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

AES-192 and AES-256 20 -- 1.5.4 Notations to Describe AES-128 23 -- Further Reading 25 -- 2 Introduction to Digital Circuits 27 -- 2.1 Basics of Modern Digital Circuits 27 -- 2.1.1 Digital Circuit Design Method 27 -- 2.1.2 Synchronous-Style Design Flow 27 -- 2.1.3 Hierarchy in Digital Circuit Design 29 -- 2.2 Classification of Signals in Digital Circuits 29 -- 2.2.1 Clock Signal 29 -- 2.2.2 Reset Signal 30 -- 2.2.3 Data Signal 31 -- 2.3 Basics of Digital Logics and Functional Modules 31 -- 2.3.1 Combinatorial Logics 31 -- 2.3.2 Sequential Logics 32 -- 2.3.3 Controller and Datapath Modules 36 -- 2.4 Memory Modules 40 -- 2.4.1 Single-Port SRAM 40 -- 2.4.2 Register File 41 -- 2.5 Signal Delay and Timing Analysis 42 -- 2.5.1 Signal Delay 42 -- 2.5.2 Static Timing Analysis and Dynamic Timing Analysis 45 -- 2.6 Cost and Performance of Digital Circuits 47 -- 2.6.1 Area Cost 47 -- 2.6.2 Latency and Throughput 47 -- Further Reading 48 -- 3 Hardware Implementations for Block Ciphers 49 -- 3.1 Parallel Architecture 49 -- 3.1.1 Comparison between Serial and Parallel Architectures 49 -- 3.1.2 Algorithm Optimization for Parallel Architectures 50 -- 3.2 Loop Architecture 51 -- 3.2.1 Straightforward (Loop-Unrolled) Architecture 51.
3.2.2 Basic Loop Architecture 53 -- 3.3 Pipeline Architecture 55 -- 3.3.1 Pipeline Architecture for Block Ciphers 55 -- 3.3.2 Advanced Pipeline Architecture for Block Ciphers 56 -- 3.4 AES Hardware Implementations 58 -- 3.4.1 Straightforward Implementation for AES-128 58 -- 3.4.2 Loop Architecture for AES-128 61 -- 3.4.3 Pipeline Architecture for AES-128 65 -- 3.4.4 Compact Architecture for AES-128 66 -- Further Reading 67 -- 4 Cryptanalysis on Block Ciphers 69 -- 4.1 Basics of Cryptanalysis 69 -- 4.1.1 Block Ciphers 69 -- 4.1.2 Security of Block Ciphers 70 -- 4.1.3 Attack Models 71 -- 4.1.4 Complexity of Cryptanalysis 73 -- 4.1.5 Generic Attacks 74 -- 4.1.6 Goal of Shortcut Attacks (Cryptanalysis) 77 -- 4.2 Differential Cryptanalysis 78 -- 4.2.1 Basic Concept and Definition 78 -- 4.2.2 Motivation of Differential Cryptanalysis 79 -- 4.2.3 Probability of Differential Propagation 80 -- 4.2.4 Deterministic Differential Propagation in Linear Computations 83 -- 4.2.5 Probabilistic Differential Propagation in Nonlinear Computations 86 -- 4.2.6 Probability of Differential Propagation for Multiple Rounds 89 -- 4.2.7 Differential Characteristic for AES Reduced to Three Rounds 91 -- 4.2.8 Distinguishing Attack with Differential Characteristic 93 -- 4.2.9 Key Recovery Attack after Differential Characteristic 95 -- 4.2.10 Basic Differential Cryptanalysis for Four-Round AES + 96 -- 4.2.11 Advanced Differential Cryptanalysis for Four-Round AES + 103 -- 4.2.12 Preventing Differential Cryptanalysis + 106 -- 4.3 Impossible Differential Cryptanalysis 110 -- 4.3.1 Basic Concept and Definition 110 -- 4.3.2 Impossible Differential Characteristic for 3.5-round AES 111 -- 4.3.3 Key Recovery Attacks for Five-Round AES 114 -- 4.3.4 Key Recovery Attacks for Seven-Round AES + 123 -- 4.4 Integral Cryptanalysis 131 -- 4.4.1 Basic Concept 131 -- 4.4.2 Processing P through Subkey XOR 132 -- 4.4.3 Processing P through SubBytes Operation 133 -- 4.4.4 Processing P through ShiftRows Operation 134 -- 4.4.5 Processing P through MixColumns Operation 134.
4.4.6 Integral Property of AES Reduced to 2.5 Rounds 135 -- 4.4.7 Balanced Property 136 -- 4.4.8 Integral Property of AES Reduced to Three Rounds and Distinguishing Attack 137 -- 4.4.9 Key Recovery Attack with Integral Cryptanalysis for Five Rounds 139 -- 4.4.10 Higher-Order Integral Property + 141 -- 4.4.11 Key Recovery Attack with Integral Cryptanalysis for Six Rounds + 143 -- Further Reading 147 -- 5 Side-Channel Analysis and Fault Analysis on Block Ciphers 149 -- 5.1 Introduction 149 -- 5.1.1 Intrusion Degree of Physical

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