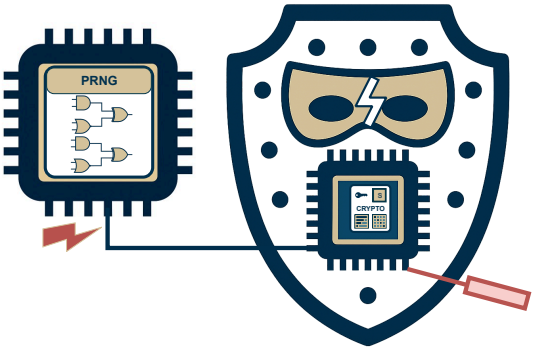
Evaluating Fault Impact on PRNGs and Side-Channel Security of Masking



Fault (FA) and side-channel (SCA) attacks are powerful physical threats to cryptographic hardware implementations. SCA aim to violate confidentiality by passively observing information leaked through physical emanations such as power consumption or electromagnetic radiation. FA, in turn, can target both confidentiality and integrity by actively injecting faults, e.g., via voltage/clock glitches, or laser irradiation, thus inducing erroneous computations exploitable by the attacker. While *masking countermeasures*, based on secret sharing schemes, aim to mitigate side-channel leakage by incorporating fresh randomness, in hardware this randomness is often generated internally by pseudo-random number generators (PRNGs). Thus, their integrity becomes a critical component of the overall security of masked designs.

This project investigates combined attacks targeting implementations that use PRNGs to provide fresh randomness for the masked cipher. The attacker is assumed to be capable of applying a single fault to the PRNG while simultaneously performing first-order leakage evaluation (e.g., using Test Vector Leakage Assessment, TVLA). By faulting the PRNG state, the adversary may induce widespread correlations among random bits that feed the masking scheme, thereby indirectly reducing the randomness quality and increasing leakage detectability.

The thesis project will be based on the analysis of implementations claiming SCA security through randomness refreshing. The work will evaluate how different fault scenarios affect the distribution of generated random bits and how this degradation propagates into the masked cryptographic computation. Leakage will be assessed using TVLA, potentially complemented by differential analysis of the PRNG state transitions to characterize the statistical impact of specific faults. If successful, such an attack would reveal an essential dependency between PRNG integrity and composable masking security. It would demonstrate that protecting randomness generation, possibly through fault-resistant or combined countermeasures, can contribute to the overall robustness of secure implementations. Experimental comparisons will be made between:

- Designs with faulted or unprotected PRNGs,
- Designs employing secure PRNGs,
- Designs using static (non-refreshing) countermeasures without internal PRNG.

These experiments will help determine whether securing the PRNG increases area and performance overheads beyond those of statically protected implementations, thus informing the trade-offs in composable hardware security.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen, Dr. Svetla Nikova		
Daily supervisor:	Dilara Toprakhisar	dilara.toprakhisar@esat.kuleuven.be	office B01.05
	Artemii Ovchinnikov	artemii.ovchinnikov@esat.kuleuven.be	office B01.11

Nature of the work:	20% literature, 20% theoretical work, 60% hardware
Number of students:	1

 © 2026 – 2027 COSIC