implementation Considerations in Diverse IoV Environments . . . . .	62
3.2	Static Batch Verification . . . . .	62
3.2.1	Proposed Scheme: Static Batch Verification . . . . .	63
3.2.2	Security Analysis . . . . .	68
3.2.3	Performance Analysis and Simulation Results . . . . .	70
3.3	Dynamic Batch Verification . . . . .	72
3.3.1	Network and Delay Model . . . . .	73
3.3.2	Proposed Method: Dynamic Batch Verification (DyBatch) . . . . .	75
3.3.3	Security Analysis . . . . .	81
3.3.4	Performance Analysis and Simulation Results . . . . .	83
3.4	Summary of the Work . . . . .	87
<b>4</b>	<b>Secure Data Handling using Tamper-Proof Devices</b>	<b>89</b>
4.1	Proposed Hybrid Architecture for Internet of Vehicles . . . . .	90
4.2	Proposed Scheme: <i>SecEdge</i> . . . . .	91
4.3	Security Proof and Analysis . . . . .	95
4.4	Performance Analysis And Simulation Results . . . . .	102
4.5	Summary of the Work . . . . .	105
<b>5</b>	<b>Lightweight Authentication using Physical Unclonable Functions</b>	<b>107</b>
5.1	PUF based Lightweight and Efficient Authentication by Integrating the Edge-computing . . . . .	108
5.1.1	Network Model . . . . .	109
5.1.2	Proposed Scheme: <i>PESPI</i> . . . . .	110
5.1.3	Security Analysis . . . . .	115
5.1.4	Performance Analysis and Simulation Results . . . . .	118
5.2	PUF-based Lightweight Authentication in Drone-assisted Internet of Vehicles . . . . .	122
5.2.1	Network Model . . . . .	124
5.2.2	Proposed Scheme: <i>SECURE</i> . . . . .	125
5.2.3	Performance Analysis and Simulation Results . . . . .	130
5.3	Summary of the Work . . . . .	133
<b>6</b>	<b>Secure Data Handling using Physical Unclonable Functions</b>	<b>135</b>
6.1	Proposed Scheme: PUF-AEAD . . . . .	136
6.1.1	Security Enhancement Using PUFs . . . . .	136
6.1.2	Modified AEAD algorithm using PUF . . . . .	138
6.1.3	Proposed Cryptographic Hardware Accelerator . . . . .	140
6.2	Security Analysis . . . . .	143
6.3	Experimental Setup and Performance Analysis . . . . .	145
6.4	Summary of the Work . . . . .	149

<b>7 Conclusion and Future Direction</b>	<b>151</b>
7.1 Chapter 1: Introduction . . . . .	151
7.2 Chapter 2: Related Work . . . . .	151
7.3 Phase 1: TPD-based Security Solutions . . . . .	152
7.3.1 Chapter 3: Lightweight Authentication and Verification: . . . . .	152
7.3.2 Chapter 4: Secure Data Handling: . . . . .	152
7.4 Phase 2: PUF-Based Security Solutions . . . . .	152
7.4.1 Chapter 5: Lightweight Authentication using PUF: . . . . .	153
7.4.2 Chapter 6: Secure Data Handling using PUF: . . . . .	153
7.5 Limitations and Future Direction . . . . .	154
 <b>Publications</b>	 <b>155</b>
 <b>References</b>	 <b>157</b>