

Contents

1	Introduction	1
1.1	Thesis Statement	3
1.1.1	Problem Statement	3
1.1.2	Thesis Contributions	4
1.2	Structure of the Thesis	5
2	Mathematical and Cryptological Background	7
2.1	Elliptic Curves and Bilinear Pairings	7
2.1.1	Elliptic Curves	7
2.1.2	Bilinear Pairings	11
2.2	Cryptographic Algorithms and Protocols	16
2.2.1	The Advanced Encryption Standard	16
2.2.2	Identity-Based Cryptography from Pairings	18
2.3	Side Channel Attacks	19
2.3.1	Timing Attacks	20
2.3.2	Power Analysis	21
2.3.3	Electromagnetic Analysis	22
2.3.4	Other Side Channels	22
2.4	Fault Attacks	23
2.4.1	RSA	23
2.4.2	Elliptic Curve Cryptography	24
2.4.3	Symmetric Cryptography	25
3	Photonic Emission Analysis	27
3.1	Photonic Emission	28
3.1.1	Photonic Emission in CMOS	28
3.1.2	Detection of Photonic Emission	29
3.1.3	Applications of Photonic Emission	31

3.2	Experimental Setups	32
3.2.1	The Target Devices	33
3.2.2	Emission Images	35
3.2.3	Spatial and Temporal Analysis	37
4	The Photonic Side Channel.	41
4.1	Simple Photonic Emission Analysis	43
4.1.1	Physical Attack	43
4.1.2	Cryptanalysis.	47
4.1.3	Countermeasures	59
4.2	Differential Photonic Emission Analysis	62
4.2.1	Physical Attack	62
4.2.2	Cryptanalysis.	65
4.2.3	Countermeasures	77
5	Higher-Order Fault Attacks Against Pairing Computations	79
5.1	Experimental Setup	81
5.1.1	Low-Cost Glitching Platform.	81
5.1.2	Instruction Skips	85
5.2	Physical Attack	85
5.2.1	Realization of Higher-Order Fault Attacks.	86
5.2.2	Second-Order Fault Attack Against the Eta Pairing	87
5.3	Cryptanalysis.	91
5.3.1	Modification of n in the Eta Pairing.	92
5.3.2	Modification of f in the Eta Pairing.	96
5.3.3	Modification of f in the Reduced Tate Pairing.	97
5.4	Countermeasures	100
6	Future Work	103
6.1	The Photonic Side Channel	103
6.1.1	Exploring the Full Attack Potential	103
6.1.2	Developing Countermeasures.	105
6.2	Fault Attacks Against Pairing-Based Cryptography.	106
6.2.1	Exploring the Full Attack Potential	107
6.2.2	Targeting Cryptographic Protocols	107
7	Conclusion.	109
7.1	The Photonic Side Channel	109
7.2	Fault Attacks Against Pairing-Based Cryptography.	110
7.3	Advice for Cryptographers	111
	References.	113

Why Cryptography Should Not Rely on Physical Attack
Complexity

Krämer, J.

2015, XXI, 122 p. 26 illus., 15 illus. in color., Hardcover

ISBN: 978-981-287-786-4