Contents

1 Introduction **1**
1.1 Preface . . . 1
1.2 Cryptography & Cybersecurity . . . 2
1.3 The Root of Security & the Chain of Security . . . 3
1.4 Side-Channel Analysis . . . 4
1.5 Side-Channel Protections . . . 5
1.5.1 Masking Schemes . . . 5
1.5.2 Generalizing to Code-based Masking . . . 6
1.6 Getting Acquainted with the Topics . . . 8
1.6.1 The Practice of Side-Channel Analysis . . . 9
1.6.2 Security Evaluations . . . 10
1.6.3 Notations and Terminologies . . . 10
1.7 Side-Channel Analyses Performance Criteria . . . 12
1.8 Overview of the Content . . . 12

2 Basics and Preliminaries **15**
2.1 Linear Codes . . . 15
2.2 Complementary Vector Spaces . . . 17
2.3 Pseudo-Boolean Functions . . . 18
2.4 Information-Theoretic Measures . . . 19

I Attacks **23**

3 Attacks on Unprotected Devices **25**
3.1 Maximum Likelihood without Masking . . . 26
3.1.1 Side-channel Analysis as a Communication Problem . . . 28
3.1.2 Optimal Attacks when the Leakage Model is Known . . . 30
3.1.3 Optimal Attacks when the Leakage Model is Partially Unknown . . . 34
3.1.4 Experimental Validation . . . 36
3.1.5 Conclusions of This Section . . . 41
3.1.6 Optimal Mono-Bit Distinguisher for Known model and Gaussian Noise . . . 42
3.1.7 Noise Distribution Resulting from Multiplication . . . 42

3.2 When are CPA and MIA Optimal? 43
3.2.1 Optimality of Mutual Information Analysis 44
3.2.2 Non-Gaussian Noise Challenge 50
3.2.3 Partially Unknown Model Challenge 53
3.2.4 Fast Computations 56
3.3 Optimal Collision Attacks 58
3.3.1 Stochastic Collision Distinguisher 64
3.3.2 The New Distinguisher in Practice 70
3.4 Kolmogorov-Smirnov Analysis (KSA) 72
3.4.1 Preliminaries 73
3.4.2 Study of Theoretical KS Distinguishers 76
3.4.3 Confusion Coefficient vs. Cryptanalytical Metrics 82
3.5 ML with Large Dimension Traces 88
3.5.1 Theoretical Solution in the Presence of Gaussian Noise . . 90
3.5.2 Examples 94
3.5.3 Comparison with PCA and LDA 97
3.5.4 Practical Validation 102
3.6 Multivariate Context 104
3.6.1 Notations and Leakage Model 106
3.6.2 Theoretical Results and Implementation 109
3.6.3 Practical Results 114
3.7 Stochastic Side-Channel Leakage Profiling 119
3.7.1 Stochastic Profiling 120
3.7.2 Orthonormalizing the Monomial Basis 123
3.7.3 Estimation of the Projection onto the Fourier Basis . . . 127
3.7.4 Application of the Results 128
3.7.5 Estimations of the Projections 129

4 Attacks on Protected Devices 133
4.1 Countermeasures and Masking 133
4.2 EM-based Attacks on Masked Implementations 134
4.2.1 Attack Scenario Description 137
4.2.2 Comparison of Various Distinguishers 139
4.2.3 Applying EM Algorithm to Side-Channel Attacks 142
4.2.4 Experimental Results on Synthetic Traces 148
4.2.5 Results on Real Traces from the DPA Contest 156
4.2.6 Discussion 159
4.3 Maximum Likelihood against Masking – Exact Results 160
4.3.1 Preliminaries 161
4.3.2 Optimal Distinguisher for Second-Order Attacks 164
4.3.3 Higher-Order Optimal Distinguisher for any Order 170
4.3.4 HOOD for Precomputation Masking Tables 173
4.3.5 More Case Studies 180
4.3.6 Algorithm of Masking Tables 181
4.4 Maximum Likelihood with Taylor Expansion 181
4.4.1 Notations 184

4.4.2 A Generic Log-Likelihood for Masked Implementations . . 186
4.4.3 Case Study: Shuffled Table Recomputation 190
4.4.4 Complexity 194
4.4.5 Simulation Results 196
4.4.6 Extra Results 199

II Evaluations 209

5 Information-Theoretic Evaluation 211
5.1 MIA and IIA 212
5.1.1 A new distinguisher based on intraclass information principle 214
5.1.2 Theoretical Analysis 218
5.1.3 Side-Channel Analysis Scenario and Soundness 222
5.1.4 Why Inter-class Information Analysis is more Discriminating than Mutual Information Analysis 225
5.1.5 Simulation Results 228
5.1.6 Comparing Side-Channel Distinguishers 229
5.1.7 Features due to the Closed-form Expression of the Success Metric 239
5.2 Cumulant Expansion of Mutual Information 242
5.2.1 Connecting Higher-order Moments with MI 242
5.2.2 Numerical Simulations 244
5.3 Alpha-Information Theory 246
5.3.1 A Primer on α-Information Theory 247
5.3.2 Fano's Inequality Applied to a Side-Channel Attack . . . 253

6 Coding-Theoretic Formalization and Evaluation 255
6.1 Introduction of Code-based Masking 255
6.1.1 Generalization of Masking 256
6.1.2 Various Instances 257
6.1.3 Tunable Linear Codes in GCBM 261
6.2 Information Leakage Quantification 263
6.2.1 Uniform Representation of Leakage Function 263
6.2.2 SNR-based Information Leakage Quantification 264
6.2.3 Simplification under Hamming Weight Model 266
6.2.4 Connecting SNR with Code Properties 268
6.2.5 Information-Theoretic Leakage Quantification 269
6.2.6 Optimal Codes for GCBM 271
6.3 Enhancing SSS-based Polynomial Masking 273
6.3.1 Further Clarifications 273
6.3.2 Representing Linear Codes in Subfield $\mathbb{F}_2$ 274
6.3.3 More Redundancy in Sharing Leaks More 274
6.3.4 Different Codes for SSS-based Masking Instances 276
6.3.5 Revisiting the Independence Condition 276

6.3.6 Comparison with Related Works 279
6.4 Constructing Best Linear Codes 282
6.4.1 Problem Clarification 283
6.4.2 Orthogonal Bases and Subfield Representations 286
6.4.3 Characterization by Weight Distribution 291
6.4.4 Discussion and Related Works 299
6.5 Quantitative Attack Evaluations against CBM 301
6.5.1 Profiling Attacks against CBM 301
6.5.2 Non-profiling Attacks against CBM 302
6.6 Detailed Proofs 302

7 Information Theoretic Bounds on the Evaluation of Attacks 307

7.1 Success Exponent 307
7.1.1 Preliminaries 309
7.1.2 Derivation of Success Exponent 312
7.1.3 Success Exponent for Few Measurements 316
7.1.4 Closed-Form Expressions of SE 317
7.1.5 Perspectives for Further Applications 324
7.1.6 Success Exponent in the Case of Masking 325
7.2 Bounds using Mutual Information 329
7.2.1 Side-Channel Seen as a Communication Channel 332
7.2.2 Theoretical Bounds on Mutual Information 335
7.2.3 Application to Additive White Gaussian Noise 341
7.2.4 Practical Applications 349
7.2.5 Link with Guessing Entropy 355
7.2.6 Proofs and Supplementary Results 357
7.3 Bounds using Conditional Alpha-Information 359
7.3.1 Conditional α-Information 360
7.3.2 Application to Side-Channel Analysis 361
7.4 Bounding Attacks on Masked Implementation 363
7.4.1 Links between MIs of Different Variables 365
7.4.2 Bounds on the Success Probability of Attack 365
Bibliography 366

List of Notations

Notations

General notations

$\mathbb{N} = \{0, 1, 2, \ldots\}$	Natural integers (positive or zero)
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$	Integers (natural integers and their opposite)
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{F}$, $\mathbb{F}_{2^\ell}$, $\mathbb{F}_p$	Finite field of order 2^ℓ or of prime order p
$w_H(x)$	Hamming weight function
$d_H(x, y)$	Hamming distance
$\|\cdot\|$	Vector space norm
$\|\cdot\|_2$	Euclidean norm
$\|\cdot\|_\alpha$	α-norm
$\mathbb{P}(E)$	Probability of an event E
$\mathbb{P}_s$	Probability of success
$\mathbb{P}_e$	Probability of error
$\mathbb{E}(X)$	Expectation of a random variable or vector X
$\mathbb{V}(X)$	Variance of random variable X
$\mathrm{Cov}(X, Y)$	Covariance between random variables X and Y
$\mathsf{H}(X)$	Shannon entropy of random variable X
$\mathsf{H}_\alpha(X)$	Rényi entropy of random variable X of order α, or α-entropy
$\mathsf{h}(X), \mathsf{h}_\alpha(X)$	Corresponding entropies of a *binary* random variable X
$\mathsf{I}(X; Y)$	Mutual information between random variables X and Y
$\mathsf{I}_\alpha(X; Y)$	α-Information between random variables X and Y
$\mathsf{D}(P\|Q)$	Divergence between probability distributions P and Q
$\mathsf{D}_\alpha(P\|Q)$	Rényi divergence between probability distributions P and Q, or α-divergence
$\mathsf{d}(p\|q), \mathsf{d}_\alpha(p\|q)$	Corresponding divergences between *binary* probability distributions p and q

Notations in side-channel analysis context

K	Secret key or subkey (e.g., one key byte)
T	Plaintext or ciphertext
X	Sensitive intermediate variable
Y	Noisy measurements, e.g., power/EM traces measured from the target device
Z	Random noise, e.g., $Z \sim \mathcal{N}(0, \sigma^2)$ for the AWGN channel
$f(X)$	Leakage function of the target device, e.g., $f(X) = w_H(X)$
$\Delta(k)$	Side-channel distinguisher for some key guess k as input
$\mathbf{M}$	Random mask
$\mathbf{X}$	Masked variables $\mathbf{X} = (X_1, X_2, \ldots, X_n)$
$\mathbf{V}$	sensitive variable for code-based masking
$\mathbf{G}$	generator matrix
$\mathbf{H}$	generator matrix of the masking code
$\mathbf{X} = \mathbf{VG} + \mathbf{MH}$	code-based masking encoding
ℓ	Bit-length of variables, e.g., subkey bytes with $\ell = 8$ or nibbles with $\ell = 4$, or single bit with $\ell = 1$
n	Number of shares in masked implementations
m	Number of random masks in secret-sharing schemes
t	Security threshold of masking schemes (masking order)
o	Statistical order of the side-channel attack or of the side-channel leakage
q, Q	Number of queries or measurements (side-channel traces)

Inner operations, useful within (symmetrical or asymmetrical) cryptographic algorithms

$+$	Addition operator	
$-$	Subtraction operator	
$\times$	Multiplication operator	
$\oplus$	Addition over fields	(= bitwise XOR over binary fields)
$\ominus$	Subtraction over fields	(= bitwise XOR over binary fields)
$\otimes$	Multiplication over fields	

Chapter 1

Introduction

1.1 Preface

Embedded devices hold secrets that are, unsurprisingly, coveted, and many malicious attackers are preparing to extract them illegitimately. Typical attacks involve measuring the device's power consumption or radiated electromagnetic (EM) field. These measurements are noisy sources of information that are, in one way or another, correlated with secrets. Consequently, analyzing these leaks enables us to recover the secrets.

The aim of this book is to formalize, characterize and quantify the actual threat level to these targets, drawing on the best mathematical tools for quantifying information leakage and characterizing leakage-based attacks. Two approaches are possible: either an optimal attack strategy can be derived (in specific contexts), or generic limits can be derived.

The tone of this book is resolutely mathematical. It aims at establishing formal foundations for techniques that are otherwise used as engineering recipes in industrial laboratories, or empirical intuitions for deriving safety levels from practical implementations. In this respect, this book is a systematization of knowledge and a compilation of relevant tools relating to the practice of side-channel analysis on embedded systems.

The contents of this book results from one decade (2014–2024) of efforts to formalize the field of side-channel analysis. This project has been initiated by Sylvain Guilley and Olivier Rioul in 2014. Along the way, we have associated PhD students, interns and colleagues to this journey. They helped to investigate eclectic aspects, which resulted in several original contributions, some of them discussed already within our community, on the occasion of annual workshops and conferences. In 2018, Wei Cheng[1] joined us to standardize and collate existing materials and new results in one single volume (i.e., the present work).

Obviously, we are indebted to our PhD students (in alphabetical order:

[1]The recent work of Wei Cheng is partially supported by National Key R&D Program of China (No. 2022YFB3103800).

Julien Béguinot, Nicolas Bruneau, Wei Cheng, Éloi de Chérisey, Annelie Heuser, Yi Liu, Houssem Maghrebi, and Damien Marion), one visiting researcher (Darshana Jayasinghe), and our colleagues (in alphabetical order: Claude Carlet, Jean-Luc Danger, Sihem Mesnager, Pablo Piantanida, Emmanuel Prouff, François-Xavier Standaert, and Ming Tang). Interaction with them has been very fruitful and we wish here to sincerely thank them for their individual contributions.

Some chapters of the present book are based on scientific articles presented at various venues in the 2014–2024 timeframe. Still, they have been properly integrated into a consistent narrative thread, and rewritten in parts to match with the uniformed notations we employed across the book. In addition, most material has been deeply reworked to make it more didactic, and more focused on the important takeaways rather than on the technicalities. We paid great care to cross-reference the different contributions in order to highlight the synergies between the book sections. The outcome is a self-contained monograph that consists in a systematization of knowledge about mathematical theory of practical side-channel analysis. It should make *mathematical foundations for side-channel analysis of cryptographic systems* accessible to:

- students in the field of embedded cybersecurity;
- professionals in secure devices design;
- governmental agencies aiming at defining optimal (normative) defense strategies.

The diversity of this audience reflects the fact that embedded cybersecurity is an issue embraced by an ecosystem. We hope our book will bring clarity to this technical subject, which has implications for the security of our daily lives in our digital society.

Book keywords: Embedded systems; Electronic devices; Cryptographic Software; Cryptographic Hardware; Side-channel analysis; Information leakage; Formalization; Mathematical analysis; Optimal distinguishers; Information theory; Statistics; Coding theory; Security bounds; Security metrics; Security cryptigraphic implementations; Systematization of Knowledge.

1.2 Cryptography & Cybersecurity

Nowadays, abundant electronic devices are proliferating in our daily life, such as SIM cards, cell-phones, bank cards, edge appliances, etc. Eurosmart's survey[2] tells us that there are about 9.54 billion shipped units of secure elements. In particular, the telecommunication market closed 2020 with around 5,1 billion units (smartcards) shipped, including 309 million units shipped for eSIM and a 4,8 billion units for SIM, which saw a significant increase. Those secure

[2]Eurosmart, https://www.eurosmart.com/2019-shipments-and-2020-outlook/

elements are widely deployed in telecom, financial services, device manufacturers, gouvernmental infrastructure, etc. However, such secure elements usually handle some sensitive information, which is highly exposed during computations when loaded, manipulated and stored. This leads to massive scales of vulnerabilities and attacks in practice. Therefore, improving their security has become an absolute priority. In addition, new regulations (such as the European Cyber-Resiliency Act) require security by design before deployment and security management after deployment.

In this respect, modern cryptography is the cornerstone for building the chain of trust and security. It plays a fundamental and pivotal role in establishing secure connectivity in this emerging digital age. In other words, cryptography enables secure communications between different parties, and evolves with computing and communication technologies. Basically, cryptography provides five primary functionalities: confidentiality, integrity, authentication, non-repudiation and key exchange. Those functionalities are well-established on the basis of various mathematical concepts such as information-theoretic security, computational complexity theory, number theory, coding theory, probability theory, etc.

