Side-Channel Analysis of Embedded Systems

Maamar Ouladj • Sylvain Guilley

Side-Channel Analysis of Embedded Systems

An Efficient Algorithmic Approach

Springer

Maamar Ouladj
Paris 8 University
Paris, France

Sylvain Guilley
Secure-IC, S.A.S.
Paris, France

ISBN 978-3-030-77221-5 ISBN 978-3-030-77222-2 (eBook)
https://doi.org/10.1007/978-3-030-77222-2

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1 General Introduction 1
References 4

Part I Classical Side-Channel Attacks

2 Foundations of Side-Channel Attacks 9
2.1 Notations 9
2.2 General Framework for Side-Channel Attacks 10
2.3 Leakage Models 11
2.3.1 Hamming Weight Leakage Model 11
2.3.2 Hamming Distance Leakage Model 11
2.3.3 The Unevenly Weighted Sum of the Bits (UWSB) Leakage Model 12
2.3.4 Polynomial Leakage Model 12
2.3.5 Leakage Model in Profiled SCA 13
2.4 SCA Security Metrics 13
2.4.1 Success Rate (SR) 13
2.4.2 Guessing Entropy (GE) 13
2.4.3 Signal-to-Noise Ratio (SNR) 13
2.4.4 Normalized Inter-Class Variance (NICV) 14
2.4.5 Information Theory Metric 14
2.4.6 Metrics in Machine Learning 15
2.4.7 Relation Between the Security Metrics 15
2.5 Pre-processing of the Leakage Traces for SCA 15
2.5.1 Traces Synchronization 16
2.5.2 Noise Filtering 16
2.5.3 Points-of-Interest (PoI) Selection 16
2.5.4 Dimensionality Reduction 17
References 17

3 Side-Channel Distinguishers 21
3.1 SCA Distinguishers Classification 21
3.2 First-Order Distinguishers 22

3.2.1 Simple Power Analysis (SPA) . . . 22
3.2.2 Differential Power Analysis (DPA) . . . 22
3.2.3 Correlation Power Analysis (CPA) . . . 23
3.2.4 Rank-Based CPAs . . . 24
3.2.5 Covariance-Based Distinguisher . . . 24
3.2.6 Collision Side-Channel Attacks . . . 24
3.2.7 Mutual Information Analysis (MIA) . . . 25
3.2.8 Kolmogorov-Smirnov Distance (KS)-Based Distinguisher . . . 25
3.2.9 Chi-Squared Test (Chi-2-Test)-Based Distinguisher . . . 26
3.2.10 Template Attack (TA) . . . 26
3.2.11 Linear Regression-Based Side-Channel Attacks (LRA) . . . 27
3.2.12 Machine Learning-Based Distinguishers . . . 27
3.3 Higher Order Distinguishers . . . 27
3.3.1 Higher Order Distinguishers Overs Combination . . . 28
3.3.2 Higher Order Distinguishers Without a Prerequisite Combination . . . 28
3.4 Comparison of Distinguishers . . . 30
References . . . 31

4 SCA Countermeasures . . . 35
4.1 Hiding . . . 35
4.1.1 Hiding on the Time Dimension . . . 36
4.1.2 Hiding on the Amplitude Dimension . . . 36
4.2 Masking Countermeasure . . . 37
4.2.1 Boolean Masking (BM) . . . 38
4.2.2 Multiplicative Masking (MM) . . . 39
4.2.3 Affine Masking (AfM) . . . 39
4.2.4 Arithmetic Masking (ArM) . . . 39
4.2.5 Polynomials-Based Masking (PM) . . . 40
4.2.6 Leakage Squeezing Masking (LSM) . . . 40
4.2.7 Rotating S-Boxes Masking (RSM) . . . 40
4.2.8 Inner Product Masking (IPM) . . . 40
4.2.9 Direct Sum Masking (DSM) . . . 41
4.2.10 Comparison Between Masking Schemes . . . 42
4.3 Combination of Countermeasures . . . 42
References . . . 42

Part II Spectral Approach in Side-Channel Attacks

5 Spectral Approach to Speed up the Processing 49
5.1 Walsh-Hadamard Transformation to Speed Up Convolution Computation 49
5.2 Convolution Product 49
5.3 Extension of the Spectral Approach to the Higher Order 50
5.4 Conclusion 52
Reference 52

6 Generalized Spectral Approach to Speed up the Correlation Power Analysis 53
6.1 Introduction 53
6.1.1 Outline 54
6.2 CPA's Preliminaries 54
6.2.1 Target of the Attack 54
6.3 Carrying Out the CPA, with Arbitrary Set of Messages, According to the Spectral Approach 55
6.3.1 Incremental CPA Computation 58
6.4 Extension of the Improvements to the Protected Implementations by Masking 60
6.5 Experiments 60
6.6 Conclusion 61
References 62

