

# Contents

<b>1</b>	<b>General Introduction</b>	1
1.1	Embedded Secure Device	4
1.2	Components Targeted in this Work	7
	References	7

## Part I Secure Embedded Devices and Their Side Channels

<b>2</b>	<b>Side-Channel Cryptanalysis: A Brief Survey</b>	11
2.1	Invasive Attacks	12
2.1.1	Micro-Probing	12
2.1.2	Reverse Engineering	12
2.1.3	Fault Attacks	12
2.2	Noninvasive Attacks	13
2.2.1	Timing Attack	13
2.2.2	Simple and Differential Power Analysis	13
2.2.3	Electromagnetic Analysis	14
2.3	Attacker's Taxonomy	14
2.4	Countermeasures	15
2.4.1	Software Level	15
2.4.2	Hardware Level	16
2.4.3	Logic Style	17
	References	17

## Part II Techniques of Measurements

<b>3</b>	<b>CMOS Devices: Sources and Models of Emanation</b>	23
3.1	Side-Channel Sources	24
3.1.1	Power Consumption in CMOS Devices	24
3.1.2	EM Emanations in CMOS Devices	25
3.2	Electromagnetic Probes	29

3.3	Leakage Models . . . . .	31
3.3.1	Hamming Distance Model . . . . .	31
3.3.2	Hamming Weight Model . . . . .	32
3.3.3	Signed Distance Model . . . . .	32
3.4	Consequences . . . . .	36
3.5	Conclusions . . . . .	37
	References . . . . .	39
<b>4</b>	<b>Measurement of the Power Consumption . . . . .</b>	<b>41</b>
4.1	The Equipment . . . . .	41
4.1.1	Frequency Content of a Trace: Choice of the Oscilloscope. . . . .	42
4.1.2	Measuring the Power Consumption. . . . .	44
4.2	Dealing with the Noise in the Trace . . . . .	45
4.3	Enhancement of the Power Consumption Measurement Process: De-embedding . . . . .	46
4.3.1	Leakage Chain Model . . . . .	48
4.3.2	De-embedding: ICEM Model . . . . .	48
4.4	Conclusions . . . . .	53
	References . . . . .	53
<b>5</b>	<b>Electromagnetic Leakage . . . . .</b>	<b>55</b>
5.1	Experimental Setup . . . . .	56
5.1.1	XYZ Table. . . . .	56
5.1.2	XY Scanning . . . . .	56
5.2	Near-Field EM Probes . . . . .	57
5.2.1	Magnetic and Electric Probes . . . . .	57
5.2.2	Experimental Results. . . . .	58
5.3	Infinite Wire Model. . . . .	59
5.3.1	The Integrated Circuit Geometry and Parameters . . . . .	61
5.3.2	Model Based on TE Waves . . . . .	61
5.4	Countermeasure: Is a Metallic Shield Relevant in this Respect?. . . . .	66
5.4.1	Circuit Layout . . . . .	67
5.4.2	Results. . . . .	67
5.5	Conclusions . . . . .	68
	References . . . . .	69
 <b>Part III Statistical Tools and Higher Order Attacks</b>		
<b>6</b>	<b>Statistical Tools . . . . .</b>	<b>73</b>
6.1	Trace and Method of Compression . . . . .	74
6.2	Non-profiled Leakage Analysis . . . . .	75

6.2.1	Identification of the Implementation Under Attack . . . . .	75
6.2.2	Selection of a Emanation Model . . . . .	76
6.2.3	Difference of Mean Test . . . . .	77
6.2.4	Correlation Analysis . . . . .	80
6.2.5	An Attack Using Measured Data. . . . .	83
6.2.6	Theoretical Predictions . . . . .	83
6.3	Device Profiled Leakage Function . . . . .	85
6.4	Key Profiled Leakage Function: Template Attack . . . . .	86
6.4.1	Template Attacks . . . . .	87
6.4.2	Improvement of the Profiling Process: Principal Component Analysis . . . . .	89
6.5	Template Attacks: Inner Versus External Current Traces . . . . .	92
6.5.1	Experimental Results on RC4. . . . .	93
6.6	Conclusions . . . . .	94
	References . . . . .	95
<b>7</b>	<b>Higher Order Attacks . . . . .</b>	<b>97</b>
7.1	The Masking Countermeasure . . . . .	98
7.2	Power Consumption Model. . . . .	99
7.3	Attack Description. . . . .	99
7.4	Simulated Attacks . . . . .	102
7.5	FPGA Results . . . . .	104
7.6	Conclusions . . . . .	106
	References . . . . .	107

## **Part IV Towards Theoretical Prediction of Side-Channel Analysis**

<b>8</b>	<b>Toward the Evaluation of an Implementation Against Side-Channel Attacks. . . . .</b>	<b>111</b>
8.1	Introduction . . . . .	111
8.2	Leakage Functions and Observations . . . . .	112
8.3	Model Specifications . . . . .	113
8.3.1	Target Implementation. . . . .	113
8.3.2	Leakage Function . . . . .	114
8.3.3	Adversarial Context. . . . .	114
8.3.4	Adversarial Strategy . . . . .	114
8.4	Evaluation Metrics. . . . .	114
8.4.1	Security: Average Success Rate of the Adversary . . . . .	114
8.4.2	Information Theoretic Metric: Conditional Entropy . . . . .	115
8.5	Investigation of Single Leakage . . . . .	116
8.5.1	Single Block Implementations . . . . .	116
8.5.2	Multiple Blocks and Key Guesses. . . . .	117
8.5.3	Noise Addition . . . . .	117

8.6	Investigation of Multiple Leakages . . . . .	119
8.6.1	Assuming Random S-Boxes . . . . .	119
8.6.2	Using Real Block Cipher Components. . . . .	120
8.7	Investigation of Masked Implementations. . . . .	121
8.8	Concluding Remarks . . . . .	127
	References . . . . .	128
<b>9</b>	<b>General Conclusion and Possible Further Directions . . . . .</b>	<b>129</b>
	References . . . . .	132
	<b>Appendix . . . . .</b>	<b>133</b>
	<b>Glossary . . . . .</b>	<b>135</b>
	<b>Index . . . . .</b>	<b>137</b>

<http://www.springer.com/978-1-4614-6782-3>

Advanced DPA Theory and Practice  
Towards the Security Limits of Secure Embedded  
Circuits

Peeters, E.

2013, XVI, 139 p., Hardcover

ISBN: 978-1-4614-6782-3