CONTENTS

INTRODUCTION 5

1 MOTIVATION 6

1.1 Goals 6

1.2 Contribution 7

2 POWER ANALYSIS FUNDAMENTALS 10

2.1 Profiling Power Analysis Attacks 11

2.1.1 Standart Template Attack 11

2.1.2 Template Attack Based on Machine Learning 16

2.2 Non-profiling Power Analysis Attacks 21

2.3 Countermeasure Methods 26

2.3.1 Hiding 26

2.3.2 Masking 29

3 STUDY OF PROTECTED IMPLEMENTATIONS 31

3.1 DPA Contest V4.1 32

3.1.1 Description of Countermeasures Implementation 33

3.1.2 Power Analysis Realized 34

3.2 DPA Contest V4.2 39

3.2.1 Description of Countermeasures Implementation 40

3.2.2 Power Analysis Realized 43

3.3 Protected Hardware Implementation 55

3.3.1 State of the Art 57

3.3.2 Contribution 58

3.3.3 Preliminaries and System Architecture 59

3.3.4 Authentication Subsystem Implementation 61

3.3.5 FPGA Subsystem Implementation 62

3.3.6 Summary 67

4 CONCLUSION 70

BIBLIOGRAPHY 71