RFID security : a lightweight paradigm /

Khattab, Ahmed
Jeddi, Zahra
Amini, Esmaeil
Bayoumi, Magdy A.

Springer,
2016

Electronic books

Monografía

Título: RFID security a lightweight paradigm Ahmed Khattab, Zahra Jeddi, Esmaeil Amini, Magdy Bayoumi

Editorial: Cham Springer 2016

Descripción física: 1 online resource (186 pages)

Mención de serie: Analog circuits and signal processing

Contenido: Preface; Acknowledgements; Contents; List of Figures; List of Tables; Part I RFID Security Preliminaries; 1 Introduction to RFID; 1.1 Automatic Identification; 1.2 RFID History and Standardization; 1.3 RFID Applications; 1.3.1 Logistics and Supply Chain Management; 1.3.2 Ticketing; 1.3.3 Health Care; 1.3.4 Security and Identification; 1.3.5 Toll Systems and Payment Applications; 1.3.6 Tacking Applications; 1.3.7 RIDF and Smart Objects; 1.4 RFID System Overview; 1.5 RFID Construction Formats; 1.6 RFID Classifications; 1.6.1 Communication Mechanism; 1.6.2 Memory; 1.6.3 Operating Frequency 1.6.4 Power Source; 1.6.4.1 Active Tags; 1.6.4.2 Semi-Passive Tags; 1.6.4.3 Passive Tags; 1.7 How Passive RFID Tags Work; 1.8 RFID Systems Advantages and Challenges; 1.8.1 Advantages of RFID Systems; 1.8.2 Challenges to RFID Systems; 1.9 Book Organization; References; 2 RFID Security Threats and Basic Solutions; 2.1 Security Attacks in RFID Systems; 2.1.1 Physical RFID Threats; 2.1.1.1 Disabling Tags; 2.1.1.2 Tag Modification; 2.1.1.3 Cloning Tags; 2.1.1.4 Reverse Engineering and Physical Exploration; 2.1.2 RFID Channel Threats; 2.1.2.1 Eavesdropping; 2.1.2.2 Snooping; 2.1.2.3 Skimming 2.1.2.4 Replay; 2.2 RFID Security Measures and Defenses; 2.2.1 Physical Solutions for RFID Privacy Protection; 2.2.1.1 Killing Tags; 2.2.1.2 Sleeping Tags; 2.2.1.3 Faraday Cage; 2.2.1.4 Blocker Tags; 2.2.1.5 Tag Relabeling; 2.2.1.6 Minimalist Cryptography; 2.2.1.7 Proxy Privacy Devices; 2.2.2 Authentication; 2.3 Concluding Remarks; References 3 Cryptography in RFID Systems; 3.1 Wireless Security Preliminaries; 3.2 Cryptography Overview; 3.2.1 Symmetric Private Key Encryption; 3.2.2 Asymmetric Public Key Encryption; 3.2.3 Hash Function; 3.3 Lightweight Cryptography; 3.4 Asymmetric Key Encryption Lightweight Cryptosystems; 3.4.1 Elliptical Curve Cryptography (ECC); 3.5 Symmetric Key Encryption Lightweight Cryptosystems; 3.5.1 Block Ciphers; 3.5.1.1 Advanced Encryption Standard (AES); 3.5.1.2 PRESENT; 3.5.2

Stream Ciphers; 3.5.2.1 Keystream; 3.5.2.2 Trivium; 3.5.2.3 Grain; 3.5.3 Hybrid Ciphers; 3.5.3.1 Hummingbird (HB) 3.6 Motivation for RBS Lightweight RFID Cryptosystems; 3.6.1 RBS Design Objectives; 3.7 Conclusion; References; Part II Lightweight RFID Redundant Bit Security; 4 RBS Cryptosystem; 4.1 Key and Number of Redundant Bits; 4.1.1 Key Space; 4.1.2 Flexibility in Security Level; 4.2 Location of Redundant Bits; 4.3 Value of Redundant Bits; 4.3.1 Message Authentication and Data Integrity; 4.3.2 Message Authentication and Redundant Bits; 4.4 Plaintext Manipulation; 4.4.1 Direct Appearance Inside the Ciphertext; 4.4.2 Bitwise Addition with a Constant-Value Keystream 4.4.3 Bitwise Addition with Variable-Value Keystream

Copyright/Depósito Legal: 962750941 962824980 963608396 963793520 964546365 967056915 967586175

ISBN: 9783319475455 electronic bk.) 3319475452 electronic bk.) 9783319475448 print) 3319475444

Materia: Radio frequency identification systems- Security measures TECHNOLOGY & ENGINEERING- Mechanical Computer architecture & logic design Imaging systems & technology Circuits & components

Autores: Khattab, Ahmed Jeddi, Zahra Amini, Esmaeil Bayoumi, Magdy A.

Enlace a formato físico adicional: Print version Khattab, Ahmed. RFID Security : A Lightweight Paradigm. Cham : Springer International Publishing, ©2016 9783319475448

Punto acceso adicional serie-Título: Analog circuits and signal processing series

---