Based on mathematical tools, it is possible to design and build theoretically secure cryptographic algorithms and protocols. In the field of symmetric key cryptography, the Data Encryption Standard (DES) [NIS99] and its successor, the Advanced Encryption Standard (AES) [NIS01], are one of the most important algorithms that have been published two decades ago by the National Institute of Standards and Technology (NIST). In the field of public key cryptography, Rivest-Shamir-Adleman (RSA) [RSA78] and Elliptic Curve Cryptography (ECC) [Mil85, Kob87] are two well-known instances that are based on the intractability of the corresponding mathematical problems.

1.3 The Root of Security & the Chain of Security

The Kerckhoffs principle, which dates back to the 19th century, is a basic rule and common consensus in modern cryptography. It stipulates that a cryptographic system must be secure, even if all the elements of the system are accessible to adversaries, with the exception of the key [Ker83a, Ker83b]. It was followed and reformulated by Claude E. Shannon in 1949, now known as Shannon's maxim: "*one ought to design (crypto) systems under the assumption that the enemy will immediately gain full familiarity with them*" [Sha49]. The keys present in a cryptosystem form the basis of the root of trust that is essential to the system. Theoretically, the above constructions (e.g., DES, AES, RSA, ECC, etc.) are computationally secure in this regard under the black-box assumption, in which an adversary can only access the inputs and outputs of the cryptosystem.

However, in practical applications, keys are not static, but dynamically manipulated in the digital world. Indeed, each stage of manipulation (computation) exposes these keys, leading to the need for a security chain to guarantee security in the real world.

In fact, any digital device leaks physically observable information [MR04] about internal states during executions. Although mathematical proofs of security for cryptographic algorithms are fundamental and indispensable, they usually cannot guarantee the practical security of the corresponding cryptographic implementations. In reality, those cryptographic algorithms must be run in some physical devices. Consequently, these physical observations generally violate the black-box setting assumption, according to which an adversary can only access the inputs and outputs of a cryptographic algorithm.

Since knowledge of certain observable information about the algorithms' internal variables is advantageous to the adversary, the black-box model is lifted to a gray-box setting by taking into account any (abstract) form of observable leakages that exists in practice. Accordingly, the attacks exploiting those physically observable leakages are called *physical attacks*.

1.4 Side-Channel Analysis

Side-channel analysis (SCA) is among the most powerful physical attacks against cryptographic implementations. Since the seminal works [Koc96, KJJ99], a very large amount of SCAs have been proposed by exploiting various observable physical leakages. Those physical leakages include (but are not limited to) running time [Koc96, DKL+98], power consumption [KJJ99, CCD00], electro-magnetic emanations [GMO01, QS01], acoustic emission [GST14, CPM+18], and photonic emission [FH08, KNSS13, CSW17]. More exploitable leakages emerge as technology improves (e.g., static leakage in nanotechnology [Mor14], spying in the context of multi-tenant FPGAs [SGMT18, RPD+18]) and in-depth understanding of behaviors of elementary circuits, like micro-architectural data leakages [GYCH18, LSG+18, KGG+18, MPW22]. Essentially, any measurable secret-dependent information or behaviors of the underlying cryptographic devices can be exploited to launch a successful side-channel attack.

In principle, side-channel analysis consists of extracting the sensitive information from noisy measurements. In many cases, the attacker can additionally purchase a blank device of the same series and learn about their leakage, in particular how it relates to the secrets. Such information can also improve the hardware attacks deployed on another device. Obviously, attacks operated in this context benefit from an advantage; it is qualified by the factor "Open samples/Samples with known secrets" in the Joint Interpretation Library (JIL) interpretation [Joi20] of the Common Evaluation Methodology (CEM).

Therefore, side-channel analysis is commonly divided into two categories, depending on the ability of the adversary and the corresponding setting:

- **Non-profiling attacks** — An adversary attempts to extract the sensitive information by correlating side-channel measurements and hypothetical leakages. Well-known attacks include simple power analysis (SPA, [Koc96]), differential power analysis (DPA, [KJJ99]), correlation power analysis (CPA, [BCO04]), and mutual information analysis (MIA, [GBTP08, VS09]).

- **Profiling attacks** are two-phrase attacks. An adversary is assumed to possess an identical device to build some exact profiles on the leakage behaviors and then apply these profiles during the attack phrase. Some well-known instances are template attack [CRR02], stochastic attack [SLP05], etc. In particular, the template attack is known as the most powerful side-channel attack if the leakage model is known perfectly.

Additionally, machine learning (including deep learning) techniques have been adapted into side-channel analysis in both non-profiling [Tim18, RAD20, PCBP21] and profiling settings [CDP17, ZBHV20, BPS+20, MDP20, WAGP20]. In essence, side-channel classifies different key hypotheses relying on observations, in which learning-based techniques shall amplify those attacks dramatically. However, those learning-based attacks tolerate a loss of interpretability on results, even in some restricted scenarios.

1.5 Side-Channel Protections

In order to protect cryptographic chips (implementations) against SCA, numerous countermeasures have been proposed, the three main ones being masking, shuffling and hiding. Masking schemes [CJRR99, ISW03, CPR07, MOP06, RP10] randomize the dependency between sensitive data and leakages by dividing each sensitive variable into several random shares to thwart SCA. Shuffling schemes [HOM06, RPD09, CS21a] randomize the order of operations during the executions. Quite differently, hiding-based countermeasures [CCD00, MOP06, RGN13] attempt to make the leakages uniformly independent to the data processed by circuit-level alteration, yet it is difficult to have any guarantee [ISU17]. Of course, these three types of protection can be constructively combined. Nevertheless, of these three categories of protection, masking is the most attractive and frequently used technique against SCA, as it offers formally provable security and can be implemented at algorithmic level without any hardware alteration. (Some simplifications must be disabled during compilation, however, otherwise the masking countermeasure can be modified or even removed).

1.5.1 Masking Schemes

Characterized by favorable provable security, masking has triggered a series of fruitful works, ranging from the theoretical construction of secure components (usually called gadgets) to the practical evaluation of resilience through side-channel attacks. Typically, the key parameter of a masking scheme is the security order t under the probing model [ISW03], which indicates the minimum order $(t + 1)$ that a successful attack must have. In a t-th order secure masking, each sensitive variable is split into at least $t + 1$ shares. The rationale is that the complexity of the attack increases exponentially with the number of shares [CJRR99, PR13] given a sufficient amount of noise, while the implementation cost increases only polynomially (quadratically or cubically in higher-order glitch-free implementations [GSF13]).

Various masking schemes have been proposed since 1999, and an overview of representative schemes is shown in Fig. 1.1. Typically instances include Boolean masking [CJRR99], inner product masking (IPM) [BFG15, BFG+17], leakage squeezing (LS) [CDG+14, CG18] and direct sum masking (DSM) [BCC+14a, PGS+17]. The proposals marked in blue are the first proposals of the corresponding schemes[3]. To the best of our knowledge, the generalized code-based masking (GCBM) [WMCS20, CGC+21a] is the most generic scheme in this respect[4]. In particular, polynomial masking [GM11, PR11] is also a special case of GCBM, which is built upon Shamir's secret sharing (SSS) scheme [Sha79].

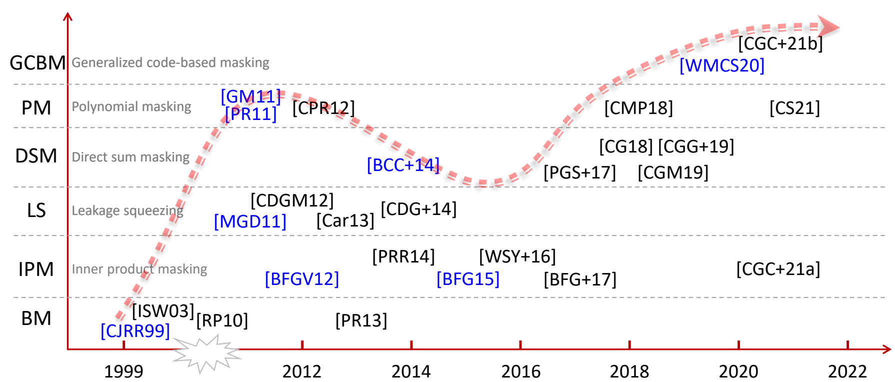

Figure 1.1: Various proposals of masking schemes with corresponding constructions, security assessment, and some variants.

Two questions arise naturally: (1) *how to measure information leakage in different schemes?* and (2) *how to choose optimal codes (or parameters) for each scheme?*

1.5.2 Generalizing to Code-based Masking

Code-based masking follows the generalization trend and unifies many schemes by focusing on the shared encodings. Two linear codes are involved, namely $\mathcal{C}$ and $\mathcal{D}$. The only requirement is that there is no nonzero codeword in their intersections [WMCS20, CGC+21a]. Consequently, the resistance of code-based masking to side-channel analysis is highly dependent on the two linear codes,

[3] Notice that the original publication on IPM [BFGV12] is not included in this figure, because it features some first-order information leakages. Those are later fixed in the improved proposal [BFG15], that we show in the figure instead.

[4] For simplicity in the sequel, we consider the code-based masking in the most general scenario.

whose coding-theoretical properties are related to algebraic complexity from the point of view of a (pseudo) Boolean function.

The first representative scheme is IPM, in which the encoding is similar to the simplest Boolean masking except that each share is equipped with a linear function (multiplied over a finite field by a public constant). It consumes n parameters in an n-share setting and enjoys the simple structure that can be implemented quite efficiently [BFG+17]. As a special instance of non-redundant code-based masking, the two linear codes in IPM are complementary, resulting in a great simplification when evaluating its side-channel resistance. In fact, we show that the side-channel security of IPM only depends on the properties of the code $\mathcal{D}$ [CGC+21b]. More generally, only code $\mathcal{D}$ matters in any non-redundant code-based masking like DSM.

Another typical example is the polynomial masking that is based on the SSS scheme. It also employs n public parameters in an n-share setting, but forms an entirely different encoding. Essentially, the encoding in SSS-based masking can be reformulated and connected to the Reed-Solomon (RS) codes [MS77, CMP18]. Considering an (n, t)-SSS based sharing as depicted in Fig. 1.2, it forms n shares while provides a t-th order privacy (side-channel resistance) rather than $n \cdot t$ parameters in a random setting. From a coding-theoretic perspective, the RS code is optimal in a given finite field in the sense that it achieves the Singleton bound [Sin64]. However, as shown in [CMP18], distinct public points play a role in the resilience and the efficiency of the protection. Therefore, the questions above still remain.

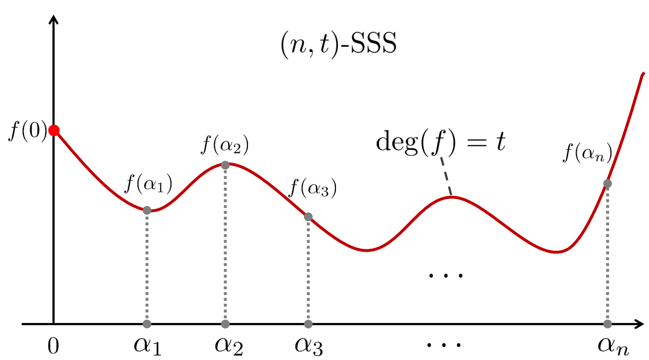

Figure 1.2: Illustration of an instance of redundant masking. In an (n, t)-SSS based polynomial masking, the sensitive variable $X = f(0)$ is encoded into n shares with a security order t.

In this book, we detail the general case of "code-based masking" which encompass most of previously proposed masking schemes. In particular, we show how to quantify the information leakage under various models on the one hand, and present evaluations of the exploitation of the information leakage on the other hand by providing attack-based results.

1.6 Getting Acquainted with the Topics

Side-channel analysis has gotten maturity over time. Table 1.1 retraces the history of key milestones. The infancy of the field was all about practical attacks.

Table 1.1: Maturity in Side-Channel Analysis

Realm	Year	Data-driven	Theoretical	Comment
Attack	1999		✔	Paul C. Kocher et al., *Differential Power Analysis*, CRYPTO 1999 [KJJ99]
	2016	✔		Houssem Maghrebi et al., *Breaking Cryptographic Imple-mentations Using Deep Learning Techniques*, SPACE 2016 [MPP16]
Distinguisher	2000	✔		Jean-Sébastien Coron et al., *Statistics and Secret Leakage*, FC 2000 [CKN00]
	2004		✔	Éric Brier et al., *Correlation Power Analysis with a Leakage Model*, CHES 2004 [BCO04]
Detection	2011	✔		Gilbert Goodwill et al., *A testing methodology for side-channel resistance validation*, NIST NIAT Workshop, 2011 [GJJR11]
Prediction	2014		✔	Victor Lomné et al., *How to Estimate the Success Rate of Higher-Order Side-Channel Attacks*, CHES 2014 [LPR+14]
Bounds	2015		✔	Alexandre Duc et al., *Making Masking Security Proofs Concrete*, EUROCRYPT 2015 [DFS15]
Information contents	2018	✔		Ishmael Belghazi et al., *Mutual Information Neural Estimation*, ICML 2018 [BBR+18].

Their theorization as distinguishers came next, where various distinguishers have different merits. Consequently, the "leakage detection" approach has been proposed to provide a security evaluation methodology, which is irrespective of distinguishers (this approach is the one followed in the International Standard ISO/IEC 17825). However, leakage detection does not allow to relate easily to a quantitative effort regarding the number of traces to exploit side-channel traces. Some works have been trying to predict the number of traces for given distinguishers, but again, such approach is specific to the given distinguishers. Therefore, the modern approach is to rely on bounds, which is an ongoing effort: We follow this approach in this book. The evaluation of bounds relies on the estimation of leakage metrics.

1.6.1 The Practice of Side-Channel Analysis

Side-channel analysis provides confidential information when being used, since it occurs during the use of a secret. Natural targets are therefore cryptographic in nature:

- operations on secret or private keys, such as key generation or diversification;
- encryption or decryption and message authentication codes, leveraging a secret key used in conjunction with a block cipher or a hash function;
- asymmetric encryption, key decapsulation mechanisms, digital signature generation, leveraging a private key, as part of a public/private key pair.

Side-channel analysis is, therefore, a real threat that can compromise the security of embedded systems. This threat can be viewed from two angles:

Offensive: devices which actually get hacked by side-channel analysis. Those can be tracked, for instance, leveraging some common vulnerabilities and exposures (CVEs), such as TPM-fail [MSEH20] (CVE-2019-11090), Minerva [JSSS20] (including CVE-2019-15809, CVE-2019-13627, CVE-2019-13627, CVE-2019-13629, CVE-2019-14318), CacheOut [vSMK+21] (CVE-2020-0549), Platypus [LKO+21] (CVE-2020-8694, CVE-2020-8695), or so-called Hertzbleed [WPH+22] (CVE-2022-23823). Note that these CVEs concern mostly attacks which require little or no laboratory equipments. Indeed, attacks which assume too much on the execution environment are not considered as eligible under CVE collection rules; thus the list of CVEs above concern only attacks that can be perpetrated from the remote or leveraging measurement apparati already embedded in computers (such as timers, voltage/power control equipment, etc.)

Defensive: inclusion of side-channel analysis within security referentials. This includes common weakness enumerations (CWEs) (e.g., CWE-1300 [MIT21]) and common criteria [Con13] for instance, where the threat is listed in a generic manner as `T.Leakage_Inherent` (line 82 page 25 of BSI-CC-PP-0084-2014 [Eur14]) and then further refined in some application documents, such as JIL [Joi20, §5.5].

Attackers may have multiple objectives:

- use of a device without paying for the subscription normally required to operate it;
- modify a device to implement more or different functionalities – or worse, to conceal stealthy backdoors;
- performing a step towards obtaining illegitimate access to debarked data (e.g. user lists, biometric data, credit card numbers, etc.).

