

Contents

Preface — V

1	Introduction to Cryptography — 1
1.1	Cryptography — 1
1.1.1	Branches of Cryptology — 1
1.1.1.1	Introduction — 1
1.1.1.2	Cryptology — 1
1.1.1.3	Cryptography — 1
1.1.1.4	Encryption — 2
1.1.1.5	Decryption — 3
1.1.1.6	Cryptographic Key — 3
1.1.1.7	Cryptographic Protocol — 3
1.1.1.8	Cryptanalysis — 3
1.1.1.9	Cryptanalyst — 4
1.1.2	Cryptographic Design Principles — 4
1.1.2.1	Confusion — 4
1.1.2.2	Diffusion — 4
1.1.2.3	Avalanche Effect — 4
1.1.2.4	Random Oracle — 5
1.1.2.5	Kerckhoffs' Principle — 5
1.1.3	Symmetric Cryptography — 5
1.1.3.1	Secret Key — 5
1.1.3.2	Number of Keys — 5
1.1.4	Asymmetric Cryptography — 6
1.1.4.1	Key Pair for Asymmetric Cryptography — 6
1.1.4.2	Private Key — 6
1.1.4.3	Public Key — 6
1.1.4.4	Asymmetric Encryption — 7
1.1.4.5	Digital Signatures — 8
1.1.4.6	Combination of Encryption and Digital Signatures — 8
1.1.4.7	Man-in-the-Middle Attack — 8
1.1.4.8	Digital Certificate — 10
1.2	One-Way Hash Function — 11
1.2.1	Characteristics — 11
1.2.2	Hash Functions in Practice — 12
1.3	Block Cipher — 12
1.3.1	Construction — 12
1.3.2	Padding — 13
1.3.3	Block Ciphers in Practice — 13
1.3.3.1	Advanced Encryption Standard — 13

1.3.3.2	Lightweight Cipher PRESENT —	16
1.4	Block Cipher Modes of Operations —	18
1.4.1	ECB Mode —	19
1.4.2	CBC Mode —	19
1.5	Bit Stream Ciphers —	20
1.6	Message Authentication Codes —	21
1.6.1	Authentication —	21
1.6.2	MAC Generation Using a Symmetric Block Cipher —	23
1.6.3	MAC Generation Using a Dedicated Hash Function —	23
1.6.4	Security Aspects of MAC —	24
1.7	Digital Signatures —	25
1.7.1	Digital Signatures with Appendix —	25
1.7.2	Digital Signatures with Message Recovery —	26
1.7.3	RSA Algorithm —	26
1.7.4	Digital Signature Algorithm —	29
1.7.5	Elliptic Curve Cryptography —	30
	References —	35
2	Threat Analysis and Risk Assessment —	37
2.1	Background —	37
2.1.1	Software in Automotive —	37
2.1.2	Threat Model —	38
2.1.3	Threat Analysis —	38
2.2	Threat Analysis and Risk Assessment in Automotive —	39
2.2.1	Security Analysis Methodologies —	39
2.2.2	HEAVENS Project Approach —	40
2.2.2.1	Threat-Level Parameters —	41
2.2.2.2	Impact-Level Parameters —	43
2.3	Case Study: Advanced Driver Assistance System —	45
2.3.1	System Background —	45
2.3.2	Vehicular Architecture —	46
2.3.3	Important Elements of the System —	46
2.3.4	Threat Identification —	50
2.3.5	Risk Assessment —	50
2.3.5.1	Automated Parking via Bluetooth —	51
2.3.5.2	Remote Access – Mobile Communications —	52
2.3.5.3	Remote Access – Wi-Fi —	53
2.3.5.4	Radar Spoofing —	54
2.3.5.5	Reflashing ADAS ECU through Physical Access —	56
2.3.5.6	Summary —	57
2.3.5.7	Security Requirements —	58
	References —	59

3	Machine Learning — 61
3.1	Machine Learning Categories — 61
3.1.2	Supervised Machine Learning — 63
3.1.2.1	Linear Regression — 64
3.1.2.2	Logistic Regression — 64
3.1.2.3	Support Vector Machines and Support Vector Regression — 65
3.1.2.4	Decision Trees — 66
3.1.2.5	Random Forests — 67
3.1.2.6	Naïve Bayes — 67
3.1.2.7	Artificial Neural Networks — 68
3.1.2.8	Bootstrap Aggregating (Bagging) and Boosting — 70
3.1.2.9	Stacked Aggregating — 71
3.1.3	Unsupervised Machine Learning — 71
3.1.3.1	Clustering Algorithms — 72
	References — 84
4	Machine Learning for Anomaly Detection — 87
4.1	Intrusion Detection Systems — 87
4.1.1	Overview and Categorization — 87
4.1.2	Categorization and Properties of ML Techniques in Intrusion Detection Systems — 89
4.1.3	Security Levels of Intrusion Detection Systems — 91
4.1.4	ML-Based Anomaly Detection — 92
4.1.5	Cyberattacks on ML-Based Intrusion Detection Systems — 99
4.1.5.1	Use of GAN Technology for Targeted Circumvention of Protection Systems — 102
4.1.6	Use of IDS for Automotive CAN — 105
4.1.6.1	CAN Bus Architecture — 106
4.1.6.2	CAN Bus Vulnerabilities and Possible Attacks — 115
4.1.6.3	Security Solutions for CAN Bus — 121
	References — 131
5	Distributed Ledger Technologies — 137
5.1	Introduction — 137
5.2	Cryptocurrencies — 139
5.3	Blockchain — 141
5.3.1	Proof of Work — 147
5.3.2	Bitcoin Vulnerabilities and Handling of Issues — 150
5.3.3	Other Blockchain Cryptocurrencies — 153
5.4	Tangle — 154
5.4.1	IOTA Bundle — 160
5.5	Hashgraph — 163

- 5.6 DLT Applications in Autonomous Driving — **180**
- 5.6.1 Financial Sector — **181**
- 5.6.2 Other Sectors — **181**
- 5.6.3 Tracking Supply Chains — **182**
- 5.6.4 Autonomous Driving Systems — **182**
- 5.6.5 Vehicle Lock/Unlock — **183**
- 5.6.6 Payments Related to Cars — **184**
- 5.6.7 Ridesharing of Autonomous Cars — **184**
- 5.6.8 Unadulterated Reading of Mileage — **185**
- 5.6.9 Motivating Ecologically Responsible Driving — **185**
- 5.6.10 Reservation of Parking Places — **186**
- 5.6.11 Avoiding Traffic Obstacles — **186**
- 5.6.12 Data Exchange for Digital Twin Synchronization — **186**
- 5.6.13 Registering and Management of Serial Numbers — **187**
- 5.6.14 Registries as the Digital Proof of Ownership — **187**
- 5.6.15 Software and Documents Release Management — **188**
- References — **188**

6 Self-Correcting and Authentication Algorithm for Automotive Applications — 190

- 6.1 Self-Learning Algorithms — **190**
- 6.2 Related Work — **191**
- 6.3 Error Correction Codes — **193**
- 6.3.1 RS codes — **194**
- 6.3.2 Turbo Codes — **194**
- 6.3.3 Low Density Parity Check Codes — **195**
- 6.4 Two-Phase Self-Correcting Algorithm — **195**
- 6.4.1 Phase-I — **196**
- 6.4.2 Phase-II — **197**
- 6.5 Learning Property — **199**
- 6.6 Security Analysis — **200**
- 6.7 Simulation Results — **202**
- References — **206**

Index — 209