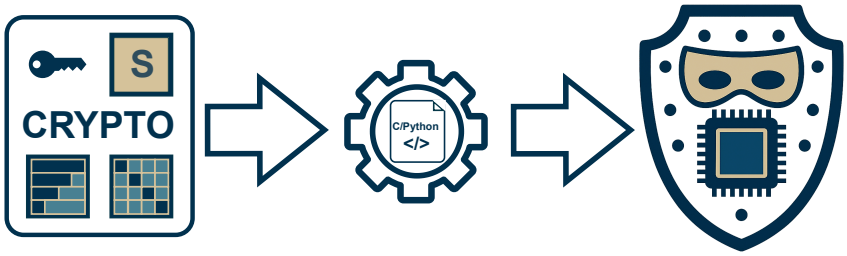
# Advancing Automated Masking: Generation of Full Cipher Logic for Side-Channel Secure Hardware




Modern cryptography provides confidentiality and integrity for digital systems, and its mathematical foundations make standardized algorithms highly resistant to brute-force and analytical attacks. However, when deployed in software or hardware, implementations may leak sensitive information through physical side channels. Since pioneering work of Kocher *et al.* [1] on power analysis, a significant research effort has focused on securing cryptographic implementations against such leakage. Masking has emerged as the dominant countermeasure: by splitting intermediate values into random shares, it prevents an attacker from learning secrets from power or electromagnetic measurements. Despite its strong theoretical guarantees, masking is challenging in practice—designers must preserve the algorithm's mathematical structure, ensure secure composability of components, and manage trade-offs in area, latency, and randomness.

To support engineers, several automated approaches for generating masked hardware have been proposed in recent years. Tools such as AGEMA [2] automatically replace an insecure register-transfer level (RTL) description of logic gates (AND, XOR) with composable masked gadgets, EASI-Mask [3] derives masked designs from high-level algorithmic descriptions, while works like AGMNC [4] focus on masked generation of nonlinear components. A recent technique, Uniform Sharing in Multiple Stages [5], follows the same approach, enabling generating masked RTL directly from lookup-table representations. However, this approach currently automates only the nonlinear parts of block ciphers, with linear layers still handcrafted.

The goal of this thesis is to extend the Uniform Sharing in Multiple Stages methodology. The student will first verify the authors' claims of applicability to arbitrary functions and then extend the toolchain to automatically generate masked linear layers for full cipher states, not only S-boxes. The next step is enabling automatic generation of the control logic, producing complete masked hardware designs. These designs will be evaluated using formal verification frameworks and statistical leakage assessment. Depending on the student's background and interests, there are several possible directions for progressing with the topic: students may synthesize and test masked implementations in COSIC's hardware security lab, investigate the unification of existing auto-generation methods, study optimization strategies for masked circuits, or propose their own improvements in consultation with the daily supervisor.

[1] `https://doi.org/10.1007/3-540-48405-1_25`; [2] `https://doi.org/10.46586/tches.v2022.i1.589-629`; [3] `https://doi.org/10.23919/DATE56975.2023.10137330`; [4] `https://doi.org/10.1007/978-3-031-61486-6_19`; [5] `https://eprint.iacr.org/2026/079`.

## Practicalities


| | |
|---|---|
| Promotors: | Prof. Dr. Ir. Vincent Rijmen, Dr. Svetla Nikova |
| Daily supervisor: | Artemii Ovchinnikov artemii.ovchinnikov@esat.kuleuven.be office B01.11 |
| Nature of the work: | 20% literature, 20% hardware, 60% software |
| Number of students: | 1 |


 © 2026 – 2027 COSIC