

Comparing Latency of Ciphers in Hardware

Advisor: **Simon Gerhalter**

Motivation

The uKNIT framework constructs ciphers round by round, allowing each round to use different components, which are optimized for both cryptographic strength and low latency. During this automated search, candidate designs are ranked by latency estimates obtained with an open-source RTL-to-GDS flow on the open SkyWater 130 nm PDK. In contrast, latency comparisons in the literature are mostly based on the academic NanGate 15 nm Open Cell Library combined with proprietary synthesis tools such as Synopsys Design Compiler. It is unclear whether the open-source flow ranks ciphers in the same way.

The goal of this thesis is to collect publicly available hardware implementations of established low-latency ciphers, evaluate them with LibreLane, and compare the resulting *relative* latencies with published NanGate 15 nm results. Deviations in the ranking will be analyzed to identify their causes (cell library composition, synthesis tool, constraints, or the definition of latency) and to assess how reliable open-source flows are for latency-driven cipher design.

Goals and Tasks

- Get familiar with low-latency cipher design, unrolled hardware implementations, and the LibreLane flow
- Collect and verify fully unrolled implementations of representative ciphers (PRINCE, Midori, etc.)
- Define a consistent measurement methodology (latency definition, constraints, synthesis settings) and automate the evaluation
- Compare the obtained ranking with published NanGate 15 nm results
- Analyze the causes of deviations, e.g. by restricting the cell library or varying synthesis strategies

Literature

- K. Hu et al.
  uKNIT: Breaking Round-Alignment for Cipher Design
  IACR Transactions on Symmetric Cryptology 2026
  doi:10.46586/tosc.a0zo-4njsuvm
- https://github.com/librelane/librelane

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 ☑ SEM

Prerequisites

- Interest in cipher and hardware designs
- Programming

Advisor Contact

simon.gerhalter@tugraz.at