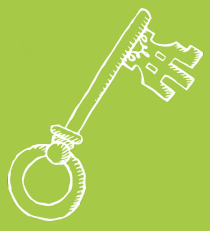


Masking the Extended Euclidean Algorithm

Advisor: **Maciej Czuprynko**

Motivation

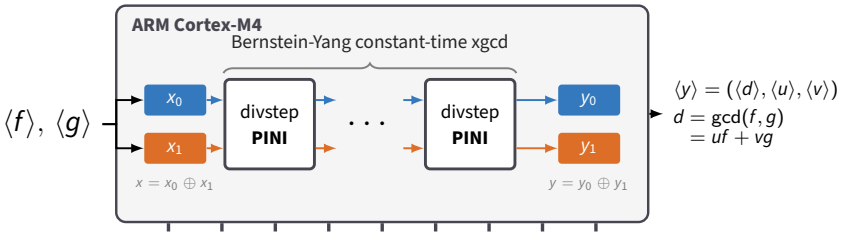
A sufficiently powerful quantum computer would break today's digital signature schemes. In response, NIST launched a call for post-quantum signatures, prompting several new candidates. One of them, SQIsign, is an isogeny-based scheme with the most compact keys and signatures.

Implementations on physical devices must also resist side-channel attacks that exploit leakage such as power consumption. A common countermeasure is masking, which splits secrets into randomized shares so that individual observations reveal nothing. Masked implementations are typically built from gadgets satisfying composable security notions such as Probe-Isolating Non-Interference (PINI), which guarantees they can be combined securely.

Since masking all of SQIsign is beyond the scope of a single project, we focus on one core building block: the extended Euclidean algorithm (xgcd), which computes the greatest common divisor (gcd) together with the Bézout coefficients. Specifically, we consider the constant-time Bernstein–Yang algorithm.

Goals and Tasks

- Get familiar with masking, PINI gadgets and the Bernstein-Yang xgcd algorithm.
- Implement a PINI secure xgcd on a Cortex-M4 microcontroller.
- Evaluate the side-channel resistance of the implementation using TVLA.
- Optimize the masked implementation.



Literature

- D. J. Bernstein et al.
  Accelerating and verifying constant-time modular inversion
  EUROCRYPT 2026
- G. Cassiers and F. Standaert
  Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference
  IEEE Trans. Inf. Forensics Secur. 2020

Courses & Deliverables

☑ **Master Project**
- Project code
- Report
- Presentation

– OR –

☑ **Master's Thesis**
- Initial presentation
- Project code
- Thesis (60+ pages)
- Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in PQC
- Knowledge of Python, C/C++ and ARM assembly
- "Side-Channel Security" course is recommended

Advisor Contact

maciej.czuprynko@tugraz.at