From the defender's perspective, the goal is to rate as precisely as possible the threat. This allows, from the security prescriber standpoint, to decide the amount of efforts that will be required from the implementor. This entails some security verification schemes, such as:

- private methods, that are aimed at confidentially (pen)testing the devices security;
- public methods, such as certification approach. In such case, standard evaluation methods are defined and applied. One emblematic example is the so-called "Common Criteria" (CC [Con13]), which are based on an international standard (namely ISO/IEC 15408:2022). The goal of a CC evaluation is to determine the assurance level of the security of a given product. This book aims at providing sound metrics that yield practical measurement of a product security.

1.6.2 Security Evaluations

From the attacker's perspective, the goal is to devise the best attack, that optimizes the success rate or the guessing entropy (metrics defined in [SMY09]). There are different contexts, namely *supervised* and *unsupervised*. The attacks also depend on the scale of measurement, and of the apriori knowledge on the Target Of Evaluation (TOE).

However, from the defender's perspective, the natural question is about normative "vulnerability assessment". Security quotations can be expressed in terms of various factors:

- elapsed time;
- expertise;
- knowledge of target of evaluation (TOE);
- window of opportunity (which include the use of open devices or devices with known secrets);
- equipment.

1.6.3 Notations and Terminologies

Throughout this book, we use the following notations.

Calligraphic letters such as $\mathcal{X}$ denote sets or linear codes; uppercase letters such as X denote random variables taking values in the corresponding set; lowercase letters such as x denote realizations of the random variable. If necessary, vectors or matrices are written in bold characters while in plain if there is no ambiguity from the context.

We write $\mathbb{K} = \mathbb{F}_{p^\ell}$ as the finite field of order p^ℓ for prime number p and positive integer ℓ. The case $p = 2$ is for bit-oriented symmetrical algorithms, while $p > 2$ is more amenable to asymmetric cryptography, which leverages prime fields as underlying structures. In the rest of this book, we shall, without loss of generality, focus on binary fields where $p = 2$. Then ℓ represents the bit-length of the corresponding variable in the field $\mathbb{F}_{2^\ell}$.

In the context of side-channel analysis, we let $X \in \mathbb{K}$ be the sensitive variable that depends on a certain secret key chunk (a.k.a. subkey) $K \in \mathbb{K}$ and let $T \in \mathbb{K}$ be the correspoding known text chunk (either plaintext or ciphertext). For instance, $X = \psi_f(T + K)$ can be the output of some cryptographic operation ψ_f in a block cipher where $+$ denote bitwise exclusive or (XOR) or modulo 2 addition. In the case of the AES, we may put $\psi_f = S$ where S denotes a substitution box (Sbox).

We let $Y \in \mathbb{R}$ denote the noisy leakage under a leakage function $\phi_f(\cdot)$ and with certain noise[5] $Z \in \mathbb{R}$. Taking the commonly assumed additive white Gaussian noise (AWGN) as an example, one has $Y = f(K+T)+Z$ where $f = \phi_f \circ \psi_f$ and where $Z \sim \mathcal{N}(0, \sigma^2)$ is Gaussian with standard deviation σ.

The adversary employs a side-channel distinguisher Δ to guess the subkey used in the cryptographic implementation by exploiting the noisy leakage Y and the known-text T. The "best" key guess, denoted as $\widehat{K} \in \mathbb{K}$, is the candidate with the maximum distinguishing score. The above setting can be viewed as a communication channel as shown in Fig. 1.3, which is adapted from [HRG14b]. For multiple side-channel measures (a.k.a. traces) are acquired, the above no-

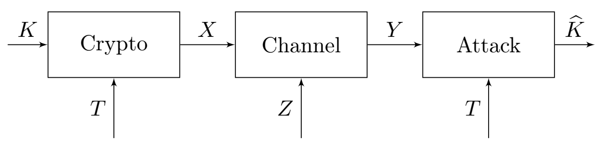

Figure 1.3: Side-channel analysis seen as a communication channel.

tations are updated accordingly in bold face.

The above communication channel view of side-channel analysis can be extended in the presence of side-channel countermeasures like masking schemes. Masking splits the sensitive variable into multiple shares, and then perform operations share by share. We let $\mathbf{M} \in \mathbb{K}^m$ denote the random masks and $\mathbf{X} \in \mathbb{K}^n$ denote the masked sharing with n shares. The essential parameter of a masking scheme is its security order t, which means that an adversary cannot obtain any information about the sensitive variable with side-channel leaks from at most t shares. Considering additive masking as an example, the sensitive variable X is split into n shares X_i such that $X = X_1 \star X_2 \star \cdots \star X_n$, where the group (field) operator $\star$ can be initialized as the exclusive OR (a.k.a. XOR) or the modular addition. In this case, the security order is $t \leq m = n - 1$. In this situation, we usually let $X_2, \ldots, X_n$ denote random masks that are generated uniformly over $\mathbb{K}$, and let X_1 be the masked variable computed from the formula $X_1 = X \star X_2 \star \cdots \star X_n$. The extended communication channel viewpoint

[5]In this book, we use the letter Z (which looks like a transposed N) to denote noise.

is depicted in Fig. 1.4 (adapted from [CLGR22a]).

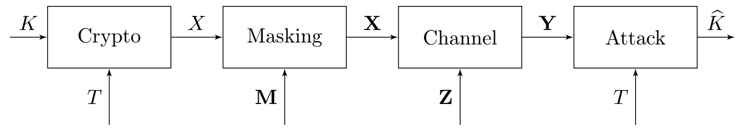

Figure 1.4: Side-channel analysis seen as a communication channel in the presence of masking countermeasure.

We mention that other side-channel countermeasures like *shuffling* [CS21a] can be encompassed straightforwardly in Fig. 1.4. Furthermore, the scope of analyses captured in Fig. 1.3 and 1.4 can be extended beyond physical side-channel analyses (e.g., web search engine [SSH+14] or timing attacks [dCGRJ16]).

We shall specify the other notations needed in the course of this book, to avoid tedious enumeration in this section.

1.7 Side-Channel Analyses Performance Criteria

The side-channels can be exploited by leveraging different key extraction strategies. For instance, the key can be recovered bit by bit, or by chunks (say ℓ bits by ℓ bits). The global key is eventually restored by divide-and-conquer.

The performances of the key ranking carried out by the adversary can be measured via three classical figures of merits:

1. the *success rate* (SR) or success probability $\mathbb{P}_s$,
2. the *success rate of order o* (SR_o, success rate in o-trials) $\mathbb{P}_{s,o}$ [SMY09], and
3. the *guessing entropy* (GE) [Mas94].

We follow the framework set up in [SMY09] and [IUH22, § 2.3] and express these metrics in terms of the a posteriori rank of the key hypothesis given the side-information.

1.8 Overview of the Content

At a high level, the contents of this book are divided into two parts: attacks and evaluations, with the exception of a few preliminaries summarized in Chap. 2. In Part I, we detail various attacks in Chap. 3 and 4 against unprotected and protected cryptographic implementations, respectively. In Part II, we start with the information-theoretic evaluations in Chap. 5, then move to the combination with coding theory to provide a full spectrum analysis on code-based masking in Chap. 6, and at last, we bridge the evaluations with attacks by presenting bounds on the probability to success in the worst-case scenarios in Chap. 7.

The main content of each chapter are summarized as follows.

In Chap. 3, we present attacks with various side-channel distinguishers against unprotected devices. The representative attacks are the optimal distinguisher based on the maximum-likelihood (ML) principle, correlation power analysis (CPA), mutual information analysis (MIA), and Kolmogorov-Smirnov analysis (KSA). In particular, we exemplify the scenarios in which CPA or MIA can be optimal under different noise assumptions. Moreover, we also present how to apply ML-based attacks with high dimension measurements, or in the multivariate context.

In Chap. 4, we continue the investigation of attacks against protected cryptographic implementations, especially in the presence of masking. The first one is the expectation-maximization (EM) based attack in the context of non-profiling attacks, especially in comparison with the second-order CPA (2O-CPA). Next, we present formally the higher-order optimal distinguisher (HOOD), which is again an ML-based approach. At last, we provide a Taylor expansion of ML attacks in order to deal with many masks in cryptographic implementations with higher-order masking.

In Chap. 5, we focus on the information-theoretic evaluations by presenting the interclass information analysis (IIA) in comparison with MIA. Next, we aim to bridge the distribution-based analyses and statistical moments-based analyses, the main idea lies in the cumulant expansion of mutual information (MI) at higher orders. We also apply this theoretical link in the analysis of higher-order maskings. At last, we introduce the α-information theory and show how it can be applied for upper bounding the success rate of any side-channel attacks.

In Chap. 6, we present a coding-theoretic formalization of various masking schemes, and essentially unifies the representation of these schemes under the so-called code-based masking (CBM) paradigm. On the basis of this unified formalization, we then propose a framework for quantifying the information leakage of CBM by using mutual information and signal-to-noise (SNR) as the leakage metrics. Interestingly, we build a formal connection between these two metrics with coding-theoretic properties of the underlying linear codes in CBM. As an important output, we define the optimal linear code for CBM and demonstrate the positive impacts on enhancing inner product masking and SSS-based polynomial masking schemes.

In Chap. 7, we aim to build a formal connection between various attacks and information-theoretic metrics. The main output is to provide some generic information-theoretic bounds that apply to any side-channel attacks. In particular, we present generic bounds based on mutual information and α-information for both unprotected and protected cryptographic devices. At last, we complete the information leakage quantification of CBM by providing attack-based evaluation results.

Bibliography

[ABDM00] Mehdi-Laurent Akkar, Régis Bevan, Paul Dischamp, and Didier Moyart. Power Analysis, What Is Now Possible... In *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 489–502. Springer, 2000. 34

[AG01] Mehdi-Laurent Akkar and Christophe Giraud. An Implementation of DES and AES Secure against Some Attacks. In LNCS, editor, *Proceedings of CHES'01*, volume 2162 of *LNCS*, pages 309–318. Springer, May 2001. Paris, France. 161, 183

[APSQ06] Cédric Archambeau, Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template Attacks in Principal Subspaces. In *CHES*, volume 4249 of *LNCS*, pages 1–14. Springer, October 10-13 2006. Yokohama, Japan. 88, 89, 98, 99

[Ari73] Suguru Arimoto. On the converse to the coding theorem for discrete memoryless channels (corresp.). *IEEE Transactions on Information Theory*, 19(3):357–359, May 1973. 331, 332

[Ari75] Suguru Arimoto. Information measures and capacity of order α for discrete memoryless channels. In Antoine Joux, editor, *Topics in Information Theory, Proc. 2nd Colloq. Math. Societatis János Bolyai*, volume 16, pages 41–52, 1975. 21, 249, 250

[BBB+13] Pierre Belgarric, Shivam Bhasin, Nicolas Bruneau, Jean-Luc Danger, Nicolas Debande, Sylvain Guilley, Annelie Heuser, Zakaria Najm, and Olivier Rioul. Time-Frequency Analysis for Second-Order Attacks. In Francillon and Rohatgi [FR14], pages 108–122. 316

[BBD+14] Shivam Bhasin, Nicolas Bruneau, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Analysis and Improvements of the DPA Contest v4 Implementation. In Chakraborty et al. [CMS14], pages 201–218. 281

[BBD+16] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rébecca Zucchini. Strong Non-Interference and Type-Directed Higher-Order

Masking. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 116–129. ACM, 2016. 256

[BBR+18] Mohamed Ishmael Belghazi, Aristide Baratin, Sai Rajeswar, Sherjil Ozair, Yoshua Bengio, R. Devon Hjelm, and Aaron C. Courville. Mutual information neural estimation. In Jennifer G. Dy and Andreas Krause, editors, *Proceedings of the 35th International Conference on Machine Learning, ICML 2018, Stockholmsmässan, Stockholm, Sweden, July 10-15, 2018*, volume 80 of *Proceedings of Machine Learning Research*, pages 530–539. PMLR, 2018. 8

[BC13] Guido Bertoni and Jean-Sébastien Coron, editors. *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*. Springer, 2013. 383, 405

[BCC10] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential properties of power functions. In *ISIT*, pages 2478–2482. IEEE, 2010. 86

[BCC+14a] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssem Maghrebi. Orthogonal Direct Sum Masking - A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks. In David Naccache and Damien Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014. Proceedings*, volume 8501 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2014. 6, 256, 259, 260, 268, 299, 368

[BCC+14b] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssem Maghrebi. Orthogonal Direct Sum Masking: A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks. Cryptology ePrint Archive, Report 2014/665, 2014. http://eprint.iacr.org/2014/665/ (extended version of conference paper [BCC+14a]). 259

[BCG+17] Nicolas Bruneau, Claude Carlet, Sylvain Guilley, Annelie Heuser, Emmanuel Prouff, and Olivier Rioul. Stochastic Collision Attack. *IEEE Trans. Information Forensics and Security*, 12(9):2090–2104, 2017. 58, 64, 66, 71, 334

[BCG+23] Julien Béguinot, Wei Cheng, Sylvain Guilley, Yi Liu, Loïc Masure, Olivier Rioul, and François-Xavier Standaert. Removing the field size loss from duc et al.'s conjectured bound for masked encodings. In Elif Bilge Kavun and Michael Pehl, editors, *Constructive Side-Channel Analysis and Secure Design - 14th International Workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, Proceedings*, volume 13979 of *Lecture Notes in Computer Science*, pages 86–104. Springer, 2023. 211

[BCGR24] Julien Béguinot, Wei Cheng, Sylvain Guilley, and Olivier Rioul. Formal security proofs via doeblin coefficients: Optimal side-channel factorization from noisy leakage to random probing. *IACR Cryptol. ePrint Arch.*, page 199, 2024. 211

[BCO04] Éric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Joye and Quisquater [JQ04], pages 16–29. 5, 8, 19, 43, 88, 110, 131, 134, 234, 266, 308, 310, 330

[BDF+17] Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub. Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 535–566, 2017. 263, 276, 278, 282

[BDG+14] Nicolas Bruneau, Jean-Luc Danger, Sylvain Guilley, Annelie Heuser, and Yannick Teglia. Boosting Higher-Order Correlation Attacks by Dimensionality Reduction. In Chakraborty et al. [CMS14], pages 183–200. 90, 108, 131, 207

[BDGN14] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Side-channel Leakage and Trace Compression Using Normalized Inter-class Variance. In *Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '14, pages 7:1–7:9, New York, NY, USA, 2014. ACM. 89

[BDMS22] Olivier Bronchain, François Durvaux, Loïc Masure, and François-Xavier Standaert. Efficient profiled side-channel analysis of masked implementations, extended. *IEEE Transactions on Information Forensics and Security*, 17:574–584, 2022. 136, 137, 159, 160

[Ben14] Josh Benaloh, editor. *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings*, volume 8366 of *Lecture Notes in Computer Science*. Springer, 2014. 397, 407

[Bet08] Koichi Betsumiya. Minimum Lee Weights of Type II Codes over $\mathbb{F}_{2^r}$. *Discret. Math.*, 308(14):3018–3022, 2008. 299

[BFG15] Josep Balasch, Sebastian Faust, and Benedikt Gierlichs. Inner Product Masking Revisited. In Oswald and Fischlin [OF15], pages 486–510. 6, 256, 257, 260

[BFG$^+$17] Josep Balasch, Sebastian Faust, Benedikt Gierlichs, Clara Paglialonga, and François-Xavier Standaert. Consolidating Inner Product Masking. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 724–754. Springer, 2017. 6, 7, 256, 257, 260, 261, 298, 299, 300

[BFGV12] Josep Balasch, Sebastian Faust, Benedikt Gierlichs, and Ingrid Verbauwhede. Theory and Practice of a Leakage Resilient Masking Scheme. In Wang and Sako [WS12], pages 758–775. 6, 256

