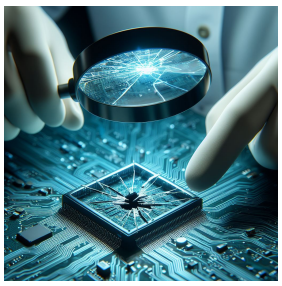
Evaluating Fault Countermeasure Techniques in the (General) Random Fault Model



Fault attacks pose a serious threat to the practical security of cryptographic implementations, where an adversary deliberately perturbs a cryptographic device to induce faulty computations and extract secret information. Over the years, several fault models have been proposed to formalize the capabilities of such adversaries and to guide the design of countermeasures. Among them, the threshold fault model is one of the most widely used due to its analytical simplicity: it assumes that the attacker can inject at most a limited number of faults in the target design. While this assumption allows clear theoretical reasoning, it does not accurately reflect physical fault injection, where techniques such as laser, electromagnetic, or voltage glitching can induce multiple, possibly correlated, faults in a single fault injection event.

To better capture such behavior, random fault models introduce a probabilistic view of fault injections. The random fault model can be seen as the probabilistic counterpart of the threshold fault model, where each injected fault occurs with a fixed probability. In the uniform random fault model, the adversary can inject faults across the whole circuit but lacks precise control over their location; each fault occurs independently with the same probability. The general random fault model extends this abstraction by assigning varying probabilities to different combinations of faults, providing a more realistic abstraction of physical attacks. Recently, the tool FIESTA [1] has been proposed to analyze countermeasures within this framework. Instead of exhaustively exploring all input–fault combinations, it randomly samples them to estimate bounds on the adversary's advantage.

This proposal aims to analyze and compare several countermeasure techniques implemented using Verilog/VHDL under these probabilistic models using FIESTA. By studying how they behave relative to the threshold model, the project seeks to better understand which countermeasures remain robust when fault injections follow more realistic, random distributions.

Practicalities

Promotor:	Prof. Dr. Ir. Vincent Rijmen
	Dr. Svetla Nikova
Daily supervisor:	Dilara Toprakhisar dilara.toprakhisar@esat.kuleuven.be office B01.05
Nature of the work:	30% literature, 10% theoretical work, 60% software
Number of students:	1

[1] https://github.com/ChairImpSec/FIESTA

 © 2026 – 2027 COSIC