UNIVERSITY NAME

DOCTORAL THESIS

Thesis Title

Author:
John SMITH

Supervisor:
Dr. James SMITH

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy

in the

Research Group Name
Department or School Name

August 24, 2017

Contents

List of Figures

List of Tables

List of Abbreviations

SCA **S**ide **C**hannel **A**ttack

List of Symbols

Chapter 1

Introduction

1.1 Introduction to Cryptography

1.1.1 Secret-Key Cryptography

1.1.2 Public-Key Cryptography

1.2 Secure Hardware and Embedded Cryptography

1.2.1 The Example of the Smart Card

1.2.2 Certification of a Secure Hardware

1.2.3 Modern More Complex Devices to Certify

1.2.4 Embedded Cryptography Vulnerabilities

Chapter 2

Introduction to Side-Channel Attacks

2.1 Introduction to Side-Channel Attacks

2.1.1 Historical Overview

2.1.2 Terminology and Generalities

Target and Leakage Model

Points of Interest

Simple vs Advanced SCAs

Vertical vs Horizontal SCAs

Profiled vs Non-Profiled SCAs

Side-Channel Algebraic Attacks

Distinguishers

SCA Metrics

2.1.3 Side-Channel Attacks vs Machine Learning

Distinguishers vs Classifiers

2.2 Main Side-Channel Countermeasures

2.2.1 Masking

2.2.2 Shuffling

2.2.3 Random Delays and Jitter

2.3 Higher-Order Attacks

2.3.1 Higher-Order Moments Analysis and Combining Functions

2.3.2 Profiling Higher-Order Attacks

Profiling with Masks Knowledge

Profiling without Masks Knowledge

2.4 Thesis Contribution and Organization

2.4.1 Foreword of this Thesis: Research of Points of Interest

2.4.2 Dimensionality Reduction Approach

Linear Methods for First-Order Attacks

Chapter 3

Points of Interest and Dimensionality Reduction

3.1 Motivations

3.1.1 The Curse of Dimensionality

3.2 Selection on Points of Interest: Classical Statistics

3.3 Related Issues: Leakage Detection and Leakage Assessment

3.4 Observations Leading to Take a Dimensionality Reduction Approach

Chapter 4

Linear Dimensionality Reduction

Chapter 5

Kernel Dimensionality Reduction

5.1 Motivation

5.1.1 Higher-Order Attacks

Higher-Order Version of Projection Pursuits

5.2 Kernel Function and Kernel Trick

5.2.1 Local Kernel Functions as Similarity Metrics

5.3 Kernel Discriminant Analysis

5.4 Experiments over Atmega328P

5.4.1 The Regularization Problem

5.4.2 The Multi-Class Trade-Off

5.4.3 Multi-Class vs 2-class Approach

5.4.4 Asymmetric Preprocessing/Attack Approach

Comparison with Projection Pursuits

Chapter 6

Machine Learning Approach

6.1 Motivation

6.2 Introduction to Machine Learning

6.2.1 The Task, the Experience and the Performance

6.2.2 Supervised, Semi-Supervised, Unsupervised Learning

6.2.3 Training, Validation and Test Sets

6.2.4 Underfitting, Overfitting and Regularization

6.2.5 Data Augmentation

6.2.6 No Free Lunch Theorem

6.3 Machine Learning Applications in Side-Channel Context

6.3.1 Profiled Attack as a Classification Problem

Support Vector Machine

Random Forest

6.4 Artificial Neural Networks

6.4.1 Motivations Leading from Kernel Machines to Deep Learning

6.4.2 The Multi-Layer Perceptron

6.5 Simulated Experiment for Profiled HO-Attacks

6.5.1 The Simulations

6.5.2 Comparison between KDA and MLP

6.6 Real-Case Experiments over ARM Cortex-M4

Chapter 7

Convolutional Neural Networks against Jitter-Based Countermeasures

Chapter 8

Neural Networks: Back to Dimensionality Reduction

Chapter 9

Conclusions and Perspectives

9.1 Summary

9.2 Strengthen Embedded Security: the Main Challenge for Machine Learning Applications