[BGH$^+$15] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul. Less is More - Dimensionality Reduction from a Theoretical Perspective. In Güneysu and Handschuh [GH15], pages 22–41. 65, 67, 105, 108, 112, 184, 351

[BGHR14] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul. Masks Will Fall Off – Higher-Order Optimal Distinguishers. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 344–365. Springer, 2014. 65, 67, 136, 141, 183, 186, 187, 193, 197, 198, 271, 280, 294

[BGK04] Johannes Blömer, Jorge Guajardo, and Volker Krummel. Provably Secure Masking of AES. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography*, volume 3357 of *Lecture Notes in Computer Science*, pages 69–83. Springer, 2004. 162, 183, 325

[BGLR09] Lejla Batina, Benedikt Gierlichs, and Kerstin Lemke-Rust. Differential Cluster Analysis. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems – CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 112–127, Lausanne, Switzerland, 2009. Springer-Verlag. 212

[BGNT15] Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Teglia. Multi-variate High-Order Attacks of Shuffled Tables Recomputation. In Helena Handschuh and Tim Güneysu, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015. Proceedings*, volume 9293 of *Lecture Notes in Computer Science*. Springer, 2015. 183, 184, 185, 190, 193, 203

[BGNT18] Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Teglia. Multivariate High-Order Attacks of Shuffled Tables Recomputation. *J. Cryptol.*, 31(2):351–393, 2018. 141

[BGP+11] Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Mutual Information Analysis: a Comprehensive Study. *J. Cryptology*, 24(2):269–291, 2011. 182, 212, 229, 331

[BHM+19] Olivier Bronchain, Julien M. Hendrickx, Clément Massart, Alex Olshevsky, and François-Xavier Standaert. Leakage certification revisited: Bounding model errors in side-channel security evaluations. Cryptology ePrint Archive, Report 2019/132, 2019. `https://ia.cr/2019/132`. 135

[BHvW12] Lejla Batina, Jip Hogenboom, and Jasper G. J. van Woudenberg. Getting more from PCA: first results of using principal component analysis for extensive power analysis. In Dunkelman [Dun12], pages 383–397. 89

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES*, volume 4727 of *LNCS*, pages 450–466. Springer, September 10-13 2007. Vienna, Austria. 316

[BL20] Rinat Breuer and Itamar Levi. How Bad Are Bad Templates? Optimistic Design-Stage Side-Channel Security Evaluation and its Cost. *Cryptogr.*, 4(4):36, 2020. 135, 156

[BLR+23] Julien Béguinot, Yi Liu, Olivier Rioul, Wei Cheng, and Sylvain Guilley. Maximal leakage of masked implementations using mrs. gerber's lemma for min-entropy. In *IEEE International Symposium on Information Theory, ISIT 2023, Taipei, Taiwan, June 25-30, 2023*, pages 654–659. IEEE, 2023. 211

[Bog07] Andrey Bogdanov. Improved Side-Channel Collision Attacks on AES. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 84–95. Springer, 2007. 61

[Bog08] Andrey Bogdanov. Multiple-Differential Side-Channel Collision Attacks on AES. In Elisabeth Oswald and Pankaj Rohatgi, editors, *CHES*, volume 5154 of *Lecture Notes in Computer Science*, pages 30–44. Springer, 2008. 61

[BP10] Olivier Benoît and Thomas Peyrin. Side-Channel Analysis of Six SHA-3 Candidates. In *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 140–157. Springer, August 17-20 2010. Santa Barbara, CA, USA. 174

[BPA07] Raphaël Le Bidan, Ramesh Pyndiah, and Patrick Adde. Some Results on the Binary Minimum Distance of Reed-Solomon Codes and Block Turbo Codes. In *Proceedings of IEEE International Conference on Communications, ICC 2007, Glasgow, Scotland, UK, 24-28 June 2007*, pages 990–994. IEEE, 2007. 299

[BPS+20] Ryad Benadjila, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. Deep learning for side-channel analysis and introduction to ASCAD database. *J. Cryptogr. Eng.*, 10(2):163–188, 2020. 5

[BR12] Normand J. Beaudry and Renato Renner. An intuitive proof of the data processing inequality. *Quantum Info. Comput.*, 12(5-6):432–441, May 2012. 336

[BR14a] Sudipto Banerjee and Anindya Roy. *Linear Algebra and Matrix Analysis for Statistics.* Texts in Statistical Science. Chapman and Hall/CRC, 2014. 1st ed. ISBN 978-1420095388. 127

[BR14b] Lejla Batina and Matthew Robshaw, editors. *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*. Springer, 2014. 380, 385, 388, 391

[BS92] Eli Biham and Adi Shamir. Differential Cryptanalysis of the Full 16-Round DES. In Ernest F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992. 72, 83

[Car03] Jean-François Cardoso. Dependence, Correlation and Gaussianity in Independent Component Analysis. *Journal of Machine Learning Research*, 4:1177–1203, 2003. ISSN 1533-7928. 243, 244, 269

[Car05] Claude Carlet. On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. In *INDOCRYPT*, volume 3797 of *LNCS*, pages 49–62. Springer, december 2005. Bangalore, India. (PDF on SpringerLink; Complete version on IACR ePrint). 85, 239

[Car10a] Claude Carlet. Boolean Functions for Cryptography and Error Correcting Codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, Y. Crama and P. Hammer eds, 2010. Preliminary version is available at `http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf`. 19, 121, 128, 270, 302

[Car10b] Claude Carlet. Vectorial Boolean Functions for Cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 398–469. Cambridge University Press, Y. Crama and P. Hammer eds, 2010. Preliminary version available at `//www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf`. 83, 88

[Car13] Claude Carlet. Correlation-Immune Boolean Functions for Leakage Squeezing and Rotating S-Box Masking against Side Channel Attacks. In Benedikt Gierlichs, Sylvain Guilley, and Debdeep Mukhopadhyay, editors, *SPACE*, volume 8204 of *Lecture Notes in Computer Science*, pages 70–74. Springer, 2013. 258

[Car21] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Monograph in *Cambridge University Press*, January 7 2021. ISBN-10: 1108473806; ISBN-13: 978-1108473804. 16

[CB02] George Casella and Roger L. Berger. *Statistical Inference*. Duxbury Press, 2002. Second edition. ISBN-10: 0534243126 – ISBN-13: 978-0534243128. 45

[CBG$^+$17] Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventzislav Nikov, Svetla Nikova, and Vincent Rijmen. Does Coupling Affect the Security of Masked Implementations? In Sylvain Guilley, editor, *Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers*, volume 10348 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2017. 298

[CCD00] Christophe Clavier, Jean-Sébastien Coron, and Nora Dabbous. Differential Power Analysis in the Presence of Hardware Countermeasures. In Çetin Kaya Koç and Christof Paar, editors, *CHES*, volume 1965 of *Lecture Notes in Computer Science*, pages 252–263. Springer, 2000. 4, 5, 207

[CDD+14] Christophe Clavier, Jean-Luc Danger, Guillaume Duc, M. Abdelaziz Elaabid, Benoît Gérard, Sylvain Guilley, Annelie Heuser, Michael Kasper, Yang Li, Victor Lomné, Daisuke Nakatsu, Kazuo Ohta, Kazuo Sakiyama, Laurent Sauvage, Werner Schindler, Marc Stöttinger, Nicolas Veyrat-Charvillon, Matthieu Walle, and Antoine Wurcker. Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest. *Journal of Cryptographic Engineering*, pages 1–16, 2014. 102

[CDG+14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, Houssem Maghrebi, and Emmanuel Prouff. Achieving side-channel high-order correlation immunity with leakage squeezing. *J. Cryptographic Engineering*, 4(2):107–121, 2014. 6, 243, 244, 256, 258, 260, 269

[CDGM14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi. Leakage squeezing: Optimal implementation and security evaluation. *J. Mathematical Cryptology*, 8(3):249–295, 2014. 243, 258

[CDP17] Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures - Profiling Attacks Without Preprocessing. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 45–68. Springer, 2017. 5, 330

[CFG+11] Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, and Vincent Verneuil. Improved Collision-Correlation Power Analysis on First Order Protected AES. In Preneel and Takagi [PT11], pages 49–62. 62, 64, 69

[CFG+14] Claude Carlet, Finley Freibert, Sylvain Guilley, Michael Kiermaier, Jon-Lark Kim, and Patrick Solé. Higher-Order CIS Codes. *Information Theory, IEEE Transactions on*, 60(9):5283–5295, Sept 2014. 169

[CG99] Claude Carlet and Philippe Guillot. A New Representation of Boolean Functions. In Marc P. C. Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *AAECC*, volume 1719 of *Lecture Notes in Computer Science*, pages 94–103. Springer, 1999. 19, 265

[CG13] Claude Carlet and Sylvain Guilley. Side-Channel Indistinguishability. In *HASP*, pages 9:1–9:8, New York, NY, USA, June 23-24 2013. ACM. 375

[CG14] Claude Carlet and Sylvain Guilley. Side-Channel Indistinguishability, July 19 2014. On HAL: `http://hal.archives-ouvertes.fr/hal-00826618`. Extended version of [CG13] with more results in appendix. 64

[CG18] Claude Carlet and Sylvain Guilley. Statistical Properties of Side-Channel and Fault Injection Attacks Using Coding Theory. *Cryptography and Communications*, 10(5):909–933, 2018. 6, 256, 257, 258, 261, 281, 283, 285, 297, 299, 364

[CG20] Wei Cheng and Sylvain Guilley. Open-source: Quantifying Information Leakages in GCM, September 2020. `http://github.com/Qomo-CHENG/GeneralizedCM`. 274, 275, 280

[CGC⁺21a] Wei Cheng, Sylvain Guilley, Claude Carlet, Jean-Luc Danger, and Sihem Mesnager. Information Leakages in Code-based Masking: A Unified Quantification Approach. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):465–495, 2021. 6, 18, 256, 259, 282, 284, 285, 286, 299, 301

[CGC⁺21b] Wei Cheng, Sylvain Guilley, Claude Carlet, Sihem Mesnager, and Jean-Luc Danger. Optimizing Inner Product Masking Scheme by a Coding Theory Approach. *IEEE Trans. Inf. Forensics Secur.*, 16:220–235, 2021. 7, 18, 243, 245, 261, 264, 265, 279, 280, 283, 284, 285, 286, 291, 292, 293, 297, 298, 299, 300, 303, 364

[CGD22] Wei Cheng, Sylvain Guilley, and Jean-Luc Danger. Information Leakage in Code-Based Masking: A Systematic Evaluation by Higher-Order Attacks. *IEEE Trans. Inf. Forensics Secur.*, 17:1624–1638, 2022. 285, 300, 301

[CGMÖ18] Claude Carlet, Cem Güneri, Sihem Mesnager, and Ferruh Özbudak. Construction of some codes suitable for both side channel and fault injection attacks. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields - 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers*, volume 11321 of *Lecture Notes in Computer Science*, pages 95–107. Springer, 2018. 273

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.*, 23:493–507, 1952. 232

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In Wiener [Wie99], pages 398–412. 5, 6, 134, 135, 160, 163, 182, 183, 190, 192, 256, 325

[CK13] Omar Choudary and Markus G. Kuhn. Efficient template attacks. In Francillon and Rohatgi [FR14], pages 253–270. 89, 110

[CKN00] Jean-Sébastien Coron, Paul C. Kocher, and David Naccache. Statistics and Secret Leakage. In *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 157–173. Springer, February 20-24 2000. Anguilla, British West Indies. 8, 31, 42

[Cla09] Christophe Clavier. DPA Contest 2008–2009, Less than 50 traces allow to recover the key, September 6-9 2009. CHES Special Session 1: DPA Contest. Lausanne, Switzerland, (slides). 353

[CLGR22a] Wei Cheng, Yi Liu, Sylvain Guilley, and Olivier Rioul. Attacking Masked Cryptographic Implementations: Information-Theoretic Bounds. In *IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, June 26 - July 1, 2022*, pages 654–659. IEEE, 2022. 12, 363, 365, 366

[CLGR22b] Wei Cheng, Yi Liu, Sylvain Guilley, and Olivier Rioul. Toward finding best linear codes for side-channel protections (extended version). *Journal of Cryptographic Engineering*, pages 1–15, 2022. 290, 297

[CMGD23] Wei Cheng, Jingdian Ming, Sylvain Guilley, and Jean-Luc Danger. Statistical higher-order correlation attacks against code-based masking. *IEEE TechRxiv Preprint*, Dec 2023. 302

[CMP18] Hervé Chabanne, Houssem Maghrebi, and Emmanuel Prouff. Linear repairing codes and side-channel attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(1):118–141, 2018. 7, 261, 262, 273

[CMS14] Rajat Subhra Chakraborty, Vashek Matyas, and Patrick Schaumont, editors. *Security, Privacy, and Applied Cryptography Engineering - 4th International Conference, SPACE 2014, Pune, India, October 18-22, 2014. Proceedings*, volume 8804 of *Lecture Notes in Computer Science*. Springer, 2014. 367, 369

[Con13] Common Criteria Consortium. Common Criteria (*aka* CC) for Information Technology Security Evaluation (ISO/IEC 15408), 2013.
Website: `http://www.commoncriteriaportal.org/`. 9, 10, 43

[Cor14] Jean-Sébastien Coron. Higher Order Masking of Look-Up Tables. In Nguyen and Oswald [NO14], pages 441–458. 179, 183

[CPM+18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In David

Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 163–177. ACM, 2018. 4

[CPR07] Jean-Sébastien Coron, Emmanuel Prouff, and Matthieu Rivain. Side Channel Cryptanalysis of a Higher Order Masking Scheme. In Paillier and Verbauwhede [PV07], pages 28–44. 5

[CRR02] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template attacks. In Burton S. Kaliski, Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 13–28. Springer, 2002. 5, 29, 30, 47, 58, 88, 89, 92, 104, 110, 119, 121, 134, 138, 160, 164, 316

[CRZ13] Guilhem Castagnos, Soline Renner, and Gilles Zémor. High-order masking by using coding theory and its application to AES. In Martijn Stam, editor, *Cryptography and Coding - 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013. Proceedings*, volume 8308 of *Lecture Notes in Computer Science*, pages 193–212. Springer, 2013. 262

[CS21a] Jean-Sébastien Coron and Lorenzo Spignoli. Secure wire shuffling in the probing model. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 215–244. Springer, 2021. 5, 12

[CS21b] Nicolas Costes and Martijn Stam. Redundant code-based masking revisited. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):426–450, 2021. 259, 275, 280, 301

[Csi95] Imre Csiszár. Generalized cutoff rates and Rényi's information measures. *IEEE Trans. Inf. Theory*, 41(1):26–34, 1995. 249, 251

[CSM+15] Kaushik Chakraborty, Sumanta Sarkar, Subhamoy Maitra, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Emmanuel Prouff. Redefining the Transparency Order. In *The Ninth International Workshop on Coding and Cryptography, WCC 2015*, April 13-17 2015. Paris, France. 324

[CSW17] Elad Carmon, Jean-Pierre Seifert, and Avishai Wool. Photonic side channel attacks against RSA. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust, HOST*

2017, McLean, VA, USA, May 1-5, 2017, pages 74–78. IEEE Computer Society, 2017. 4

[CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, July 18 2006. ISBN-10: ISBN-10: 0471241954, ISBN-13: 978-0471241959, 2nd edition. 92, 215, 216, 219, 220, 223, 224, 226, 233, 237, 249, 314, 321, 335, 336, 340, 356, 365

[CTO+14] Mathieu Carbone, Sébastien Tiran, Sébastien Ordas, Michel Agoyan, Yannick Teglia, Gilles R. Ducharme, and Philippe Maurine. On adaptive bandwidth selection for efficient MIA. In Prouff [Pro14], pages 82–97. 44

[CV94] Florent Chabaud and Serge Vaudenay. Links Between Differential and Linear Cryptoanalysis. In Alfredo De Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer, 1994. 83

