1. Record Nr. UNINA9910817441703321

Autore	Sakiyama Kazuo <1971->
Titolo	Security of block ciphers : from algorithm design to hardware implementation / / Kazuo Sakiyama, The University of Electro-Communications, Japan, Yu Sasaki, NTT Secure Platform Laboratories, Japan, Yang Li, Nanjing University of Aeronautics and Astronautics, China
Pubbl/distr/stampa	Singapore : , : John Wiley & Sons Singapore Pte, Ltd., , 2015 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2015]
ISBN	1-118-66004-8 1-118-66002-1 1-118-66003-X
Edizione	[1st edition]
Descrizione fisica	1 online resource (312 p.)
Collana	Wiley - IEEE
Altri autori (Persone)	SasakiYu LiYang <1986 June 28->
Disciplina	005.8/2
Soggetti	Computer security - Mathematics Data encryption (Computer science) Ciphers Computer algorithms
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	-- Preface xi -- About the Authors xiii -- 1 Introduction to Block Ciphers 1 -- 1.1 Block Cipher in Cryptology 1 -- 1.1.1 Introduction 1 -- 1.1.2 Symmetric-Key Ciphers 1 -- 1.1.3 Efficient Block Cipher Design 2 -- 1.2 Boolean Function and Galois Field 3 -- 1.2.1 INV, OR, AND, and XOR Operators 3 -- 1.2.2 Galois Field 3 -- 1.2.3 Extended Binary Field and Representation of Elements 4 -- 1.3 Linear and Nonlinear Functions in Boolean Algebra 7 -- 1.3.1 Linear Functions 7 -- 1.3.2 Nonlinear Functions 7 -- 1.4 Linear and Nonlinear Functions in Block Cipher 8 -- 1.4.1 Nonlinear Layer 8 -- 1.4.2 Linear Layer 11 -- 1.4.3 Substitution-Permutation Network (SPN) 12 -- 1.5 Advanced Encryption Standard (AES) 12 -- 1.5.1 Specification of AES-128 Encryption 12 -- 1.5.2 AES-128 Decryption 19 -- 1.5.3 Specification of

Attacks 149 -- 5.1.2 Passive and Active Noninvasive Physical Attacks 151 -- 5.1.3 Cryptanalysis Compared to Side-Channel Analysis and Fault Analysis 151 -- 5.2 Basics of Side-Channel Analysis 152 -- 5.2.1 Side Channels of Digital Circuits 152 -- 5.2.2 Goal of Side-Channel Analysis 154 -- 5.2.3 General Procedures of Side-Channel Analysis 155 -- 5.2.4 Profiling versus Non-profiling Side-Channel Analysis 156 -- 5.2.5 Divide-and-Conquer Algorithm 157 -- 5.3 Side-Channel Analysis on Block Ciphers 159 -- 5.3.1 Power Consumption Measurement in Power Analysis 160 -- 5.3.2 Simple Power Analysis and Differential Power Analysis 163 -- 5.3.3 General Key Recovery Algorithm for DPA 164 -- 5.3.4 Overview of Attack Targets 169 -- 5.3.5 Single-Bit DPA Attack on AES-128 Hardware Implementations 181 -- 5.3.6 Attacks Using HW Model on AES-128 Hardware Implementations 186 -- 5.3.7 Attacks Using HD Model on AES-128 Hardware Implementations 192 -- 5.3.8 Attacks with Collision Model + 199 -- 5.4 Basics of Fault Analysis 203 -- 5.4.1 Faults Caused by Setup-Time Violations 205 -- 5.4.2 Faults Caused by Data Alternation 208 -- 5.5 Fault Analysis on Block Ciphers 208 -- 5.5.1 Differential Fault Analysis 208 -- 5.5.2 Fault Sensitivity Analysis + 215 -- Acknowledgment 223 -- Bibliography 223 -- 6 Advanced Fault Analysis with Techniques from Cryptanalysis 225 -- 6.1 Optimized Differential Fault Analysis 226 -- 6.1.1 Relaxing Fault Model 226 -- 6.1.2 Four Classes of Faulty Byte Positions 227. 6.1.3 Recovering Subkey Candidates of sk10 228 -- 6.1.4 Attack Procedure 230 -- 6.1.5 Probabilistic Fault Injection 231 -- 6.1.6 Optimized DFA with the MixColumns Operation in the Last Round + 232 -- 6.1.7 Countermeasures against DFA and Motivation of Advanced DFA 236 -- 6.2 Impossible Differential Fault Analysis 237 -- 6.2.1 Fault Model 238 -- 6.2.2 Impossible DFA with Unknown Faulty Byte Positions 238 -- 6.2.3 Impossible DFA with Fixed Faulty Byte Position 244 -- 6.3 Integral Differential Fault Analysis 245 -- 6.3.1 Fault Model 246 -- 6.3.2 Integral DFA with Bit-Fault Model 247 -- 6.3.3 Integral DFA with Random Byte-Fault Model 251 -- 6.3.4 Integral DFA with Noisy Random Byte-Fault Model + 254 -- 6.4 Meet-in-the-Middle Fault Analysis 260 -- 6.4.1 Meet-in-the-Middle Attack on Block Ciphers 260 -- 6.4.2 Meet-in-the-Middle Attack for Differential Fault Analysis 263 -- Further Reading 268 -- 7 Countermeasures against Side-Channel Analysis and Fault Analysis 269 -- 7.1 Logic-Level Hiding Countermeasures 269 -- 7.1.1 Overview of Hiding Countermeasure with WDDL Technique 270 -- 7.1.2 WDDL-NAND Gate 272 -- 7.1.3 WDDL-NOR and WDDL-INV Gates 273 -- 7.1.4 Precharge Logic for WDDL Technique 273 -- 7.1.5 Intrinsic Fault Detection Mechanism of WDDL 276 -- 7.2 Logic-Level Masking Countermeasures 277 -- 7.2.1 Overview of Masking Countermeasure 277 -- 7.2.2 Operations on Values with Boolean Masking 278 -- 7.2.3 Re-masking and Unmasking 278 -- 7.2.4 Masked AND Gate 279 -- 7.2.5 Random Switching Logic 281 -- 7.2.6 Threshold Implementation 283 -- 7.3 Higher Level Countermeasures 285 -- 7.3.1 Algorithm-Level Countermeasures 286 -- 7.3.2 Architecture-Level Countermeasures 289 -- 7.3.3 Protocol-Level Countermeasure 290 -- Bibliography 291 -- Index 293.

