Computer Architecture and Design Methodologies

Series Editors

Anupam Chattopadhyay, Nanyang Technological University, Singapore, Singapore

Soumitra Kumar Nandy, Indian Institute of Science, Bangalore, India

Jürgen Teich, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Erlangen, Germany

Debdeep Mukhopadhyay, Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, India

Twilight zone of Moore's law is affecting computer architecture design like never before. The strongest impact on computer architecture is perhaps the move from unicore to multicore architectures, represented by commodity architectures like general purpose graphics processing units (gpgpus). Besides that, deep impact of application-specific constraints from emerging embedded applications is presenting designers with new, energy-efficient architectures like heterogeneous multi-core, accelerator-rich System-on-Chip (SoC). These effects together with the security, reliability, thermal and manufacturability challenges of nanoscale technologies are forcing computing platforms to move towards innovative solutions. Finally, the emergence of technologies beyond conventional charge-based computing has led to a series of radical new architectures and design methodologies.

The aim of this book series is to capture these diverse, emerging architectural innovations as well as the corresponding design methodologies. The scope covers the following.

- Heterogeneous multi-core SoC and their design methodology
- Domain-specific architectures and their design methodology
- Novel technology constraints, such as security, fault-tolerance and their impact on architecture design
- Novel technologies, such as resistive memory, and their impact on architecture design
- Extremely parallel architectures

More information about this series at https://link.springer.com/bookseries/15213

Anubhab Baksi

Classical and Physical Security of Symmetric Key Cryptographic Algorithms

Springer

Anubhab Baksi
Temasek Laboratories
Nanyang Technological University
Singapore, Singapore

ISSN 2367-3478 ISSN 2367-3486 (electronic)
Computer Architecture and Design Methodologies
ISBN 978-981-16-6521-9 ISBN 978-981-16-6522-6 (eBook)
https://doi.org/10.1007/978-981-16-6522-6

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

About This Book

Symmetric key cryptography is one of the cornerstones of security in the modern era of electronic communication. The symmetric key algorithms, known as the ciphers, are to satisfy certain requirements in order to be considered secure, which are broadly classified as classical attack and physical attack. We show new results in context of both the classical and physical attacks to advance the state of the art.

In classical attack, we first show an issue related to a common modelling using Mixed Integer Linear Programming (MILP). We provide a new MILP modelling that overcomes this issue and explores heuristic options to reduce the solution time taken by the MILP solver. Our analysis shows that the solution time can be improved nearly ten-folds by using a proper heuristic. Second, we show how Machine Learning (ML) can be used as a generic tool in the analysis of the symmetric key ciphers. In the process, we demonstrate how the existing security notions (that do not use ML) underestimate the vulnerability of the ciphers. To the best of our knowledge, this is the first generic application of ML in this field.

In physical attack, we start with new mathematical results related to the Differential Fault Attack (DFA) from the point of view of the cipher designer. Next, we make use of these results to propose a cipher named DeFault, which has an in-built resistance against DFA. While all other methods to thwart DFA rely on some form of duplication, DeFault has an inherent protection against DFA that does not use duplication and hence is the first of its kind. Third, we analyse the so-called infective countermeasure that is used as a duplication-based DFA countermeasure in more depth. We construct new schemes, show weakness of an existing scheme, and propose a simple patch to another scheme to fix its weakness, among other results. Last, we propose a low-cost countermeasure to a newly proposed fault model, named Statistical Ineffective Fault analysis (SIFA). In contrast to the existing SIFA countermeasures that rely on some form of triplication at its core, our countermeasure uses duplication and thus is the most cost-effective.

Contents

1 Introduction 1
1.1 Context and Motivation 1
1.2 Research Directions 3
1.2.1 Cipher Design and Classical Cryptanalysis 3
1.2.2 Realization/Mapping 5
1.2.3 Physical Attack and Countermeasure 5
1.3 Standardization of Ciphers 6
1.4 Organization 7
References 10

2 Fundamentals of Symmetric Key Cryptography 13
2.1 Building Blocks 13
2.1.1 Boolean Function 13
2.1.2 Substitution Box (SBox) 14
2.1.3 Linear Layer 19
2.2 Primitives 19
2.2.1 (Un-keyed) Permutation 19
2.2.2 Block Cipher 20
2.2.3 Stream Cipher 21
2.2.4 Hash Function 22
2.2.5 Message Authentication Code (MAC) 24
2.2.6 Authenticated Encryption with Associated Data (AEAD) 25
2.3 Cipher Families 26
2.3.1 Substitution Permutation Network (SPN) 26
2.3.2 Feistel Network 27
2.3.3 Add–Rotation–XOR (ARX) Construction 29
2.4 Description of Exemplary Ciphers 30
2.4.1 ADVANCED ENCRYPTION STANDARD (AES) 30
2.4.2 PRESENT-80 33
2.4.3 GIFT-128 35