[CZC+17] Wei Cheng, Chao Zheng, Yuchen Cao, Yongbin Zhou, Hailong Zhang, Sylvain Guilley, and Laurent Sauvage. How Far Can We Reach? Breaking RSM-Masked AES-128 Implementation Using Only One Trace. *IACR Cryptology ePrint Archive*, 2017:1144, 2017. 281

[dCGHR18] Éloi de Chérisey, Sylvain Guilley, Annelie Heuser, and Olivier Rioul. On the optimality and practicability of mutual information analysis in some scenarios. *Cryptography and Communications*, 10(1):101–121, 2018. 135

[dCGRJ16] Éloi de Chérisey, Sylvain Guilley, Olivier Rioul, and Darshana Jayasinghe. Template Attacks with Partial Profiles and Dirichlet Priors: Application to Timing Attacks. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016, HASP@ICSA 2016, Seoul, Republic of Korea, June 18, 2016*, pages 7:1–7:8. ACM, 2016. 12

[dCGRP19a] Éloi de Chérisey, Sylvain Guilley, Olivier Rioul, and Pablo Piantanida. An Information-Theoretic Model for Side-Channel Attacks in Embedded Hardware. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, pages 310–315. IEEE, 2019. 363, 365

[dCGRP19b] Éloi de Chérisey, Sylvain Guilley, Olivier Rioul, and Pablo Piantanida. Best Information is Most Successful. Cryptology ePrint Archive, Report 2019/491, extended version of [dCGRP19c], 2019. https://eprint.iacr.org/2019/491. 339

[dCGRP19c] Éloi de Chérisey, Sylvain Guilley, Olivier Rioul, and Pablo Piantanida. Best Information Is Most Successful — Mutual Information and Success Rate in Side-Channel Analysis. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(2):49–79, 2019. 253, 360, 361, 362, 363, 364, 365, 366, 378

[DDF14] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying Leakage Models: From Probing Attacks to Noisy Leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440. Springer, 2014. 276

[DDGS14] Jean-Luc Danger, Nicolas Debande, Sylvain Guilley, and Youssef Souissi. High-order Timing Attacks. In *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*, CS2 '14, pages 7–12, New York, NY, USA, 2014. ACM. 89

[DDP13] Guillaume Dabosville, Julien Doget, and Emmanuel Prouff. A New Second-Order Side Channel Attack Based on Linear Regression. *IEEE Trans. Computers*, 62(8):1629–1640, 2013. 68

[Del75] Philippe Delsarte. The Association Schemes of Coding Theory. In *Combinatorics*, pages 143–161. Springer, 1975. 284

[DFS15] Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making Masking Security Proofs Concrete - Or How to Evaluate the Security of Any Leaking Device. In Oswald and Fischlin [OF15], pages 401–429. 8, 185, 187, 243, 276, 308, 330, 332, 349, 357, 363

[DGH+18] Jean-Luc Danger, Sylvain Guilley, Annelie Heuser, Axel Legay, and Ming Tang. Physical Security Versus Masking Schemes. In Çetin Kaya Koç, editor, *Cyber-Physical Systems Security.*, pages 269–284. Springer, 2018. 264

[DKL+98] Jean-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, and J.-L. Willems. A Practical Implementation of the Timing Attack. In *CARDIS*, pages 167–182, 1998. http://citeseer.nj.nec.com/dhem98practical.html. 4

[DLR77] Arthur P. Dempster, Nan M. Laird, and Donald B. Rubin. Maximum Likelihood from Incomplete Data via the EM Algorithm. *Journal of the Royal Statistical Society, Series B*, 39(1):1–38, 1977. 141

[DPRS11] Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate side channel attacks and leakage modeling. *J. Cryptographic Engineering*, 1(2):123–144, 2011. 26, 27, 34, 36, 38, 41, 43, 60, 61, 76, 109, 135, 136, 221, 229, 234, 310

[DSE+12] Nicolas Debande, Youssef Souissi, M. Abdelaziz Elaabid, Sylvain Guilley, and Jean-Luc Danger. Wavelet transform based pre-processing for side channel analysis. In *45th Annual IEEE/ACM International Symposium on Microarchitecture, MICRO 2012, Workshops Proceedings, Vancouver, BC, Canada, December 1-5, 2012*, pages 32–38. IEEE Computer Society, 2012. 89

[DSV14] François Durvaux, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. How to Certify the Leakage of a Chip? In Nguyen and Oswald [NO14], pages 459–476. 44, 329

[DSVC+14] François Durvaux, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Jean-Baptiste Mairy, and Yves Deville. Efficient Selection of Time Samples for Higher-Order DPA with Projection Pursuits. Cryptology ePrint Archive, Report 2014/412, 2014. http://eprint.iacr.org/2014/412. To appear at COSADE 2015 (LNCS), April 13-14 2015, Berlin, Germany. 90

[Dun12] Orr Dunkelman, editor. *Topics in Cryptology - CT-RSA 2012 - The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 - March 2, 2012. Proceedings*, volume 7178 of *Lecture Notes in Computer Science*. Springer, 2012. 371, 384

[DZFL14] A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo. A statistical model for higher order DPA on masked devices. In Batina and Robshaw [BR14b], pages 147–169. 169, 183

[Eur14] Eurosmart (https://www.eurosmart.com/). Security IC Platform Protection Profile with Augmentation Packages (PP 0084), January 13 2014. BSI-CC-PP-0084-2014. Version 1.0. https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf. 9

[EWTS14] Hassan Eldib, Chao Wang, Mostafa Taha, and Patrick Schaumont. QMS: Evaluating the Side-Channel Resistance of Masked Software from Source Code. In *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference*, DAC '14, pages 209:1–209:6, New York, NY, USA, 2014. ACM. 243

[Fan52] Robert M. Fano. *Class notes for course 6.574: Transmission of Information*. MIT, Cambridge, MA, 1952. 253

[FB14] Serge Fehr and Stefan Berens. On the conditional Rényi entropy. *IEEE Trans. Inf. Theory*, 60(11):6801–6810, 2014. 21, 249, 250, 252

[FH08] Julie Ferrigno and Martin Hlavác. When AES blinks: introducing optical side channel. *IET Inf. Secur.*, 2(3):94–98, 2008. 4

[Fis22] Ronald A. Fisher. On the mathematical foundations of theoretical statistics. *Philosophical Transactions of the Royal Society of London, A*, 222:309–368, 1922. 163

[Fis25] Ronald A. Fisher. *Statistical Methods for Research Workers*. Oliver and Boyd, Edinburgh, 1925. 237, 238, 322

[FLD12] Yunsi Fei, Qiasi Luo, and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis. In Prouff and Schaumont [PS12], pages 233–250. 76, 80, 94, 230, 234, 236, 308, 310, 312, 317, 318, 319, 345

[For65] G. David Forney. *Concatenated Codes*. PhD thesis, M.I.T. Dept. of Electrical Engineering, December 1965. 290

[FR14] Aurélien Francillon and Pankaj Rohatgi, editors. *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*, volume 8419 of *LNCS*. Springer, 2014. 367, 376, 383, 408

[Gal68] Robert G. Gallager. *Information theory and reliable communication*. Wiley, 1968. 27, 29

[GBPV10] Benedikt Gierlichs, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede. Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis. In *CT-RSA*, volume 5985 of *LNCS*, pages 221–234. Springer, March 1-5 2010. San Francisco, CA, USA. 141, 164

[GBTP08] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In *CHES, 10th International Workshop*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, August 10-13 2008. Washington, D.C., USA. 5, 43, 46, 48, 49, 55, 138, 141, 212, 223, 308, 310, 316, 331

[GCS+08] Sylvain Guilley, Sumanta Chaudhuri, Laurent Sauvage, Philippe Hoogvorst, Renaud Pacalet, and Guido Marco Bertoni. Security Evaluation of WDDL and SecLib Countermeasures against Power Attacks. *IEEE Transactions on Computers*, 57(11):1482–1497, nov 2008. 89

[GGP+15] Cezary Glowacz, Vincent Grosso, Romain Poussier, Joachim Schüth, and François-Xavier Standaert. Simpler and More Efficient Rank Estimation for Side-Channel Security Assessment. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 117–129. Springer, 2015. 105

[GH15] Tim Güneysu and Helena Handschuh, editors. *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*. Springer, 2015. 370

[GHP04a] Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential Power Analysis Model and some Results. In Kluwer, editor, *Proceedings of WCC/CARDIS*, pages 127–142, Aug 2004. Toulouse, France. DOI: 10.1007/1-4020-8147-2_9. 83, 85

[GHP04b] Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential Power Analysis Model and Some Results. In Quisquater et al. [QPDK04], pages 127–142. 214, 239

[GHPS07] Sylvain Guilley, Philippe Hoogvorst, Renaud Pacalet, and Johannes Schmidt. Improving Side-Channel Attacks by Exploiting Substitution Boxes Properties. In Presse Universitaire de Rouen et du Havre, editor, *BFCA*, pages 1–25, 2007. May 02–04, Paris, France, http://www.liafa.jussieu.fr/bfca/books/BFCA07.pdf. 312

[GHR15] Sylvain Guilley, Annelie Heuser, and Olivier Rioul. A Key to Success - Success Exponents for Side-Channel Distinguishers. In Alex Biryukov and Vipul Goyal, editors, *Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings*, volume 9462 of *Lecture Notes in Computer Science*, pages 270–290. Springer, 2015. 330, 332, 345, 347

[GHR17] Sylvain Guilley, Annelie Heuser, and Olivier Rioul. Codes for Side-Channel Attacks and Protections. In Said El Hajji, Abderrahmane Nitaj, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security - Second International Conference, C2SI 2017, Rabat, Morocco, April 10-12, 2017, Proceedings - In Honor of Claude Carlet*, volume 10194 of *Lecture Notes in Computer Science*, pages 35–55. Springer, 2017. 363

[GJJR11] Gilbert Goodwill, Benjamin Jun, Joshua Jaffe, and Pankaj Rohatgi. A testing methodology for side-channel resistance validation, September 2011. NIST Non-Invasive

Attack Testing Workshop, http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf. 8

[GLRP06] Benedikt Gierlichs, Kerstin Lemke-Rust, and Christof Paar. Templates vs. Stochastic Methods. In *CHES*, volume 4249 of *LNCS*, pages 15–29. Springer, October 10-13 2006. Yokohama, Japan. 88, 89, 116, 135

[GM11] Louis Goubin and Ange Martinelli. Protecting AES with Shamir's Secret Sharing Scheme. In Preneel and Takagi [PT11], pages 79–94. 6, 256, 259, 260

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '01, pages 251–261, London, UK, UK, 2001. Springer-Verlag. 4, 244, 363

[GS18] Vincent Grosso and François-Xavier Standaert. Masking Proofs Are Tight and How to Exploit it in Security Evaluations. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 385–412. Springer, 2018. 243, 340

[GSF13] Vincent Grosso, François-Xavier Standaert, and Sebastian Faust. Masking vs. Multiparty Computation: How Large Is the Gap for AES? In Bertoni and Coron [BC13], pages 400–416. 6, 134, 256, 257

[GSP13] Vincent Grosso, François-Xavier Standaert, and Emmanuel Prouff. Low Entropy Masking Schemes, Revisited. In Francillon and Rohatgi [FR14], pages 33–43. 281

[GST14] Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 444–461. Springer, 2014. 4

[GYCH18] Qian Ge, Yuval Yarom, David Cock, and Gernot Heiser. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *J. Cryptographic Engineering*, 8(1):1–27, 2018. 4

[Hal00] Anders Hald. The Early History of the Cumulants and the Gram-Charlier Series. *International Statistical Review*, 68(2):137–153, 2000. 244

[HGR14] Annelie Heuser, Sylvain Guilley, and Olivier Rioul. A Theoretical Study of Kolmogorov-Smirnov Distinguishers: Side-Channel Analysis vs. Differential Cryptanalysis. Cryptology ePrint Archive, Report 2014/008, 2014. http://eprint.iacr.org/2014/008. 240, 241

[HKSS11] Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger. How a symmetry metric assists side-channel evaluation - a novel model verification method for power analysis. In *Proceedings of the 2011 14th Euromicro Conference on Digital System Design*, DSD '11, pages 674–681, Washington, DC, USA, 2011. IEEE Computer Society. 233, 312, 317

[HKSS12] Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger. A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models. In Dunkelman [Dun12], pages 365–382. 54, 60, 119

[HM13a] Suvadeep Hajra and Debdeep Mukhopadhyay. Multivariate leakage model for improving non-profiling DPA on noisy power traces. In Dongdai Lin, Shouhuai Xu, and Moti Yung, editors, *Information Security and Cryptology - 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013, Revised Selected Papers*, volume 8567 of *Lecture Notes in Computer Science*, pages 325–342. Springer, 2013. 90

[HM13b] Suvadeep Hajra and Debdeep Mukhopadhyay. SNR to Success Rate: Reaching the Limit of Non-Profiling DPA. Cryptology ePrint Archive, Report 2013/865, 2013. http://eprint.iacr.org/2013/865/. 90

[HM14] Suvadeep Hajra and Debdeep Mukhopadhyay. On the optimal pre-processing for non-profiling differential power analysis. In Prouff [Pro14], pages 161–178. 88, 90

[HM15] Suvadeep Hajra and Debdeep Mukhopadhyay. Reaching the limit of nonprofiling DPA. *IEEE Trans. on CAD of Integrated Circuits and Systems*, 34(6):915–927, 2015. 90

[HOM06] Christoph Herbst, Elisabeth Oswald, and Stefan Mangard. An AES Smart Card Implementation Resistant to Power Analysis Attacks. In Jianying Zhou, Moti Yung, and Feng Bao, editors, *ACNS*, volume 3989 of *Lecture Notes in Computer Science*, pages 239–252, 2006. 5, 182

[HRG14a] Annelie Heuser, Olivier Rioul, and Sylvain Guilley. A Theoretical Study of Kolmogorov-Smirnov Distinguishers — Side-Channel Analysis vs. Differential Cryptanalysis. In Prouff [Pro14], pages 9–28. 142

[HRG14b] Annelie Heuser, Olivier Rioul, and Sylvain Guilley. Good Is Not Good Enough - Deriving Optimal Distinguishers from Communication Theory. In Batina and Robshaw [BR14b], pages 55–74. 11, 43, 44, 47, 51, 63, 65, 67, 92, 105, 110, 116, 122, 139, 316, 317, 319, 320, 329, 332, 333, 345, 360, 361, 363, 364

[HSS12] Annelie Heuser, Werner Schindler, and Marc Stöttinger. Revealing side-channel issues of complex circuits by enhanced leakage models. In Rosenstiel and Thiele [RT12], pages 1179–1184. 119, 127

[HV94] Te Sun Han and Sergio Verdú. Generalizing the Fano inequality. *IEEE Transactions on Information Theory*, 40(4):1247–1251, Jul. 1994. 253

[HZ12] Annelie Heuser and Michael Zohner. Intelligent Machine Homicide - Breaking Cryptographic Devices Using Support Vector Machines. In Werner Schindler and Sorin A. Huss, editors, *COSADE*, volume 7275 of *LNCS*, pages 249–264. Springer, 2012. 330

[ISU17] Vincent Immler, Robert Specht, and Florian Unterstein. Your Rails Cannot Hide from Localized EM: How Dual-Rail Logic Fails on FPGAs. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 403–424. Springer, 2017. 5

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private Circuits: Securing Hardware against Probing Attacks. In *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, August 17–21 2003. Santa Barbara, California, USA. 5, 134, 182, 256, 282, 363

[IUH22] Akira Ito, Rei Ueno, and Naofumi Homma. Perceived information revisited new metrics to evaluate success rate of side-channel attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(4):228–254, 2022. 12

