

Contents

Part I RFID Security Preliminaries

1	Introduction to RFID	3
1.1	Automatic Identification	4
1.2	RFID History and Standardization	6
1.3	RFID Applications	7
1.3.1	Logistics and Supply Chain Management	8
1.3.2	Ticketing	10
1.3.3	Health Care	10
1.3.4	Security and Identification	11
1.3.5	Toll Systems and Payment Applications	11
1.3.6	Tacking Applications	11
1.3.7	RIDF and Smart Objects	12
1.4	RFID System Overview	12
1.5	RFID Construction Formats	14
1.6	RFID Classifications	16
1.6.1	Communication Mechanism	16
1.6.2	Memory	17
1.6.3	Operating Frequency	17
1.6.4	Power Source	19
1.7	How Passive RFID Tags Work	21
1.8	RFID Systems Advantages and Challenges	22
1.8.1	Advantages of RFID Systems	23
1.8.2	Challenges to RFID Systems	23
1.9	Book Organization	24
	References	25
2	RFID Security Threats and Basic Solutions	27
2.1	Security Attacks in RFID Systems	27
2.1.1	Physical RFID Threats	28
2.1.2	RFID Channel Threats	29
2.1.3	System Threats	32

2.2	RFID Security Measures and Defenses	33
2.2.1	Physical Solutions for RFID Privacy Protection	34
2.2.2	Authentication	38
2.3	Concluding Remarks	39
	References	40
3	Cryptography in RFID Systems	43
3.1	Wireless Security Preliminaries	44
3.2	Cryptography Overview	45
3.2.1	Symmetric Private Key Encryption	45
3.2.2	Asymmetric Public Key Encryption	46
3.2.3	Hash Function	48
3.3	Lightweight Cryptography	50
3.4	Asymmetric Key Encryption Lightweight Cryptosystems	51
3.4.1	Elliptical Curve Cryptography (ECC)	52
3.5	Symmetric Key Encryption Lightweight Cryptosystems	53
3.5.1	Block Ciphers	53
3.5.2	Stream Ciphers	59
3.5.3	Hybrid Ciphers	64
3.6	Motivation for RBS Lightweight RFID Cryptosystems	67
3.6.1	RBS Design Objectives	68
3.7	Conclusion	69
	References	69
 Part II Lightweight RFID Redundant Bit Security		
4	RBS Cryptosystem	75
4.1	Key and Number of Redundant Bits	76
4.1.1	Key Space	76
4.1.2	Flexibility in Security Level	80
4.2	Location of Redundant Bits	81
4.3	Value of Redundant Bits	81
4.3.1	Message Authentication and Data Integrity	82
4.3.2	Message Authentication and Redundant Bits	84
4.4	Plaintext Manipulation	85
4.4.1	Direct Appearance Inside the Ciphertext	85
4.4.2	Bitwise Addition with a Constant-Value Keystream	86
4.4.3	Bitwise Addition with Variable-Value Keystream	86
4.5	Implementation	87
4.5.1	MAC Generator	87
4.5.2	Chosen MAC Algorithm for RBS	89
4.5.3	Adapting the Chosen MAC to RBS	92
4.5.4	Encryption	94
4.5.5	Decryption	95
4.5.6	Reception/Transmission	95

4.6	Overall RBS System	98
4.7	Conclusion	98
	References	100
5	RBS Security Analysis	101
5.1	Security Model	101
5.2	Mathematical Background	102
5.3	RBS Security Against Common Attacks	104
5.3.1	Brute Force Attack	104
5.3.2	Known-Plaintext Attack	105
5.3.3	Chosen-Plaintext Attack	105
5.3.4	Chosen-Ciphertext Attack	106
5.3.5	Differential Attack	107
5.3.6	Substitution Attack	109
5.3.7	Related Key Attack	109
5.3.8	Linear Cryptanalysis	111
5.3.9	Algebraic Attack	112
5.3.10	Cube Attack	113
5.3.11	Side Channel Attack	113
5.4	Conclusion	115
	References	115
6	RBS Performance Evaluation	117
6.1	ASIC Implementation of RBS	118
6.2	Comparison of Ciphers	120
6.2.1	Area	123
6.2.2	Performance	125
6.2.3	Area-Time Product	131
6.2.4	Hardware Efficiency	133
6.2.5	Power	133
6.2.6	Energy	136
6.2.7	Energy-per-Bit	136
6.2.8	Trade-offs	138
6.2.9	Power-Area-Time Product	139
6.3	Conclusions	140
	References	145
7	RBS RFID Security and the Internet of Things	147
7.1	RBS Characterizing Features	148
7.2	RBS Future Extensions	149
7.3	The Internet of Things (IoT)	150
7.3.1	IoT History	151
7.3.2	IoT Challenges	153
7.3.3	Applications	154

7.4	RFID Systems in Internet of Things (IoT)	154
7.4.1	The Architecture of IoT Based on RFID	155
7.4.2	IoT Additional Requirements from RFID Systems	156
7.4.3	Security Issues with RFID-Based IoT Architectures	156
7.5	Integrating RFID in IoT Applications	157
7.5.1	RFID with Sensing Capabilities	157
7.5.2	Integrating RFID in Sensor Node Architectures	157
7.5.3	Integrating RFID Readers in Sensor Node Architectures ...	159
7.5.4	Mixed RFID/WSN Architecture	160
7.6	RFID-Based IoT Applications	160
7.6.1	Health Care Applications	160
7.6.2	Supply Chain Applications	161
7.6.3	Battlefield Applications	161
	References	161
	Glossary	163
	About the Authors	165
	Index	169

RFID Security

A Lightweight Paradigm

Khattab, A.; Jeddi, Z.; Amini, E.; Bayoumi, M.

2017, XXII, 171 p. 80 illus., 61 illus. in color., Hardcover

ISBN: 978-3-319-47544-8