2.4.4 CHASKEY 36
2.5 Formidability of the Attacker 39
2.5.1 Conventional Notions of Security 39
2.5.2 Power of the Attacker 39
2.5.3 Objective of the Attacker 40
2.6 Major Classical Attacks 42
2.6.1 Differential Attack 42
2.6.2 Linear Attack 44
2.6.3 Algebraic Attack 44
2.6.4 Integral/Cube Attack 46
2.6.5 Impossible Differential Attack 47
2.7 Device Implementation 47
2.8 Additional Topics 49
2.8.1 Black Box–Grey Box–White Box Models 49
2.8.2 Mixed Integer Linear Programming (MILP) 50
2.8.3 Machine Learning (ML) 51
2.8.4 Competitions 54
References 55

3 Fault Attack 59
3.1 Introduction 59
3.2 Fault Models 60
3.2.1 Precise Bit Flip 60
3.2.2 Single/Multiple Fault Adversary 60
3.2.3 Random/Deterministic Fault Model 61
3.2.4 Information Theoretic View 61
3.2.5 Other Aspects 61
3.3 Data Alteration Methods 62
3.3.1 Volatility 62
3.3.2 Modification of Operation 62
3.3.3 Modification of Operand 63
3.4 Sources of Fault Injection 65
3.5 Analysis Methods 68
3.5.1 Difference-Based Fault Analysis 69
3.5.2 Collision-Based Fault Analysis 76
3.5.3 Statistics-Based Fault Analysis 77
3.5.4 Others 80
3.6 Generalized Fault Attack Automation Frameworks 81
3.6.1 Cipher Level Approaches 81
3.6.2 Implementation Level Approaches 82
3.7 Countermeasures 82
3.7.1 Detection 84
3.7.2 Infection 85
3.7.3 Prevention 86

3.7.4 Re-keying, Tweak and Tweak-in-Plaintext, Masking Plaintext 86
3.7.5 Attacks on Countermeasures 87
3.7.6 Specialized Countermeasures Against Statistical Ineffective Fault Attack 88
References 89

4 Side Channel Attack 99
4.1 Introduction and Background 99
4.2 Power Analysis 101
4.2.1 Simple Power Analysis 102
4.2.2 Differential Power Analysis (DPA) 102
4.2.3 Template Attack 103
4.2.4 Correlation Power Analysis (CPA) 103
4.2.5 Countermeasures 103
4.3 Case Study: Side Channel Analysis of CHASKEY 104
4.3.1 Practical Attack Setups 104
4.3.2 Experimental Results 105
References 107

5 New Insights on Differential and Linear Bounds Using Mixed Integer Linear Programming 109
5.1 Introduction 110
5.2 Background 111
5.2.1 Branch Number to Model SBox (Inscrypt'11) 112
5.2.2 Convex Hull to Model SBox—Active SBox Count (Eprint'13) 113
5.2.3 Convex Hull to Model SBox—Exact Bound (Eprint'14) 115
5.2.4 Redundant Constraints to Reduce Solution Time (Eprint'19) 116
5.3 Problem with Convex Hull Modelling 116
5.4 Automated Bounds with MILP: Our Proposal 121
5.4.1 Modelling 122
5.4.2 Optimizations 123
5.4.3 Results 126
5.5 Conclusion 131
5.6 Supplementary Discussion 132
5.6.1 Detailed Description on MILP Modelling of XOR 132
5.6.2 Illustration with MILP Model for 1-Round Differential Bound for GIFT-128 133
5.6.3 Illustration with MILP Model of Previous Constraints for 4-Round Differential Bound for GIFT-128 133
References 139