[Joi20] Joint Interpretation Library. Application of Attack Potential to Smartcards, Version 3.1, June 2020. `https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-1.pdf`, retrieved on January 6, 2024. 4, 9

[JPS05] Marc Joye, Pascal Paillier, and Berry Schoenmakers. On Second-Order Differential Power Analysis. In *CHES*, volume 3659 of *LNCS*, pages 293–308. Springer, August 29 – September 1st 2005. Edinburgh, UK. 160

[JQ04] Marc Joye and Jean-Jacques Quisquater, editors. *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*. Springer, 2004. 369, 402, 408

[JSSS20] Jan Jancar, Vladimir Sedlacek, Petr Svenda, and Marek Sýs. Minerva: The curse of ECDSA nonces systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(4):281–308, 2020. 9

[Kar05] O.J.W.F. Kardaun. *Classical Methods of Statistics*. Springer, 2005. 32, 39, 238, 322

[KDOP15] Su Min Kim Kim, Tan Tai Do, Tobias J. Oechtering, and Gunnar Peters. On the Entropy Computation of Large Complex Gaussian Mixture Distributions. *IEEE Transactions on Signal Processing*, 63(17):4710–4723, Sept 2015. 340

[Ker83a] Auguste Kerckhoffs. La cryptographie militaire (1). *Journal des sciences militaires*, 9:5–38, January 1883. `http://en.wikipedia.org/wiki/Kerckhoffs_law`. 3

[Ker83b] Auguste Kerckhoffs. La cryptographie militaire (2). *Journal des sciences militaires*, 9:161–191, February 1883. `http://en.wikipedia.org/wiki/Kerckhoffs_law`. 3, 244

[KGD18] Naghmeh Karimi, Sylvain Guilley, and Jean-Luc Danger. Impact of Aging on Template Attacks. In *Proceedings of the 28th ACM Great Lakes Symposium on VLSI*, GLSVLSI '18. ACM, May 23-25 2018. Chicago, Illinois, USA. 135, 159

[KGG$^+$18] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre Attacks: Exploiting Speculative Execution. *CoRR*, abs/1801.01203, 2018. 4

[KGP$^+$09] Peter Karsmakers, Benedikt Gierlichs, Kristiaan Pelckmans, Katrien De Cock, Johan Suykens, Bart Preneel, and Bart De Moor. Side channel attacks on cryptographic devices as a classification problem. COSIC technical report, 2009. 89

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Wiener [Wie99], pages 388–397. 4, 8, 19, 31, 42, 92, 134, 162, 173, 212, 234, 244, 308, 316, 329, 363

[KNSS13] Juliane Krämer, Dmitry Nedospasov, Alexander Schlösser, and Jean-Pierre Seifert. Differential Photonic Emission Analysis. In Prouff [Pro13], pages 1–16. 4

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematic of Computation*, 48:203–209, 1987. 3

[Koc96] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996. 4, 329

[Kol33] Andrey Nikolaevich Kolmogorov. Sulla determinazione empirica di una legge di distribuzione. *Giorn. Ist. Ital. Attuari*, 4:83–91, 1933. 77

[KSK09] Yuichi Komano, Hideo Shimizu, and Shinichi Kawamura. Built-in determined sub-key correlation power analysis. Cryptology ePrint Archive, Report 2009/161, 2009. http://eprint.iacr.org/2009/161. 353

[KSS10] Michael Kasper, Werner Schindler, and Marc Stöttinger. A stochastic method for security evaluation of cryptographic FPGA implementations. In Jinian Bian, Qiang Zhou, Peter Athanas, Yajun Ha, and Kang Zhao, editors, *FPT*, pages 146–153. IEEE, 2010. 37, 119, 131

[KWW21] Brian Kurkoski, Tadashi Wadayama, and Shun Watanabe, editors. *IEEE Information Theory Workshop, ITW 2021, Kanazawa, Japan, October 17-21, 2021*. IEEE, 2021. 388, 402

[LB10] Thanh-Ha Le and Maël Berthier. Mutual Information Analysis under the View of Higher-Order Statistics. In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC*, volume 6434 of *Lecture Notes in Computer Science*, pages 285–300. Springer, 2010. 212

[LBC+23] Yi Liu, Julien Béguinot, Wei Cheng, Sylvain Guilley, Loïc Masure, Olivier Rioul, and François-Xavier Standaert. Improved alpha-information bounds for higher-order masked cryptographic implementations. In *IEEE Information Theory Workshop, ITW 2023, Saint-Malo, France, April 23-28, 2023*, pages 81–86. IEEE, 2023. 211

[LBM15] Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. A machine learning approach against a masked AES - Reaching the limit of side-channel attacks with a learning model. *J. Cryptographic Engineering*, 5(2):123–139, 2015. 135

[LCGR21] Yi Liu, Wei Cheng, Sylvain Guilley, and Olivier Rioul. On conditional alpha-information and its application to side-channel analysis. In Kurkoski et al. [KWW21], pages 1–6. 20, 21, 22, 359, 360, 361, 362

[LD02] Jérôme Lacan and Emmanuelle Delpeyroux. The q-ary Image of Some q^m-ary Cyclic Codes: Permutation Group and Soft-decision Decoding. *IEEE Trans. Inf. Theory*, 48(7):2069–2078, 2002. 299

[Lem75] Abraham Lempel. Matrix Factorization Over GF(2) and Trace-Orthogonal Bases of $GF(2^n)$. *SIAM J. Comput.*, 4(2):175–186, 1975. 287

[LKO+21] Moritz Lipp, Andreas Kogler, David F. Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, and Daniel Gruss. PLATYPUS: Software-based Power Side-Channel Attacks on x86. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 355–371. IEEE, 2021. 9

[LM18] Liran Lerman and Olivier Markowitch. Efficient profiled attacks on masking schemes. *IEEE Transactions on Information Forensics and Security*, 14(6):1445–1454, 2018. 135

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and Its Applications #20. Cambridge University Press, 1997. ISBN 10: 0521392314, ISBN 13: 9780521392310. 287

[LP07] Kerstin Lemke-Rust and Christof Paar. Analyzing Side Channel Leakage of Masked Implementations with Stochastic Methods. In Joachim Biskup and Javier López, editors, *Computer Security - ESORICS 2007, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007, Proceedings*, volume 4734 of *Lecture Notes in Computer Science*, pages 454–468. Springer, 2007. 182

[LPR13] Victor Lomné, Emmanuel Prouff, and Thomas Roche. Behind the Scene of Side Channel Attacks. In Sako and Sarkar [SS13], pages 506–525. 38, 44, 50, 112, 128

[LPR+14] Victor Lomné, Emmanuel Prouff, Matthieu Rivain, Thomas Roche, and Adrian Thillard. How to Estimate the Success Rate of Higher-Order Side-Channel Attacks. In Batina and Robshaw [BR14b], pages 35–54. 8, 308, 310, 312, 330, 332

[LPS09] Yingbin Liang, H. Vincent Poor, and Shlomo Shamai. Information theoretic security. *Found. Trends Commun. Inf. Theory*, 5(4-5):355–580, 2009. 361

[LRP07] Kerstin Lemke-Rust and Christof Paar. Gaussian Mixture Models for Higher-Order Side Channel Analysis. In Paillier and Verbauwhede [PV07], pages 14–27. 136, 137, 138, 149, 156, 157, 182

[LSG+18] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading Kernel Memory from User Space. In William Enck and Adrienne Porter Felt, editors, *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018.*, pages 973–990. USENIX Association, 2018. 4

[Mah36] Prasanta Chandra Mahalanobis. On the Generalised Distance in Statistics. *Proceedings of the National Institute of Sciences of India*, 2(1):49—55, 1936. 66, 110

[Man04] Stefan Mangard. Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness. In *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 222–235. Springer, 2004. San Francisco, CA, USA. 321, 330

[Mas93] James L Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279. Citeseer, 1993. 261

[Mas94] James L. Massey. Guessing and entropy. In *Proceedings of 1994 IEEE International Symposium on Information Theory*, pages 204–, Jun 1994. 12, 355

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993. 83

[MCGD12] Houssem Maghrebi, Claude Carlet, Sylvain Guilley, and Jean-Luc Danger. Optimal First-Order Masking with Linear and Non-linear Bijections. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT*, volume 7374 of *Lecture Notes in Computer Science*, pages 360–377. Springer, 2012. 140, 258

[MCZL21] Jingdian Ming, Wei Cheng, Yongbin Zhou, and Huizhong Li. APT: efficient side-channel analysis framework against inner product masking scheme. In *39th IEEE International Conference on Computer Design, ICCD 2021, Storrs, CT, USA, October 24-27, 2021*, pages 575–582. IEEE, 2021. 302

[MDP20] Loïc Masure, Cécile Dumas, and Emmanuel Prouff. A Comprehensive Study of Deep Learning for Side-Channel Analysis. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(1):348–375, 2020. 5, 135

[Mes00a] Thomas S. Messerges. Securing the AES finalists against power analysis attacks. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 150–164. Springer, 2000. 183

[Mes00b] Thomas S. Messerges. Using Second-Order Power Analysis to Attack DPA Resistant Software. In *CHES*, volume 1965 of *LNCS*, pages 238–251. Springer-Verlag, August 17-18 2000. Worcester, MA, USA. 141, 160, 163, 192, 325

[MGD11] Houssem Maghrebi, Sylvain Guilley, and Jean-Luc Danger. Leakage Squeezing Countermeasure against High-Order Attacks. In Claudio Agostino Ardagna and Jianying Zhou, editors, *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011. Proceedings*, volume 6633 of *Lecture Notes in Computer Science*, pages 208–223. Springer, 2011. 257, 299

[MGPV09] Elke De Mulder, Benedikt Gierlichs, Bart Preneel, and Ingrid Verbauwhede. Practical DPA attacks on MDPL. In *First IEEE International Workshop on Information Forensics and Security, WIFS 2009, London, UK, December 6-9, 2009*, pages 191–195. IEEE, 2009. 51

[Mil85] Victor S. Miller. Use of Elliptic Curves in Cryptography. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985. 3

[MIT21] MITRE. CWE-1300: Improper Protection of Physical Side Channels, 2021. `https://cwe.mitre.org/data/definitions/1300.html`. 9

[MK08] Geoffrey McLachlan and Thriyambakam Krishnan. *The EM Algorithm and Extensions*. Wiley Series in Probability and Statistics. Wiley-Blackwell, 29 april 2008. 2nd Edition. ISBN-10: 0471201707 ISBN-13: 978-0471201700. 64

[MM12] Seiichi Matsuda and Shiho Moriai. Lightweight Cryptography for the Cloud: Exploit the Power of Bitslice Implementation. In Prouff and Schaumont [PS12], pages 408–425. 52

[MME10] Amir Moradi, Oliver Mischke, and Thomas Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack. In *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 125–139. Springer, August 17-20 2010. Santa Barbara, CA, USA. 63, 69

[MMPS09] Amir Moradi, Nima Mousavi, Christof Paar, and Mahmoud Salmasizadeh. A Comparative Study of Mutual Information Analysis under a Gaussian Assumption. In *WISA (Information Security Applications, 10th International Workshop)*, volume 5932 of *Lecture Notes in Computer Science*, pages 193–205. Springer, August 25-27 2009. Busan, Korea. 30, 44, 53, 79, 212, 223, 312, 316

[MMS13] Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Indranil Sengupta. Constrained Search for a Class of Good Bijective S-Boxes With Improved DPA Resistivity. *IEEE Transactions on Information Forensics and Security*, 8(12):2154–2163, 2013. 88

[Mod89] R. Moddemeijer. On estimation of entropy and mutual information of continuous distributions. *Signal Processing*, 16(3):233–248, March 1989. 237, 238, 322, 323

[MOP06] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, December 2006. ISBN 0-387-30857-1, `http://www.dpabook.org/`. 5, 72, 75, 76, 78, 79

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007. 181

[Mor12] Amir Moradi. Statistical tools flavor side-channel collision attacks. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 428–445. Springer, 2012. 63, 64

[Mor14] Amir Moradi. Side-Channel Leakage through Static Power - Should We Care about in Practice? In Batina and Robshaw [BR14b], pages 562–579. 4

[MOS11a] Stefan Mangard, Elisabeth Oswald, and François-Xavier Standaert. One for All - All for One: Unifying Standard DPA Attacks. *Information Security, IET*, 5(2):100–111, 2011. ISSN: 1751-8709 ; Digital Object Identifier: 10.1049/iet-ifs.2010.0096. 26, 31

[MOS11b] Stefan Mangard, Elisabeth Oswald, and François-Xavier Standaert. One for all - all for one: unifying standard differential power analysis attacks. *IET Information Security*, 5(2):100–110, 2011. 229, 309, 310

[MOW14] Luke Mather, Elisabeth Oswald, and Carolyn Whitnall. Multi-target DPA attacks: Pushing DPA beyond the limits of a desktop computer. In Sarkar and Iwata [SI14], pages 243–261. 105

[MP13] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields*. Chapman and Hall/CRC, June 17 2013. ISBN 9781439873786 - CAT# K13417. 17

[MPP16] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. Breaking Cryptographic Implementations Using Deep Learning Techniques. In Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, *Security, Privacy, and Applied Cryptography Engineering - 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings*, volume 10076 of *Lecture Notes in Computer Science*, pages 3–26. Springer, 2016. 8

[MPW22] Ben Marshall, Dan Page, and James Webb. MIRACLE: micro-architectural leakage evaluation A study of micro-architectural power leakage across many devices. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(1):175–220, 2022. 4

[MR04] Silvio Micali and Leonid Reyzin. Physically Observable Cryptography (Extended Abstract). In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004. 4

[MRGD12] Houssem Maghrebi, Olivier Rioul, Sylvain Guilley, and Jean-Luc Danger. Comparison between Side-Channel Analysis Distinguishers. In Tat Wing Chim and Tsz Hon Yuen, editors, *ICICS*, volume 7618 of *LNCS*, pages 331–340. Springer, 2012. 36, 70, 72, 74, 77, 87, 170, 212, 217, 229, 310, 316

[MRS22] Loïc Masure, Olivier Rioul, and François-Xavier Standaert. A nearly tight proof of duc et al.'s conjectured security bound for masked implementations. In Ileana Buhan and Tobias Schneider, editors, *Smart Card Research and Advanced Applications - 21st International Conference, CARDIS 2022, Birmingham, UK, November 7-9, 2022, Revised Selected Papers*, volume 13820 of *Lecture Notes in Computer Science*, pages 69–81. Springer, 2022. 211

[MS77] F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, North Holland, 1977. ISBN: 978-0-444-85193-2. 7, 15, 16, 17, 273, 283, 292

[MS86] Judy H. Moore and Gustavus J. Simmons. Cycle Structures of the DES with Weak and Semi-Weak Keys. In Andrew M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 9–32. Springer, 1986. 29

[MS14] Amir Moradi and François-Xavier Standaert. Moments-correlating DPA. *IACR Cryptology ePrint Archive*, 2014:409, June 2 2014. 190

[MS16] Amir Moradi and François-Xavier Standaert. Moments-Correlating DPA. In Begül Bilgin, Svetla Nikova, and Vincent Rijmen, editors, *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*, pages 5–15. ACM, 2016. 242

[MS23] Loïc Masure and François-Xavier Standaert. Prouff and Rivain's Formal Security Proof of Masking, Revisited - Tight Bounds in the Noisy Leakage Model. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 343–376. Springer, 2023. 211

[MSEH20] Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, and Nadia Heninger. TPM-FAIL: TPM meets Timing and Lattice Attacks. In Srdjan Capkun and Franziska Roesner, editors, *29th USENIX Security Symposium, USENIX Security 2020, August 12-14, 2020*, pages 2057–2073. USENIX Association, 2020. 9