Sommario/riassunto

A comprehensive evaluation of information security analysis spanning the intersection of cryptanalysis and side-channel analysisWritten by authors known within the academic cryptography community, this book presents the latest developments in current researchUnique in its combination of both algorithmic-level design and hardware-level implementation; this all-round approach - algorithm to implementation - covers security from start to completionDeals with AES (Advanced Encryption standard), one of the most used symmetric-key ciphers, which helps the reader to learn the fundamental theory of cr

2. Record Nr. UNINA9911019090903321

Autore	Sun Haijian
Titolo	5G and Beyond Wireless Communication Networks
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2023 ©2023
ISBN	9781119089490 1119089492 9781119089469 1119089468
Edizione	[1st ed.]
Descrizione fisica	1 online resource (211 pages)
Collana	IEEE Press Series
Altri autori (Persone)	HuRose Qingyang QianYi
Disciplina	621.38456
Soggetti	5G mobile communication systems Wireless communication systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- About the Authors -- Preface -- Acknowledgments -- Chapter 1 Introduction to 5G and Beyond Network -- 1.1 5G and Beyond System Requirements -- 1.1.1 Technical Challenges -- 1.2 Enabling Technologies -- 1.2.1 5G New Radio -- 1.2.1.1 Nonorthogonal Multiple Access (NOMA) -- 1.2.1.2 Channel Codes -- 1.2.1.3 Massive MIMO -- 1.2.1.4 Other 5G NR Techniques -- 1.2.2 Mobile Edge Computing (MEC) -- 1.2.3 Hybrid and Heterogeneous Communication Architecture for Pervasive IoTs -- 1.3 Book Outline -- Chapter 2 5G Wireless Networks with Underlaid D2D Communications -- 2.1 Background -- 2.1.1 MUMIMO -- 2.1.2 D2D Communication -- 2.1.3 MUMIMO and D2D in 5G -- 2.2 NOMAAided Network with Underlaid D2D -- 2.3 NOMA with SIC and Problem Formation -- 2.3.1 NOMA with SIC -- 2.3.2 Problem Formation -- 2.4 Precoding and User Grouping Algorithm -- 2.4.1 ZeroForcing Beamforming -- 2.4.1.1 First ZF Precoding -- 2.4.1.2 Second ZF Precoding -- 2.4.2 User Grouping and Optimal Power Allocation -- 2.4.2.1 First ZF Precoding -- 2.4.2.2 Second ZF Precoding -- 2.5 Numerical Results -- 2.6 Summary -- Chapter 3 5G NOMAEnabled