6 Machine Learning-Assisted Differential Distinguishers for Lightweight Ciphers 141
6.1 Introduction 142
6.2 Background 144
6.2.1 Markov Ciphers 144
6.2.2 Gohr's Work on SPECK (CRYPTO'19) 146
6.3 Basic Description of the Ciphers 147
6.3.1 GIMLI 147
6.3.2 ASCON 149
6.3.3 KNOT 149
6.4 Machine Learning-Based Distinguishers 150
6.4.1 Model 1: Multiple Input Differences 150
6.4.2 Model 2: One Input Difference 153
6.4.3 Comparison with Existing Models 154
6.5 Results on Round-Reduced Ciphers 154
6.5.1 GIMLI (Model 1) 154
6.5.2 ASCON and KNOT (Model 1) 156
6.5.3 CHASKEY (Model 2) 157
6.6 Choice of Machine Learning Model 157
6.7 Conclusion and Follow-Up Problems 159
References 161

7 Differential Paradox: How an SBox Plays Against Differential Fault Analysis 163
7.1 Introduction 163
7.2 Difference Distribution Table-Related Properties 164
7.3 Characterizing SBoxes in View of DFA 167
7.4 Implication of Our Analysis and Future Work 174
References 175

8 DEFAULT: Cipher-Level Resistance Against Differential Fault Attack 177
8.1 Introduction 177
8.2 Background 180
8.2.1 DFA Models 180
8.2.2 DFA Protection 181
8.2.3 Feasibility of Cipher-Level Protection Against Faults 182
8.2.4 Working Principle for DFA 184
8.3 Construction of DFA-Resistant Layer/Cipher 185
8.3.1 Ad-hoc DFA Protection to Any Cipher (DEFAULT-LAYER) 185
8.3.2 Extension to a Full-Fledged Cipher (DEFAULT) 186
8.3.3 Construction of DEFAULT-LAYER 187
8.3.4 Construction of DEFAULT-CORE (and DEFAULT) 189

8.4 Design Rationale 191
- 8.4.1 Design Philosophy 191
- 8.4.2 Structure of the DEFAULT PermBits 193
- 8.4.3 Selection of the DEFAULT SBoxes 194
- 8.4.4 Unbiased Linear Structures 197

8.5 Security Analysis 198
- 8.5.1 Protection Against Differential Fault Attack 199
- 8.5.2 Protection Against Classical Cryptanalysis 201
- 8.5.3 Protection Against Side Channels Attacks 203

8.6 Automated Bounds for Differential and Linear Attacks 204

8.7 Performance 206
- 8.7.1 Hardware Benchmark 206
- 8.7.2 Software Benchmark 207

8.8 Conclusion 208

8.9 Supplementary Discussion 210

References 214

9 To Infect or Not to Infect: A Critical Analysis of Infective Countermeasures in Fault Attacks 217

9.1 Introduction 217

9.2 Background 220
- 9.2.1 Context of Differential Fault Analysis 220
- 9.2.2 Early Countermeasures: Detection-Based 220
- 9.2.3 Evolution of Infective Countermeasures 221
- 9.2.4 Notations and Terminologies 222
- 9.2.5 Necessity and Sufficiency of Randomness 226
- 9.2.6 Scope and Applicability 226
- 9.2.7 Connection with Side Channel Countermeasures 229

9.3 Type I Constructions 230
- 9.3.1 Multiplication-Based Constructions 230
- 9.3.2 Derivative-Based Constructions 231
- 9.3.3 New Type I Schemes 231
- 9.3.4 Benchmarking Results for Type I Schemes 235

9.4 Type II/Cipher-Level Constructions 237
- 9.4.1 Critical Look at CHES'14 Countermeasure 241
- 9.4.2 Our Patch for LatinCrypt'12 Countermeasure 243

9.5 Conclusion 249

References 250

10 A Novel Duplication-Based Countermeasure to Statistical Ineffective Fault Analysis 255

10.1 Introduction 255

10.2 Fault Attack Preliminaries 258
- 10.2.1 Differential Fault Attack (DFA) 258
- 10.2.2 General Countermeasures Against Fault Attacks 258

10.3 Statistical Ineffective Fault Attack (SIFA) 259

10.3.1 Duplication-Based Countermeasures and Need for Specialization 259
10.3.2 Existing SIFA Countermeasures 261
10.4 Our Proposed Solution 262
10.4.1 Adopting Inverted Logic to Symmetric Key Ciphers 265
10.4.2 Benchmarks 268
10.4.3 Evaluation 269
10.4.4 Comparison with Existing Countermeasures 269
10.4.5 Connection with Side Channel Countermeasures 272
10.5 Conclusion 272
References 273

11 Concluding Remarks 277
11.1 Synopsis 277
11.2 Interesting Problems for Future Research 279
References 281

Index 283