[MZC+20] Jingdian Ming, Yongbin Zhou, Wei Cheng, Huizhong Li, Guang Yang, and Qian Zhang. Mind the balance: Revealing the vulnerabilities in low entropy masking schemes. *IEEE Trans. Inf. Forensics Secur.*, 15:3694–3708, 2020. 281

[MZCL22] Jingdian Ming, Yongbin Zhou, Wei Cheng, and Huizhong Li. Optimizing higher-order correlation analysis against inner product masking scheme. *IEEE Trans. Inf. Forensics Secur.*, 17:3555–3568, 2022. 302

[Nad05] Saralees Nadarajah. A generalized normal distribution. *Journal of Applied Statistics*, 32(7):685–694, 2005. 33

[NIS99] NIST/ITL/CSD. Data Encryption Standard. FIPS PUB 46-3, Oct 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. 3

[NIS01] NIST/ITL/CSD. Advanced Encryption Standard (AES). FIPS PUB 197, Nov 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (also ISO/IEC 18033-3:2010). 3, 86, 244, 341

[NO14] Phong Q. Nguyen and Elisabeth Oswald, editors. *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*. Springer, 2014. 376, 380

[NRS11] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. *J. Cryptology*, 24(2):292–321, 2011. 185

[NS94] Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994. 19

[NSGD12] Maxime Nassar, Youssef Souissi, Sylvain Guilley, and Jean-Luc Danger. RSM: A Small and Fast Countermeasure for AES, Secure against 1st and 2nd-order Zero-offset SCAs. In Rosenstiel and Thiele [RT12], pages 1173–1178. 281, 299

[OF15] Elisabeth Oswald and Marc Fischlin, editors. *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*. Springer, 2015. 370, 379

[OM07] Elisabeth Oswald and Stefan Mangard. Template Attacks on Masking — Resistance Is Futile. In Masayuki Abe, editor, *CT-RSA*, volume 4377 of *Lecture Notes in Computer Science*, pages 243–256. Springer, 2007. 135, 160, 163, 164, 166, 182, 192, 325

[OMHT06] Elisabeth Oswald, Stefan Mangard, Christoph Herbst, and Stefan Tillich. Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers. In Pointcheval [Poi06], pages 192–207. 89

[OP12] David Oswald and Christof Paar. Improving Side-Channel Analysis with Optimal Linear Transforms. In Stefan Mangard, editor, *CARDIS*, volume 7771 of *Lecture Notes in Computer Science*, pages 219–233. Springer, 2012. 88, 90

[PCBP21] Guilherme Perin, Lukasz Chmielewski, Lejla Batina, and Stjepan Picek. Keep it unsupervised: Horizontal attacks meet deep learning. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):343–372, 2021. 5

[PdHL09] Jing Pan, Jerry I. den Hartog, and Jiqiang Lu. You cannot hide behind the mask: Power analysis on a provably secure S-box implementation. In Heung Youl Youm and Moti Yung, editors, *Information Security Applications, 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers*, volume 5932 of *Lecture Notes in Computer Science*, pages 178–192. Springer, 2009. 190

[PDW89] Marcel J.M. Pelgrom, Aad C.J. Duinmaijer, and Anton P.G. Welbers. Matching properties of MOS transistors. *IEEE Journal of Solid State Circuits*, 24(5):1433–1439, 1989. DOI: 10.1109/JSSC.1989.572629. 35

[PEB+14] Stjepan Picek, Barış Ege, Lejla Batina, Domagoj Jakobovic, and Kostas Papagiannopoulos. Optimality and Beyond: The Case of 4×4 S-boxes. In *HOST*, IEEE Computer Society, May 2014. Arlington, USA. 88

[PGS+17] Romain Poussier, Qian Guo, François-Xavier Standaert, Claude Carlet, and Sylvain Guilley. Connecting and Improving Direct Sum Masking and Inner Product Masking. In Thomas Eisenbarth and Yannick Teglia, editors, *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*, volume 10728 of *Lecture Notes in Computer Science*, pages 123–141. Springer, 2017. 6, 256, 259, 260, 261, 264, 278, 283, 285, 299

[PHG19] Stjepan Picek, Annelie Heuser, and Sylvain Guilley. Profiling Side-channel Analysis in the Restricted Attacker Framework. *IACR Cryptology ePrint Archive*, 2019:168, 2019. 330

[PMMB15] Stjepan Picek, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Lejla Batina. Modified Transparency Order Property: Solution or Just Another Attempt. In *Security, Privacy, and Applied Cryptography Engineering - 5th International Conference, SPACE 2015, Jaipur, Rajasthan, India, October 3-7, 2015. Proceedings*, 2015. 324

[Poi06] David Pointcheval, editor. *Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2006, Proceedings*, volume 3860 of *LNCS*. Springer, 2006. 394, 403

[PR07] Emmanuel Prouff and Matthieu Rivain. A Generic Method for Secure SBox Implementation. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *WISA*, volume 4867 of *Lecture Notes in Computer Science*, pages 227–244. Springer, 2007. 183

[PR09] Emmanuel Prouff and Matthieu Rivain. Theoretical and Practical Aspects of Mutual Information Based Side Channel Analysis. In Springer, editor, *ACNS*, volume 5536 of *LNCS*, pages 499–518, June 2-5 2009. Paris-Rocquencourt, France. 212, 222, 312

[PR10] Emmanuel Prouff and Matthieu Rivain. Theoretical and practical aspects of mutual information-based side channel analysis. *International Journal of Applied Cryptography (IJACT)*, 2(2):121–138, 2010. 26, 49, 73, 78, 79, 212, 222, 223, 229

[PR11] Emmanuel Prouff and Thomas Roche. Higher-Order Glitches Free Implementation of the AES Using Secure Multi-party Computation Protocols. In Preneel and Takagi [PT11], pages 63–78. 6, 256, 259, 260, 280, 299

[PR13] Emmanuel Prouff and Matthieu Rivain. Masking against Side-Channel Attacks: A Formal Security Proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2013. 6, 134, 135, 245, 256, 330, 332, 363

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Trans. Computers*, 58(6):799–811, 2009. 135, 138, 140, 160, 163, 164, 166, 169, 170, 174, 192, 233, 312, 317, 325

[PRC12] Gilles Piret, Thomas Roche, and Claude Carlet. PICARO – A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *ACNS*, volume 7341 of *Lecture Notes in Computer Science*, pages 311–328. Springer, 2012. 88

[Pro05] Emmanuel Prouff. DPA Attacks and S-Boxes. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 424–441. Springer, 2005. 72, 85, 88, 214, 239, 240, 241, 324

[Pro13] Emmanuel Prouff, editor. *Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013, Paris, France, March 6-8, 2013, Revised Selected Papers*, volume 7864 of *Lecture Notes in Computer Science*. Springer, 2013. 387

[Pro14] Emmanuel Prouff, editor. *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers*, volume 8622 of *Lecture Notes in Computer Science*. Springer, 2014. 378, 384, 385, 399

[PRR14] Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. On the Practical Security of a Leakage Resilient Masking Scheme. In Benaloh [Ben14], pages 169–182. 256

[PS12] Emmanuel Prouff and Patrick Schaumont, editors. *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*. Springer, 2012. 381, 390, 398

[PSDQ05] Éric Peeters, François-Xavier Standaert, Nicolas Donckers, and Jean-Jacques Quisquater. Improved Higher-Order Side-Channel Attacks with FPGA Experiments. In *CHES*, volume 3659 of *LNCS*, pages 309–323. Springer, 2005. 182

[PT11] Bart Preneel and Tsuyoshi Takagi, editors. *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 – October 1, 2011. Proceedings*, volume 6917 of *LNCS*. Springer, 2011. 374, 383, 396

[PV07] Pascal Paillier and Ingrid Verbauwhede, editors. *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *LNCS*. Springer, 2007. 377, 389

[PV10] Yury Polyanskiy and Sergio Verdú. Arimoto channel coding converse and Rényi divergence. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1327–1333, 2010. 251, 252

[QPDK04] Jean-Jacques Quisquater, Pierre Paradinas, Yves Deswarte, and Anas Abou El Kalam, editors. *Smart Card Research and Advanced Applications VI, IFIP 18th World Computer Congress, TC8/WG8.8 & TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS), 22-27 August 2004, Toulouse, France*, volume 153 of *IFIP*. Kluwer/Springer, 2004. 382

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smard Cards. In I. Attali and T. P. Jensen, editors, *Smart Card Programming and Security (E-smart 2001)*, volume 2140 of *LNCS*, pages 200–210. Springer-Verlag, September 2001. Nice, France. ISSN 0302-9743. 4

[Ŕ61] Alfred Rényi. On measures of entropy and information. In *Proc. Fourth Berkeley Symposium on Mathematical Statistics and Probability*, volume 1: Contributions to the Theory of Statistics, pages 547–561, Berkeley, CA, 1961. University of California Press. 20, 248

[Rab88] Patrice Rabizzoni. Relation Between the Minimum Weight of a Linear Code over GF(q^m) and Its q-art Image over GF(q). In Gérard D. Cohen and Jacques Wolfmann, editors, *Coding Theory and Applications, 3rd International Colloquium, Toulon, France, November 2-4, 1988, Proceedings*, volume 388 of *Lecture Notes in Computer Science*, pages 209–212. Springer, 1988. 299, 300

[RAD20] Keyvan Ramezanpour, Paul Ampadu, and William Diehl. SCAUL: power side-channel analysis with unsupervised learning. *IEEE Trans. Computers*, 69(11):1626–1638, 2020. 5

[Rao73] C. Radhakrishna Rao. *Linear Statistical Inference and its Applications*. J. Wiley and Sons, New York, 2nd edition, 1973. 236, 308, 319

[RCG21] Olivier Rioul, Wei Cheng, and Sylvain Guilley. Cumulant expansion of mutual information for quantifying leakage of a protected secret. In *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*, pages 2596–2601. IEEE, 2021. 242, 243, 245, 246

[Ret92] Charles T. Retter. Gaps in the Binary Weight Distributions of Reed-Solomon Codes. *IEEE Trans. Inf. Theory*, 38(6):1688–1697, 1992. 299

[RGN13] Pablo Rauzy, Sylvain Guilley, and Zakaria Najm. Formally Proved Security of Assembly Code Against Leakage. *IACR Cryptology ePrint Archive*, 2013:554, 2013. (Also appears at PROOFS 2014, Busan, South Korea). 5

[RGV12] Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede. Selecting Time Samples for Multivariate DPA Attacks. In Prouff and Schaumont [PS12], pages 155–174. 90

[RGV14a] Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede. A note on the use of margins to compare distinguishers. In *COSADE (*to appear*)*, Lecture Notes in Computer Science. Springer, April 14-15 2014. Paris, France. 27

[RGV14b] Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede. Generic DPA Attacks: Curse or Blessing? In Prouff [Pro14], pages 98–111. 46, 49

[RHGD16] Olivier Rioul, Annelie Heuser, Sylvain Guilley, and Jean-Luc Danger. Inter-class vs. mutual information as side-channel distinguishers. In *IEEE International Symposium on Information Theory, ISIT 2016, Barcelona, Spain, July 10-15, 2016*, pages 805–809. IEEE, 2016. 334

[Rio11] Olivier Rioul. Information theoretic proofs of entropy power inequalities. *IEEE Trans. Inf. Theory*, 57(1):33–55, 2011. 246

[Rio18] Olivier Rioul. Rényi entropy power inequalities via normal transport and rotation. *Entropy*, 20(9, 641):1–17, Sept. 2018. 250

[Rio21] Olivier Rioul. A primer on alpha-information theory with application to leakage in secrecy systems. In *5th conference on Geometric Science of Information (GSI'21), Paris, France, 21-23 July 2021*, Lecture Notes in Computer Science, 2021. 361

[Riv08] Matthieu Rivain. On the Exact Success Rate of Side Channel Analysis in the Gaussian Model. In *Selected Areas in Cryptography*, volume 5381 of *LNCS*, pages 165–183. Springer, August 14-15 2008. Sackville, New Brunswick, Canada. 29, 30, 230, 236, 308, 310, 311, 312, 319, 330, 332

[Rog11] Phillip Rogaway, editor. *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*. Springer, 2011. 405, 407

[RP10] Matthieu Rivain and Emmanuel Prouff. Provably Secure Higher-Order Masking of AES. In Stefan Mangard and François-Xavier Standaert, editors, *CHES*, volume 6225 of *LNCS*, pages 413–427. Springer, 2010. 5, 134, 181, 183, 256, 282, 363

[RPD09] Matthieu Rivain, Emmanuel Prouff, and Julien Doget. Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers. In *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 171–188. Springer, September 6-9 2009. Lausanne, Switzerland. 5, 182, 207

[RPD+18] Chethan Ramesh, Shivukumar B. Patil, Siva Nishok Dhanuskodi, George Provelengios, Sébastien Pillement, Daniel E. Holcomb, and Russell Tessier. FPGA Side Channel Attacks without Physical Access. In *26th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines, FCCM 2018, Boulder, CO, USA, April 29 - May 1, 2018*, pages 45–52. IEEE Computer Society, 2018. 4

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. 3

[RSD06] Chester Rebeiro, A. David Selvakumar, and A. S. L. Devi. Bitslice implementation of AES. In David Pointcheval, Yi Mu, and Kefei Chen, editors, *Cryptology and Network Security, 5th International Conference, CANS 2006, Suzhou, China, December 8-10, 2006, Proceedings*, volume 4301 of *Lecture Notes in Computer Science*, pages 203–212. Springer, 2006. 52

[RSV+11] Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Dina Kamel, and Denis Flandre. A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2011. 89, 119, 159

[RT12] Wolfgang Rosenstiel and Lothar Thiele, editors. *2012 Design, Automation & Test in Europe Conference & Exhibition, DATE 2012, Dresden, Germany, March 12-16, 2012*. IEEE, 2012. 385, 394

[Rud76] Walter Rudin. *Principles of mathematical analysis*. McGraw-Hill Book Co., New York, third edition, 1976. International Series in Pure and Applied Mathematics. 221

[SA08] François-Xavier Standaert and Cédric Archambeau. Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages. In *CHES*, volume 5154 of *Lecture Notes in Computer Science*, pages 411–425. Springer, August 10–13 2008. Washington, D.C., USA. 89, 101, 351

[Sat] Akashi Satoh. Side-channel Attack Standard Evaluation Board, SASEBO-GII. Project of the AIST – RCIS (Research Center for Information Security), http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-GII-en.html [Accessed on May 31, 2015]. 102

[SBdMVC08] François-Xavier Standaert, Philippe Bulens, Giacomo de Meulenaer, and Nicolas Veyrat-Charvillon. Improving the Rules of the DPA Contest. Cryptology ePrint Archive, Report 2008/517, December 8 2008. http://eprint.iacr.org/2008/517. 212

[Sch05] Werner Schindler. On the optimization of side-channel attacks by advanced stochastic methods. In Serge Vaudenay, editor, *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, volume 3386 of *Lecture Notes in Computer Science*, pages 85–103. Springer, 2005. 131

[SDM+12] Youssef Souissi, Nicolas Debande, Sami Mekki, Sylvain Guilley, Ali Maalaoui, and Jean-Luc Danger. On the Optimality of Correlation Power Attack on Embedded Cryptographic Systems. In Ioannis G. Askoxylakis, Henrich Christopher Pöhls, and Joachim Posegga, editors, *WISTP*, volume 7322 of *Lecture Notes in Computer Science*, pages 169–178. Springer, June 20-22 2012. 26, 89

[SG86] B. W. Silverman and P. J. Green. *Density Estimation for Statistics and Data Analysis*. Chapman & Hall/CRC, London, 1986. 229

[SGMT18] Falk Schellenberg, Dennis R. E. Gnad, Amir Moradi, and Mehdi Baradaran Tahoori. An inside job: Remote power analysis attacks on FPGAs. In Jan Madsen and Ayse K. Coskun, editors, *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018*, pages 1111–1116. IEEE, 2018. 4

