Max Planck Institute for Security and Privacy, Kookmin University, Kookmin University

Artifact Packaging with the Absence of the Target Hardware in Mind

Vincent Hwang, YoungBeom Kim, and Seog Chung Seo

September 9, 2025

Our work

Performance improvement (cycle count) of lattice-based cryptosystems

- Dilithium and
- Saber.

Platforms.

- Board `nucleo-f207` with a Cortex-M3 processor (ISA: Armv7-M).
  - Bare-metal target.
  - Board-dependent configurations.
- 8-bit AVR (in software emulation env.).

For more information, see:

- Paper:
  - `https://tches.iacr.org/index.php/TCHES/article/view/11926`
  - PQC (Software), Sept. 15.
- Artifact: `https://github.com/vincentvbh/PolyMul_Without_PowerfulMul`

Our artifact

Ideally, the following suffices.

- A `nucleo-f207` with a Cortex-M3 processor.
- Software: cross-compiler, ...

In reality, people face several issues.

- Access to a non-`nucleo-f207` board with a Cortex-M3.
  - Generate configuration files from `libopencm3`.
  - Reproduce cycle counts.
- No access to a board with a Cortex-M3.
  - Software emulation.
  - Correctness: functionality and test vectors.

Thanks for listening