Towards a Constant Leakage Rate: Verifying Security in the Random-Probing Model

Sara Sahraee*[1]

[1]LIRMM – Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier – France

Résumé

Masking is one of the most commonly used countermeasures against side-channel attacks. Efficiently evaluating the security of masked cryptographic schemes against a side-channel adversary is, however, a non-trivial task. Many works perform masking proofs in the t-probing model. This model enables a relatively straightforward security analysis, but has the drawback of failing to capture horizontal attacks, in which a side-channel adversary can exploit the repeated manipulation of shared values to retrieve the secrets.

The random-probing model was introduced as an intermediary step in the reduction of the t-probing model to the more realistic noisy leakage model. It is parametrised by a certain leakage rate p, and is able to capture the notion of noise in leaking schemes as well as horizontal attacks. Several recent works have focused on optimising this leakage rate, in particular by focusing on the construction of masked schemes which tolerate a constant leakage rate, i.e. not dependant on the masking order.

In this talk, we present our ongoing work on the verification of the leakage rate of gadgets in recent literature. We explore the random-probing security of several multiplication gadgets built to resist horizontal attacks, whose prior security claims were mostly heuristic. This evaluation is done using automatic verification tools (IronMask, STRAPS, PERSEUS, . . .) to compute the tolerated leakage rate of the gadgets. We present the performances and limitations of such tools as well as analysing their optimality when compared to theoretical analyses. Finally, we discuss the bottlenecks in the computation of random-probing security and provide some insights into alternative approaches.

*Intervenant