

Contents

Introduction	xi
1. Fault Attacks and Fault Models	1
1.1. Inducing Faults in the Physical World	2
1.1.1. Countermeasures	6
1.2. Characterizing Fault Models	7
1.3. Definition of Fault Types	9
1.4. Definition of Fault Models	12
1.4.1. Fault Models Affecting a Single Bit	14
1.4.2. Fault Models Affecting a Bounded Number of Bits	16
1.4.3. Fault Models Affecting an Arbitrary Number of Bits	19
1.5. Validity and Applicability of the Proposed Fault Models	22
1.6. Other Attack Scenarios	24
1.6.1. Code Change Attacks	24
1.6.2. Oracle Attacks	24
2. New Attacks on Plain RSA	29
2.1. The Differential Fault Attack on Right-To-Left Repeated Squaring	30
2.1.1. Flaws in the Plain RSA Attack	33
2.1.2. Correcting Algorithm 2.5 and Lemma 2.7.	35
2.2. An Attack on The Left-To-Right Repeated Squaring Algorithm	45
2.2.1. Fault Attack Starting From the MSBs	47
2.2.2. Fault Attack Starting From the LSBs	56
2.3. Concluding Remarks and Open Problems	70
3. A New Countermeasure Against Attacks on CRT-RSA	73
3.1. CRT-RSA and the Bellcore Attack	73
3.2. Countermeasures	78
3.2.1. Infective Errors	79
3.3. A New Countermeasure Against Random Faults	84
3.3.1. Efficiency Of The New Algorithm	86
3.4. Security Analysis of the Proposed Countermeasure	87
3.4.1. Undetectable Errors.	87
3.4.2. Excluding the Two Messages $m = 0$ and $m = 1$	92
3.4.3. Further Security Considerations	93
3.4.4. Summarizing the Results.	94
3.5. Adapting to Other Fault Models	94
3.5.1. Undetectable Faults in the Single Bit Fault Model	94

3.5.2.	Undetectable Faults in the Byte Fault Model	97
3.6.	Attacks Against our Proposed Algorithm	98
3.6.1.	Bit and Byte Faults	98
3.6.2.	Wagner’s Attack	100
3.7.	Concluding Remarks and Open Problems	101
4.	Fault Attacks on Elliptic Curve Cryptosystems	103
4.1.	Elliptic Curve Cryptography	103
4.1.1.	Affine Coordinates	104
4.1.2.	Projective Coordinates	106
4.1.3.	Elliptic Curve Cryptosystems	107
4.1.4.	Elliptic Curve Parameters in Practice	108
4.2.	Existing Fault Attacks on Elliptic Curve Cryptosystems	108
4.3.	Undetectable Faulty Points in Point Addition	111
4.3.1.	Examples for a Detailed Analysis of Undetectable Errors	112
4.4.	Attacks Inducing Undetectable Faults	115
4.4.1.	Faults Induced into Point Addition Using Random Faults	115
4.4.2.	Faults Induced into Point Addition Using Bit Faults	116
4.5.	Sign Change Faults	117
5.	Sign Change Faults — Attacking Elliptic Curve Cryptosystems	123
5.1.	Sign Change Attack on NAF-based Left-to-Right Repeated Doubling	124
5.1.1.	Sign Change Attack Targeting Q'_i in Line 4.	125
5.1.2.	Other Attacks	131
5.1.3.	Recovering The Bits Starting From The MSB	132
5.2.	Sign Change Attack on NAF-based Right-to-Left Repeated Doubling	135
5.2.1.	Sign Change Attack Targeting Q_i in Line 4.	135
5.2.2.	Other Attacks	136
5.2.3.	Recovering The Bits Starting From The MSB	138
5.3.	Attacks on the Standard Repeated Doubling Algorithms	138
5.4.	Sign Change Attack on Montgomery’s Binary Method	138
5.4.1.	Preliminaries	139
5.4.2.	Sign Change Attack Targeting $P1_{(i+1)}$	141
5.4.3.	False Positives	144
5.4.4.	Other Attacks	149
5.4.5.	Recovering The Bits Starting From The MSB	152
5.5.	Concluding Remarks	155
6.	Securing Elliptic Curve Cryptosystems	157
6.1.	Previously Proposed Countermeasures	157
6.2.	A New Countermeasure Against Sign Change Attacks	158
6.2.1.	On the Choice of E_p and E_t	159
6.2.2.	Analysis of the Countermeasure.	160
6.2.3.	Infective Computations	163

7. Sign Change Attacks — RSA Revisited	165
7.1. Sign Change Faults in Left-to-Right Repeated Squaring	166
7.2. Sign Change Faults in Right-to-Left Repeated Squaring	166
8. Conclusion and Open Problems	169
A. Detailed Fault Analysis of Affine Elliptic Curve Addition	171
A.1. Attacks Targeting $\lambda = (y_1 - y_2)/(x_1 - x_2)$	171
A.2. Attacks Targeting $x_3 = \lambda^2 - x_1 - x_2$	175
A.3. Attacks Targeting $y_3 = -y_1 + \lambda \cdot (x_1 - x_3)$	177
Bibliography	181
Symbols, Acronyms and Notation	189