Part III Coalescence-based Side-Channel Attacks

7 Coalescence Principle 67
7.1 Difference Between SCAs with and Without Coalescence 67
7.2 Optimization of the Stochastic Collision Attack Thanks to the Coalescence 70
7.2.1 Preliminaries 70
7.2.2 New Concept of Stochastic Collision Distinguisher . . . 71
7.2.3 Main Result 74
7.3 Conclusion 76
References 77

8 Linear Regression Analysis with Coalescence Principle 79
8.1 Introduction 79
8.1.1 State-of-the-Art's Review 79
8.1.2 Contributions 80
8.1.3 Outline 81
8.2 Mathematical Modelization 81
8.2.1 Description of Stochastic Attacks 81

8.3 LRA Study and Improvements of Its Implementation 84
8.3.1 LRA with Assumption of Equal Images Under different Subkeys (EIS) 84
8.3.2 Spectral Approach Computation to Speed up LRA (with EIS) 86
8.3.3 Further Improvement 87
8.3.4 Incremental Implementation of LRA 92
8.4 Extension of the Improvements to the Protected Implementations by Masking 92
8.4.1 Normalized Product Combination Against Arithmetic Masking 93
8.5 Experiments 94
8.5.1 LRA with and Without Spectral Approach 94
8.5.2 SCAs with and Without Coalescence 95
8.5.3 LRA Against Higher Order Masking 95
8.6 Conclusion and Perspectives 97
References 98

9 Template Attack with Coalescence Principle 101
9.1 Introduction 101
9.1.1 Context: The Side-Channel Threat 101
9.1.2 Problem: Making the Most of High Dimensionality . . . 101
9.1.3 State-of-the-Art 102
9.1.4 Contributions 103
9.1.5 Outline 104
9.2 Mathematical Modelization of the Problem and Notations 104
9.2.1 Side-Channel Problem 104
9.2.2 Additional Notations 105
9.3 Formalization of Template Attacks 107
9.3.1 Template Attack (Without Coalescence) 107
9.3.2 Template Attack (With Coalescence) 109
9.3.3 State-of-the-Art Dimensionality Reduction for TA 111
9.4 Efficiently Computing Templates with Coalescence 113
9.4.1 Simplification by the Law of Large Number (LLN) . . . 113
9.4.2 Profiling and Attack Algorithms 115
9.4.3 Improved Profiling and Attack Algorithms 115
9.4.4 Extension of Our Approach to Masked Implementations 115
9.4.5 Computational Performance Analysis 119
9.5 Experiments 121
9.5.1 Traces Used for the Case Study 121
9.5.2 Template Attacks with Windows of Increasing Size . . . 123
9.5.3 Comparison with PCA 124

9.5.4 Template Attack after Dimensionality Reduction (over First Eigen-Components) . . . 125
9.5.5 Study of Our Approach with Simulated Traces . . . 126
9.6 Conclusion . . . 129
References . . . 130

10 Spectral Approach to Process the High-Order Template Attack Against any Masking Scheme . . . 133
10.1 Introduction . . . 133
10.1.1 Related Works . . . 133
10.1.2 Contributions . . . 134
10.1.3 Outline . . . 135
10.2 Preliminaries . . . 135
10.2.1 Linear Algebra and Linear Codes . . . 135
10.3 Higher Order Template Attack . . . 136
10.3.1 High-Order Boolean Masking . . . 136
10.3.2 Attack on High-Order Boolean Masking . . . 137
10.3.3 Computing the Template Profile Functions $p(X_q^{(w)}|.)$ . . . 140
10.3.4 Equivalent Multivariate Signal-to-Noise Ratio (SNR) . . . 141
10.4 Type of Fourier Transform per Masking Scheme . . . 141
10.4.1 Type of Fourier Transform for Inner Product Masking (IPM) Scheme . . . 142
10.4.2 Type of Fourier Transform for Direct Sum Masking (DSM) Scheme . . . 143
10.4.3 Multi-share DSM (MS-DSM) . . . 144
10.4.4 Type of Fourier Transform for the Polynomial DSM (PDSM) Scheme . . . 147
10.4.5 Type of Fourier Transform for the Rotating S-boxes Masking (RSM) Scheme . . . 147
10.4.6 Type of Fourier Transform for the Leakage Squeezing Masking (LSM) Scheme . . . 148
10.5 Experiments . . . 148
10.5.1 Results of High-Order Attacks on Boolean Masking . . . 148
10.5.2 Results of MS-DSM applied to PRESENT . . . 149
10.5.3 Further Improvement in Performance . . . 155
10.6 Conclusion and Perspectives . . . 155
10.6.1 Conclusion . . . 155
10.6.2 Perspectives . . . 156

10.7 Appendix: Multi-Share DSM Scheme 156
10.7.1 Incorrect Multi-Share DSM Scheme 156
10.7.2 Correct Multi-Share DSM Scheme 157
References 158