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, October 1949. 3, 244

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979. 6, 256

[SHAS10] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh. Profiling attack using multivariate regression analysis. *IEICE Electronics Express*, 7(15):1139–1144, 2010. 89, 94, 105

[SI14] Palash Sarkar and Tetsu Iwata, editors. *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*. Springer, 2014. 392, 406

[Sib69] Robin Sibson. Information radius. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 14(2):149–160, 1969. 21, 249, 251

[Sin64] Richard C. Singleton. Maximum Distance q-nary Codes. *IEEE Trans. Information Theory*, 10(2):116–118, 1964. 7, 284

[SK96] Katsumi Sakakibara and Masao Kasahara. On the Minimum Distance of a q-ary Image of a q^m-ary Cyclic Code. *IEEE Trans. Inf. Theory*, 42(5):1631–1635, 1996. 299

[SKM+13] Fabrizio De Santis, Michael Kasper, Stefan Mangard, Georg Sigl, Oliver Stein, and Marc Stöttinger. On the Relationship between Correlation Power Analysis and the Stochastic Approach: An ASIC Designer Perspective. In Goutam Paul and Serge Vaudenay, editors, *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*, volume 8250 of *Lecture Notes in Computer Science*, pages 215–226. Springer, 2013. 135

[SKS09] François-Xavier Standaert, François Koeune, and Werner Schindler. How to Compare Profiled Side-Channel Attacks? In Springer, editor, *ACNS*, volume 5536 of *LNCS*, pages 485–498, June 2-5 2009. Paris-Rocquencourt, France. 27, 68, 120, 128

[SL80] Gadiel Seroussi and Abraham Lempel. Factorization of Symmetric Matrices and Trace-Orthogonal Bases in Finite Fields. *SIAM J. Comput.*, 9(4):758–767, 1980. 287

[SLC+21] Patrick Solé, Yi Liu, Wei Cheng, Sylvain Guilley, and Olivier Rioul. Linear programming bounds on the kissing number of q-ary codes. In Kurkoski et al. [KWW21], pages 1–5. 15

[SLFP04] Kai Schramm, Gregor Leander, Patrick Felke, and Christof Paar. A Collision-Attack on AES: Combining Side Channel- and Differential-Attack. In Joye and Quisquater [JQ04], pages 163–175. 61, 69

[SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In LNCS, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005. Edinburgh, Scotland, UK. 5, 31, 34, 38, 60, 67, 114, 119, 123, 131, 135, 136

[Smi48] Nikolai Vasilevich Smirnov. Tables for estimating the goodness of fit of empirical distributions. *Annals of Mathematical Statistics*, 19(2):279–281, 1948. 77

[SMY09] François-Xavier Standaert, Tal Malkin, and Moti Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *EUROCRYPT*, volume 5479 of *LNCS*, pages 443–461. Springer, April 26-30 2009. Cologne, Germany. 10, 12, 28, 47, 196, 213, 229, 308, 312, 332, 360, 363

[SNG+10] Youssef Souissi, Maxime Nassar, Sylvain Guilley, Jean-Luc Danger, and Florent Flament. First Principal Components Analysis: A New Side Channel Distinguisher. In Kyung Hyune Rhee and DaeHun Nyang, editors, *ICISC*, volume 6829 of *Lecture Notes in Computer Science*, pages 407–419. Springer, 2010. 89

[Sny05] Jan A. Snyman. *Practical mathematical optimization: an introduction to basic optimization theory and classical and new gradient-based algorithms*. Applied optimization. Springer, New York, 2005. 64

[SO94] Alan Stuart and Keith Ord. *Kendall's Advanced Theory of Statistics: Distribution Theory*. Wiley-Blackwell, June 2 1994. 6th Edition. ISBN-10: 0470665300; ISBN-13: 978-0470665305. 188

[SOR+14] Daehyun Strobel, David Oswald, Bastian Richter, Falk Schellenberg, and Christof Paar. Microcontrollers as (in)security devices for pervasive computing applications. *Proceedings of the IEEE*, 102(8):1157–1173, 2014. 89

[SP00] George Saon and Mukund Padmanabhan. Minimum bayes error feature selection for continuous speech recognition. In Todd K. Leen, Thomas G. Dietterich, and Volker Tresp, editors, *Advances in Neural Information Processing Systems 13, Papers from Neural Information Processing Systems (NIPS) 2000, Denver, CO, USA*, pages 800–806. MIT Press, 2000. 218

[SP06] Kai Schramm and Christof Paar. Higher Order Masking of the AES. In Pointcheval [Poi06], pages 208–225. 160

[SPAQ06] François-Xavier Standaert, Eric Peeters, Cédric Archambeau, and Jean-Jacques Quisquater. Towards security limits in side-channel attacks. In *CHES*, volume 4249 of *Lecture Notes in Computer Science*, pages 30–45. Springer, October 10-13 2006. Yokohama, Japan. 329

[SPQ05] F. X Standaert, E. Peeters, and J-J Quisquater. On the masking countermeasure and higher-order power analysis attacks. In *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, volume 1, pages 562–567 Vol. 1, 2005. 160

[SPRQ06] François-Xavier Standaert, Éric Peeters, Gaël Rouvroy, and Jean-Jacques Quisquater. An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays. *Proceedings of the IEEE*, 94(2):383–394, February 2006. (Invited Paper). 234

[SS13] Kazue Sako and Palash Sarkar, editors. *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the*

Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I, volume 8269 of *Lecture Notes in Computer Science*. Springer, 2013. 388

[SSH+14] Alexander Schaub, Emmanuel Schneider, Alexandros Hollender, Robin Touillon, Laurent Jolie, Vinicius Calasans, Olivier Rioul, Sylvain Guilley, and Annelie Heuser. Attacking Suggest Boxes in Web Applications Over HTTPS Using Stochastic Side-Channel Algorithms. In *CRiSIS*, Lecture Notes in Computer Science. Springer, August 27-29 2014. Trento, Italia.
↦ Up-to-date version: http://eprint.iacr.org/2014/959. 12

[Sta10] François-Xavier Standaert. Introduction to Side-Channel Attacks Secure Integrated Circuits and Systems. In Ingrid M. R. Verbauwhede, editor, *Secure Integrated Circuits and Systems*, Integrated Circuits and Systems, chapter 2, pages 27–42. Springer US, Boston, MA, 2010. 234

[SV18] Igal Sason and Sergio Verdú. Arimoto-Rényi conditional entropy and bayesian m-ary hypothesis testing. *IEEE Trans. Inf. Theory*, 64(1):4–25, 2018. 250

[SVO+10] François-Xavier Standaert, Nicolas Veyrat-Charvillon, Elisabeth Oswald, Benedikt Gierlichs, Marcel Medwed, Markus Kasper, and Stefan Mangard. The World Is Not Enough: Another Look on Second-Order DPA. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*, pages 112–129. Springer, 2010. 135, 151, 160, 163, 164, 169, 170, 182, 198, 271

[SWP03] Kai Schramm, Thomas J. Wollinger, and Christof Paar. A new class of collision attacks and its application to DES. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 2003. 61

[Tch67] Pafnouti Tchebichef. Des valeurs moyennes. *Journal de mathématiques pures et appliqués*, 12(2):177–184, 1867. 232

[TELa] TELECOM ParisTech. DPA Contest, 2nd edition. http://www.DPAcontest.org/v2/ [Accessed on May 31, 2015]. 89, 102

[TELb] TELECOM ParisTech SEN research group. DPA Contest. http://www.DPAcontest.org/. 351, 352

[TEL10] TELECOM ParisTech SEN research group. DPA Contest (2^{nd} edition), 2009–2010. http://www.DPAcontest.org/v2/. 353

[TEL14] TELECOM ParisTech SEN research group. DPA Contest (4^{th} edition), 2013–2014. http://www.DPAcontest.org/v4/. 75, 109, 206, 281

[Tim18] Benjamin Timon. Non-Profiled Deep Learning-Based Side-Channel Attacks. *IACR Cryptology ePrint Archive*, 2018:196, 2018. 5

[TPR13] Adrian Thillard, Emmanuel Prouff, and Thomas Roche. Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack. In Bertoni and Coron [BC13], pages 21–36. 166, 230, 234, 308, 310, 317, 318

[TWO13] Michael Tunstall, Carolyn Whitnall, and Elisabeth Oswald. Masking Tables – An Underestimated Security Risk. In Shiho Moriai, editor, *FSE*, volume 8424 of *Lecture Notes in Computer Science*, pages 425–444. Springer, 2013. 161, 174, 183, 190, 193

[Uni] University of Sydney (Australia). Magma Computational Algebra System. http://magma.maths.usyd.edu.au/magma/, Accessed on 2022-08-22. 274

[VCGRS12] Nicolas Veyrat-Charvillon, Benoît Gérard, Mathieu Renauld, and François-Xavier Standaert. An Optimal Key Enumeration Algorithm and Its Application to Side-Channel Attacks. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography*, volume 7707 of *Lecture Notes in Computer Science*, pages 390–406. Springer, 2012. 105

[VCMKS12] Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François-Xavier Standaert. Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note. In Wang and Sako [WS12], pages 740–757. 182

[VCS09] Nicolas Veyrat-Charvillon and François-Xavier Standaert. Mutual Information Analysis: How, When and Why? In *CHES*, volume 5747 of *LNCS*, pages 429–443. Springer, September 6-9 2009. Lausanne, Switzerland. 74, 77, 212, 229, 237, 321

[VCS11] Nicolas Veyrat-Charvillon and François-Xavier Standaert. Generic Side-Channel Distinguishers: Improvements and Limitations. In Rogaway [Rog11], pages 354–372. 212

[vEH14] Tim van Erven and Peter Harremoës. Rényi divergence and Kullback-Leibler divergence. *IEEE Trans. Inf. Theory*, 60(7):3797–3820, 2014. 248, 249, 251

[Ver15] Sergio Verdú. α-mutual information. In *2015 Information Theory and Applications Workshop, ITA 2015, San Diego, CA, USA, February 1-6, 2015*, pages 1–6. IEEE, 2015. 21, 249, 250, 251

[VGS14] Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert. Soft Analytical Side-Channel Attacks. In Sarkar and Iwata [SI14], pages 282–296. 58, 105

[VO07] Andrew J. Viterbi and Jim K. Omura. *Principles of digital communication and coding*. McGraw-Hill series in electrical engineering, 2007. ISBN 0070675163, 9780070675162. 27, 29

[VS09] Nicolas Veyrat-Charvillon and François-Xavier Standaert. Mutual Information Analysis: How, When and Why? In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, volume 5747 of *Lecture Notes in Computer Science*, pages 429–443. Springer, 2009. 5, 44, 53, 317

[vSMK+21] Stephan van Schaik, Marina Minkin, Andrew Kwong, Daniel Genkin, and Yuval Yarom. CacheOut: Leaking Data on Intel CPUs via Cache Evictions. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 339–354. IEEE, 2021. 9

[vW01] Manfred von Willich. A technique with an information-theoretic basis for protecting secret data from differential power attacks. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 44–62. Springer, 2001. 329

[WAGP20] Lennert Wouters, Victor Arribas, Benedikt Gierlichs, and Bart Preneel. Revisiting a methodology for efficient CNN architectures in profiling attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):147–168, 2020. 5

[WCG+22] Qianmei Wu, Wei Cheng, Sylvain Guilley, Fan Zhang, and Wei Fu. On Efficient and Secure Code-based Masking: A Pragmatic Evaluation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(3):192–222, 2022. 298, 300, 301, 302

[Wei] Eric W Weisstein. Cumulant. From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/Cumulant.html. 188

[Wie99] Michael J. Wiener, editor. *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa*

Barbara, California, USA, August 15-19, 1999, Proceedings, volume 1666 of *Lecture Notes in Computer Science*. Springer, 1999. 375, 386

[WMCS20] Weijia Wang, Pierrick Méaux, Gaëtan Cassiers, and François-Xavier Standaert. Efficient and Private Computations with Code-Based Masking. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(2):128–171, 2020. 6, 18, 256, 257, 259, 260, 264, 266, 280, 282

[WO11a] Carolyn Whitnall and Elisabeth Oswald. A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework. In Rogaway [Rog11], pages 316–334. 44, 49, 212, 213, 227, 230

[WO11b] Carolyn Whitnall and Elisabeth Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. *J. Cryptographic Engineering*, 1(2):145–160, 2011. 27, 34, 46, 72, 74, 85, 230, 311

[WO13] Carolyn Whitnall and Elisabeth Oswald. Profiling DPA: efficacy and efficiency trade-offs. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 37–54. Springer, 2013. 134

[WOM11] Carolyn Whitnall, Elisabeth Oswald, and Luke Mather. An Exploration of the Kolmogorov-Smirnov Test as a Competitor to Mutual Information Analysis. In Emmanuel Prouff, editor, *CARDIS*, volume 7079 of *Lecture Notes in Computer Science*, pages 234–251. Springer, 2011. 44, 74, 77, 138, 142, 212, 230

[WOS14] Carolyn Whitnall, Elisabeth Oswald, and François-Xavier Standaert. The Myth of Generic DPA ... and the Magic of Learning. In Benaloh [Ben14], pages 183–205. 27, 32, 34, 45, 57, 73, 82, 136, 137, 167, 212, 222

[WPH+22] Yingchen Wang, Riccardo Paccagnella, Elizabeth Tang He, Hovav Shacham, Christopher Fletcher, and David Kohlbrenner. Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on `x86`, August 10-12 2022. 31st USENIX Security Symposium. Boston, MA, USA. `https://www.hertzbleed.com/hertzbleed.pdf`. 9

[WS12] Xiaoyun Wang and Kazue Sako, editors. *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing,* *China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*. Springer, 2012. 370, 405

[WSM04] Isaac Woungang, Alireza Sadeghian, and William W. Melek. Bounds on the Minimum Distances of a Class of q-ary Images of q^m-ary Irreducible Cyclic Codes. In *Proceedings of the 2004 IEEE International Symposium on Information Theory, ISIT 2004, Chicago Downtown Marriott, Chicago, Illinois, USA, June 27 - July 2, 2004*, page 185. IEEE, 2004. 299

[WW04] Jason Waddle and David A. Wagner. Towards Efficient Second-Order Power Analysis. In Joye and Quisquater [JQ04], pages 1–15. 160, 192

[WYS+18] Weijia Wang, Yu Yu, François-Xavier Standaert, Junrong Liu, Zheng Guo, and Dawu Gu. Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips. *IEEE Trans. Inf. Forensics Secur.*, 13(5):1301–1316, 2018. 135, 136, 137, 148, 153, 160

[YE13] Xin Ye and Thomas Eisenbarth. On the Vulnerability of Low Entropy Masking Schemes. In Francillon and Rohatgi [FR14], pages 44–60. 281

[YM94] Xiang Yang and James L Massey. The condition for a cyclic code to have a complementary dual. *Discrete Mathematics*, 126(1):391–393, 1994. 17

[ZBHV20] Gabriel Zaid, Lilian Bossuet, Amaury Habrard, and Alexandre Venelli. Methodology for efficient CNN architectures in profiling attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(1):1–36, 2020. 5

[ZDFL15] Liwei Zhang, A. Adam Ding, Yunsi Fei, and Pei Luo. A Unified Metric for Quantifying Information Leakage of Cryptographic Devices Under Power Analysis Attacks. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 338–360. Springer, 2015. 243

[ZZSZ13] Hui Zhao, Yongbin Zhou, François-Xavier Standaert, and Hailong Zhang. Systematic Construction and Comprehensive Evaluation of Kolmogorov-Smirnov Test Based Side-Channel Distinguishers. In Robert H. Deng and Tao Feng, editors, *ISPEC*, volume 7863 of *Lecture Notes in Computer Science*, pages 336–352. Springer, 2013. 74, 122, 212, 317