Contents

1 Introduction **9**

1.1 Previous work and knowledge 11

1.2 The subject of hardware security 13

1.3 Motivation and overview 17

2 Background **21**

2.1 Security evolution in silicon chips 23

2.1.1 Memory types 31

2.1.2 Types of security protection 43

2.2 Developers and attackers 47

2.3 Failure analysis techniques 49

3 Attack Technologies **52**

3.1 Introduction 52

3.1.1 Protection levels 53

3.1.2 Attack categories 56

3.1.3 Attack scenarios 57

3.2 Non-invasive attacks 58

3.3 Invasive attacks 59

3.4 Semi-invasive attacks 62

4 Non-Invasive Attacks **64**

4.1 Obscurity vs security 65

4.2 Timing attacks 66

4.3 Brute force attacks 67

4.4 Power analysis 69

4.5 Glitch attacks 73

4.5.1 Clock glitches 73

4.5.2 Power glitches . . . 75
4.6 Data remanence . . . 76
4.6.1 Low temperature data remanence in SRAM . . . 77
4.6.2 Data remanence in non-volatile memories . . . 81
4.6.3 Requirements for reliable data deleting from memory . . . 88

5 Invasive Attacks 90

5.1 Sample preparation . . . 90
5.1.1 Decapsulation . . . 91
5.1.2 Deprocessing . . . 95
5.2 Reverse engineering . . . 98
5.2.1 Optical imaging for layout reconstruction . . . 98
5.2.2 Memory extraction . . . 100
5.3 Microprobing . . . 102
5.3.1 Laser cutter . . . 104
5.3.2 FIB workstation . . . 106
5.4 Chip modification . . . 107

6 Semi-Invasive Attacks 109

6.1 UV attacks . . . 110
6.1.1 Locating the security fuses . . . 110
6.1.2 Toothpick attack . . . 111
6.1.3 EEPROM and Flash issues . . . 113
6.2 Backside imaging techniques . . . 114
6.3 Active photon probing . . . 117
6.3.1 Laser scanning techniques . . . 119
6.3.2 Reading the logic state of CMOS transistors . . . 120
6.4 Fault injection attacks . . . 122
6.4.1 Changing SRAM contents . . . 122
6.4.2 Non-volatile memory contents modification . . . 127
6.5 Modelling the attacks . . . 129
6.5.1 Modelling the logic state reading . . . 129
6.5.2 Modelling the fault injection attack . . . 131

7 Hardware Security Analysis **134**

7.1 Evolution against UV attacks 134

7.2 Semi-invasive analysis of different security implementations 136

7.2.1 Using laser scanning technique for analysis 137

7.2.2 Using fault injection technique for analysis 138

8 Defence Technologies **140**

8.1 Unmarking, remarking and repackaging 141

8.2 Multilevel and multipoint protection 143

8.3 Burning access circuit and destroying test interface 145

8.4 Smartcards and tamper protection 147

8.5 Asynchronous logic 148

9 Conclusion and Further Work **150**

Appendix. Overview of different microcontrollers and smartcards **155**

Glossary **157**

Bibliography **161**