

# Contents

<b>List of Notations</b>	<b>v</b>
Cryptography . . . . .	v
Side-channel analysis . . . . .	v
Statistics . . . . .	vi
Sets and elements . . . . .	vi
List of Abbreviations . . . . .	vii
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>xi</b>
<b>List of Listings</b>	<b>xiii</b>
<b>1 Introduction</b>	<b>1</b>
<b>I Preliminary notions</b>	<b>5</b>
<b>2 Cryptography</b>	<b>7</b>
2.1 Ciphers . . . . .	8
2.1.1 Block ciphers . . . . .	10
2.1.2 Attacks on block ciphers . . . . .	17
2.2 Summary . . . . .	20
<b>3 Side-channel analysis</b>	<b>21</b>
3.1 Types of side-channel attacks . . . . .	22
3.1.1 Information channel . . . . .	22
3.1.2 Invasiveness . . . . .	24
3.1.3 Interference . . . . .	24
3.1.4 Profiled and unprofiled attacks . . . . .	26
3.1.5 Simple and differential analysis . . . . .	27
3.1.6 Summary of types of side-channel attacks . . . . .	28

3.2	Power analysis . . . . .	28
3.2.1	Acquisition setup . . . . .	29
3.2.2	Target operation . . . . .	35
3.2.3	Leakage model . . . . .	39
3.2.4	Distinguishers . . . . .	41
3.2.5	Key enumeration . . . . .	51
3.3	Analysis of side-channel attacks . . . . .	52
3.3.1	Performance of an attack . . . . .	53
3.4	Countermeasures . . . . .	55
3.4.1	Masking . . . . .	55
3.4.2	Hiding . . . . .	60
3.4.3	Other countermeasures . . . . .	61
3.4.4	Summary on countermeasures . . . . .	63
3.5	Summary . . . . .	64
<b>4</b>	<b>The problem of leakage detection</b>	<b>65</b>
4.1	Leakage detection . . . . .	66
4.2	Analysis during early stages . . . . .	68
4.3	Goals . . . . .	71
<b>II</b>	<b>Contributions</b>	<b>73</b>
<b>5</b>	<b>Simulation tools for side-channel analysis</b>	<b>75</b>
5.1	Motivation . . . . .	78
5.2	Levels of abstraction . . . . .	83
5.3	Survey of existing simulators . . . . .	86
5.3.1	Other works related to simulations . . . . .	94
5.4	Summary . . . . .	95
<b>6</b>	<b>SILK</b>	<b>97</b>
6.1	Description of the tool . . . . .	98
6.1.1	Parameters . . . . .	99
6.1.2	Discussion . . . . .	102
6.2	Evaluation of S-boxes . . . . .	104
6.2.1	Results based on theoretical metrics . . . . .	105
6.2.2	Experimental results on simulations . . . . .	106
6.2.3	Experimental results on a real device . . . . .	112
6.3	Improvement of S-boxes . . . . .	114
6.3.1	Genetic algorithms and search strategy . . . . .	114
6.3.2	Results for Correlation Power Analysis . . . . .	117
6.3.3	Results for Template Attacks . . . . .	121

---

6.3.4	Discussion . . . . .	122
6.4	Scalable shuffling schemes . . . . .	127
6.4.1	Extensions of random start index . . . . .	128
6.4.2	Reverse shuffle . . . . .	131
6.4.3	Sweep swap shuffle . . . . .	132
6.5	Analysis of shuffling schemes . . . . .	135
6.5.1	Randomization . . . . .	135
6.5.2	Number of shuffles . . . . .	137
6.5.3	Resources . . . . .	139
6.5.4	Resistance against side-channel attacks . . . . .	142
6.5.5	Applications & modifications . . . . .	147
6.5.6	Discussion . . . . .	147
6.6	Summary . . . . .	150
<b>7</b>	<b>ASCOLD</b>	<b>153</b>
7.1	Acquisition setup and evaluation . . . . .	154
7.2	ILA-Breaching Effects . . . . .	154
7.2.1	Overwrite effect . . . . .	155
7.2.2	Memory remnant effect . . . . .	156
7.2.3	Neighbour leakage effect . . . . .	158
7.3	Description of the tool . . . . .	161
7.4	1st order masked S-box for Rectangle cipher . . . . .	163
7.5	Summary . . . . .	168
<b>8</b>	<b>SAVRASCA</b>	<b>171</b>
8.1	Description of the tool . . . . .	172
8.2	Analysis of the DPA Contest 4 . . . . .	174
8.3	Analysis of AES-RSM used in DPA Contest 4 . . . . .	178
8.3.1	Mask bias . . . . .	178
8.3.2	Experimental results . . . . .	182
8.3.3	Balanced values for masks . . . . .	189
8.4	Note on DPA Contest 4.2 . . . . .	194
8.5	Summary . . . . .	196
<b>9</b>	<b>Conclusions</b>	<b>199</b>
<b>A</b>	<b>SILK example</b>	<b>207</b>
<b>B</b>	<b>Success rate of S-boxes using simulations</b>	<b>209</b>
<b>C</b>	<b>S-boxes generated using evolutionary computations</b>	<b>211</b>
C.1	Success rate of attacks on the S-boxes . . . . .	213

<b>D</b>	<b>Heatmaps of shuffling schemes</b>	<b>215</b>
<b>E</b>	<b>Success rates of attacks on shuffling schemes</b>	<b>221</b>
<b>F</b>	<b>ASCOLD example</b>	<b>225</b>
<b>G</b>	<b>List of microcontrollers supported by SAVRASCA</b>	<b>227</b>
	<b>Bibliography</b>	<b>229</b>