Abstract

Resumo

Contents

List of Tables

List of Figures

Listings

List of Algorithms

Acronyms

Chapter 1

Introduction

1.1 Context

1.2 Motivation

1.3 Contribution

1.4 Structure of the Dissertation

Chapter 2

Background

This chapter introduces various concepts that are essential for understanding the later sections of this dissertation.

Chapter 3

High Assurance Cryptography

Chapter 4

Jasmin

This chapter provides an overview of the most relevant features of the Jasmin framework. Jasmin [1, 2] is a verfication-friendly, low-level framework suitable for writing high-assurance and high-speed cryptographic implementations.

Chapter 5

Implementation

In this chapter, we describe the Jasmin implementation of a type-checked big number library which is proven to be resistant against Spectre v1 attacks.

Chapter 6

Conclusion & Future Work

This chapter provides a succinct summary and draws conclusions based on the work done.

Future Work

Appendix A

Notation

$\mathbb{Z}_n^*$	Multiplicative group of integers modulo n
$\mathbb{F}_q$	Finite field with q elements
$E(\mathbb{F}_p)$	Elliptic curve defined over the prime field $\mathbb{F}_p$
$\mathcal{O}$	The point at infinity of an elliptic curve

Appendix B

Benchmarks

Bibliography

[1] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, and Pierre-Yves Strub. Jasmin: High-Assurance and High-Speed Cryptography. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 18071823, New York, NY, USA, 2017. Association for Computing Machinery. ISBN: 9781450349468. doi:10.1145/3133956.3134078.

[2] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Vincent Laporte, Tiago Oliveira, and Pierre-Yves Strub. The last mile: High-assurance and high-speed cryptographic implementations. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 965–982. IEEE, 2020.