# The relevance and challenges of random probing security for post-quantum algorithms. Application to Raccoon signature scheme.

Mélissa Rossi*[1]

[1]CryptoExperts – CryptoExperts – France

**Résumé**

The random probing model is a side-channel security model that formalizes a leakage scenario where each wire in a circuit leaks with a fixed probability p. This model has practical relevance as it can be reduced to the noisy leakage model, which is widely recognized as the appropriate framework for power and electromagnetic side-channel attacks. While straightforward to describe, it is more challenging to achieve provable security and efficiency within this model, especially compared to the t-probing model (where the attacker gets the value of at most t probes of its choice).
I will introduce the various security notions associated with this model and explain why they are difficult to apply to concrete algorithms. Together with my co-authors, Sonia Belaïd and Matthieu Rivain, we provided the first fully secure instantiation of a post-quantum algorithm in the random probing model (presented in Eurocrypt 2025). Specifically, we focused on Raccoon, whose masking-friendly structure makes it an ideal starting point. However, the performance remains underwhelming, particularly in terms of randomness consumption.
All in all, I aim to convince you that random probing is the future of side-channel security, and a lot of exciting work still lies ahead.

*Intervenant