

YOU are Speed: Ultra Fast Side-channel Secure Masked Circuits




Advisor: **Rishub Nagpal**

Motivation

Masking is a fundamental technique to protect cryptographic circuits from leaking secret-data via side-channels. In hardware, masking incurs a severe performance penalty and disrupts efficient pipeline architectures due to the need for security-critical registers. These registers stop circuit glitches which could leak secret data through power side-channels. So-called “low-latency” masking architectures aim to eliminate these registers by introducing asynchronous circuit design techniques and dual-rail logic.

The main challenge in low-latency masking is to develop something that can be implemented in a generic fashion (i.e., with minimal backend layout restrictions) and still be secure. Thus, the goal of this thesis is to investigate new developments in low-latency masking and propose new architectures which can be both secure and very fast.

Goals and Tasks

-  Get familiar with the state-of-the-art in low-latency hardware masking
-  Develop a new masking scheme
-  Evaluate your new masking scheme with practical evaluation and formal proofs.



Literature

- > R. Nagpal et al.
Riding the Waves Towards Generic Single-Cycle Masking in Hardware
<https://doi.org/10.46586/tches.v2022.i4.693-717>
- > Z. Zhang, S. Petkova-Nikova, and V. Nikov
Glitch-Stopping Circuits: Hardware Secure Masking without Registers
<https://doi.org/10.1145/3658644.3670335>

Courses & Deliverables

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

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in side-channel attacks and hardware design
- > Programming in Verilog

Advisor Contact

rishub.nagpal@tugraz.at