

Constant-time Jasmin Library for Cortex-M4

Advisor: **Selim Kirbiyik**

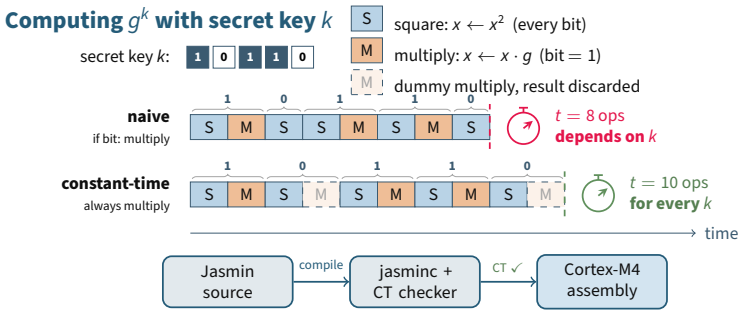
Motivation

Attackers can learn about a secret being computed by measuring the time it takes to compute a function. Hence having constant-time implementations of algorithms is crucial. Jasmin is a language which can generate and certify an implementation as being constant time. For embedded devices such as Cortex-M4 there is no existing library which designers can utilize.

In this topic, you will explore performant constant time designs for embedded applications. Cortex-M4 offers instructions which allow fast arithmetic with specific word-sizes. Constructing a parametric Jasmin library of cryptographic primitives will lower the barrier towards having secure embedded implementations.

Goals and Tasks

- Understand constant-time implementations
- Explore the design space for fast constant time primitives
- Construct constant-time Jasmin cryptographic primitives library



An example showing CT versus non-CT execution.

Literature

- T. Pornin
  BearSSL - Constant-Time Crypto
  www.bearssl.org/constanttime.html

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE

Prerequisites

- Interest in secure implementations
- Programming (Cortex-M4 Assembly, C/C++, Python)

Advisor Contact

selim.kirbiyik@tugraz.at