Wireless Networks -- 3.1 Background -- 3.2 Error Propagation in NOMA -- 3.3 SIC and Problem Formulation -- 3.3.1 SIC with Error Propagation -- 3.3.2 Problem Formation -- 3.4 Precoding and Power Allocation -- 3.4.1 Precoding Design -- 3.4.2 Case Studies for Power Allocation -- 3.4.2.1 Case I -- 3.4.2.2 Case II -- 3.5 Numerical Results -- 3.6 Summary -- Chapter 4 NOMA in Relay and IoT for 5G Wireless Networks -- 4.1 Outage Probability Study in a NOMA Relay System -- 4.1.1 Background -- 4.1.2 System Model -- 4.1.2.1 NOMA Cooperative Scheme -- 4.1.2.2 NOMA TDMA Scheme -- 4.1.3 Outage Probability Analysis -- 4.1.3.1 Outage Probability in NOMA Cooperative Scheme -- 4.1.4 Outage Probability in NOMA TDMA Scheme.
4.1.5 Outage Probability with Error Propagation in SIC -- 4.1.5.1 Outage Probability in NOMA Cooperative Scheme with EP -- 4.1.5.2 Outage Probability in NOMA TDMA Scheme with EP -- 4.1.6 Numerical Results -- 4.2 NOMA in a mmWaveBased IoT Wireless System with SWIPT -- 4.2.1 Introduction -- 4.2.2 System Model -- 4.2.2.1 Phase 1 Transmission -- 4.2.2.2 Phase 2 Transmission -- 4.2.3 Outage Analysis -- 4.2.3.1 UE 1 Outage Probability -- 4.2.3.2 UE 2 Outage Probability -- 4.2.3.3 Outage at High SNR -- 4.2.3.4 Diversity Analysis for UE 2 -- 4.2.4 Numerical Results -- 4.2.5 Summary -- Chapter 5 Robust Beamforming in NOMA Cognitive Radio Networks: Bounded CSI -- 5.1 Background -- 5.1.1 Related Work and Motivation -- 5.1.1.1 Linear EH Model -- 5.1.1.2 Nonlinear EH Model -- 5.1.2 Contributions -- 5.2 System and Energy Harvesting Models -- 5.2.1 System Model -- 5.2.2 Nonlinear EH Model -- 5.2.3 Bounded CSI Error Model -- 5.2.3.1 NOMA Transmission -- 5.3 Power MinimizationBased Problem Formulation -- 5.3.1 Problem Formulation -- 5.3.2 Matrix Decomposition -- 5.4 Maximum Harvested Energy Problem Formulation -- 5.4.1 Complexity Analysis -- 5.5 Numerical Results -- 5.5.1 Power Minimization Problem -- 5.5.2 Energy Harvesting Maximization Problem -- 5.6 Summary -- Chapter 6 Robust Beamforming in NOMA Cognitive Radio Networks: Gaussian CSI -- 6.1 Gaussian CSI Error Model -- 6.2 Power MinimizationBased Problem Formulation -- 6.2.1 BernsteinType Inequality I -- 6.2.2 Bernstein Type Inequality II -- 6.3 Maximum Harvested Energy Problem Formulation -- 6.3.1 Complexity Analysis -- 6.4 Numerical Results -- 6.4.1 Power Minimization Problem -- 6.4.2 Energy Harvesting Maximization Problem -- 6.5 Summary -- Chapter 7 Mobile Edge Computing in 5G Wireless Networks -- 7.1 Background -- 7.2 System Model -- 7.2.1 Data Offloading -- 7.2.2 Local Computing.
7.3 Problem Formulation -- 7.3.1 Update pk, tk, and fk -- 7.3.2 Update Lagrange Multipliers -- 7.3.3 Update Auxiliary Variables -- 7.3.4 Complexity Analysis -- 7.4 Numerical Results -- 7.5 Summary -- Chapter 8 Toward Green MEC Offloading with Security Enhancement -- 8.1 Background -- 8.2 System Model -- 8.2.1 Secure Offloading -- 8.2.2 Local Computing -- 8.2.3 Receiving Computed Results -- 8.2.4 Computation Efficiency in MEC Systems -- 8.3 Computation Efficiency Maximization with Active Eavesdropper -- 8.3.1 SCABased Optimization Algorithm -- 8.3.2 Objective Function -- 8.3.3 Proposed Solution to P4 with given (k,k) -- 8.3.4 Update (k,k) -- 8.4 Numerical Results -- 8.5 Summary -- Chapter 9 Wireless Systems for Distributed Machine Learning -- 9.1 Background -- 9.2 System Model -- 9.2.1 FL Model Update -- 9.2.2 Gradient Quantization -- 9.2.3 Gradient Sparsification -- 9.3 FL Model Update with Adaptive NOMA Transmission -- 9.3.1 Uplink NOMA Transmission -- 9.3.2 NOMA Scheduling -- 9.3.3 Adaptive Transmission -- 9.4 Scheduling and Power Optimization -- 9.4.1 Problem Formulation -- 9.5 Scheduling Algorithm and Power Allocation -- 9.5.1 Scheduling Graph

Construction -- 9.5.2 Optimal scheduling Pattern -- 9.5.3 Power Allocation -- 9.6 Numerical Results -- 9.7 Summary -- Chapter 10 Secure Spectrum Sharing with Machine Learning: An Overview -- 10.1 Background -- 10.1.1 SS: A Brief History -- 10.1.2 Security Issues in SS -- 10.2 MLBased Methodologies for SS -- 10.2.1 MLBased CRN -- 10.2.1.1 Spectrum Sensing -- 10.2.1.2 Spectrum Selection -- 10.2.1.3 Spectrum Access -- 10.2.1.4 Spectrum Handoff -- 10.2.2 Database Assisted SS -- 10.2.2.1 MLBased EZ Optimization -- 10.2.2.2 Incumbent Detection -- 10.2.2.3 Channel Selection and Transaction -- 10.2.3 MLBased LTEU/LTELAA -- 10.2.3.1 MLBased LBT Methods -- 10.2.3.2 MLBased Duty Cycle Methods.
10.2.3.3 GameTheoryBased Methods -- 10.2.3.4 Distributed AlgorithmBased Methods -- 10.2.4 Ambient Backscatter Networks -- 10.2.4.1 Information Extraction -- 10.2.4.2 Operating Mode Selection and User Coordination -- 10.2.4.3 AmBCCR Methods -- 10.3 Summary -- Chapter 11 Secure Spectrum Sharing with Machine Learning: Methodologies -- 11.1 Security Concerns in SS -- 11.1.1 Primary User Emulation Attack -- 11.1.2 Spectrum Sensing Data Falsification Attack -- 11.1.3 Jamming Attacks -- 11.1.4 Intercept/Eavesdrop -- 11.1.5 Privacy Issues in DatabaseAssisted SS Systems -- 11.2 MLAssisted Secure SS -- 11.2.1 StateoftheArt Methods of Defense Against PUE Attack -- 11.2.1.1 MLBased Detection Methods -- 11.2.1.2 Robust Detection Methods -- 11.2.1.3 MLBased Attack Methods -- 11.2.2 StateoftheArt Methods of Defense Against SSDF Attack -- 11.2.2.1 Outlier Detection Methods -- 11.2.2.2 ReputationBased Detection Methods -- 11.2.2.3 SSDF and PUE Combination Attacks -- 11.2.3 StateoftheArt Methods of Defense Against Jamming Attacks -- 11.2.3.1 MLBased AntiJamming Methods -- 11.2.3.2 Attacker Enhanced AntiJamming Methods -- 11.2.3.3 AmBC Empowered Anti Jamming Methods -- 11.2.4 StateoftheArt Methods of Defense Against Intercept/Eavesdrop -- 11.2.4.1 RLBased AntiEavesdropping Methods -- 11.2.5 StateoftheArt MLBased Privacy Protection Methods -- 11.2.5.1 Privacy Protection for PUs in SS Networks -- 11.2.5.2 Privacy Protection for SUs in SS Networks -- 11.2.5.3 Privacy Protection for ML Algorithms -- 11.3 Summary -- Chapter 12 Open Issues and Future Directions for 5G and Beyond Wireless Networks -- 12.1 Joint Communication and Sensing -- 12.2 SpaceAirGround Communication -- 12.3 Semantic Communication -- 12.4 DataDriven Communication System Design -- Appendix A Proof of Theorem 5.1 -- Bibliography -- Index -- EULA.

Sommario/riassunto

This book delves into the advancements and challenges of 5G and beyond wireless communication networks. It covers a range of topics including new radio technologies, massive MIMO, and non-orthogonal multiple access. The book also explores device-to-device communications, mobile edge computing, and secure spectrum sharing with machine learning. It is aimed at researchers, practitioners, and students in the field of electrical and computer engineering, providing insights into the future directions and potential applications of wireless networks. The authors, Haijian Sun, Rose Qingyang Hu, and Yi Qian, bring expertise from academia to discuss the technical requirements and enabling technologies for next-generation networks.