Secure and Verified Cryptographic Implementations in The Random Probing Model

Abdul Rahman Taleb[1,2]

[1] CryptoExperts, France
[2] Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

abdul.taleb@cryptoexperts.com

The masking countermeasure is among the most powerful countermeasures to counteract side-channel attacks. Leakage models have been exhibited to theoretically reason on the security of such masked implementations. So far, the most widely used leakage model is the probing model defined by Ishai, Sahai, and Wagner (CRYPTO 2003). While it is advantageously convenient for security proofs, it does not capture an adversary exploiting full leakage traces as, e.g., in horizontal attacks. Those attacks target the multiple manipulations of the same share to reduce noise and recover the corresponding value. To capture a wider class of attacks, another model was introduced and is referred to as the random probing model. From a leakage parameter p, each wire of the circuit leaks its value with probability p. This model enjoys practical relevance thanks to a reduction to the noisy leakage model, which is admitted as the suitable formalization for power and electromagnetic side-channel attacks. In addition, the random probing model is much more convenient than the noisy leakage model to prove the security of masking schemes. While this model much better reflects the physical reality of side channels, it requires more complex security proofs and does not yet come with practical constructions, which is why the community is starting to study this model and assess its convenience.

During the presentation, I will give an overview of the framework introduced by Belaïd, Coron, Prouff, Rivain, and Taleb (CRYPTO 2020) to generate random probing secure circuits, and which was later improved by Belaïd, Rivain, and Taleb (EUROCRYPT 2021) and by Belaïd, Rivain, Taleb and Vergnaud (ASIACRYPT 2021). Namely, I will exhibit the security analysis for circuits in the random probing model, introducing formal notions such as (p, ε)-random probing security where ε would represent a certain "failure event probability". I will also talk about the random probing expansion strategy which aims to arbitrarily amplify the security level of any circuit. The corresponding so-called expanding compiler somehow extends base gadgets (*i.e.* circuits) as soon as they satisfy a notion called random probing expandability (RPE). Introduced in (CRYPTO 2020), it was later improved with tighter properties and improved complexities in (EUROCRYPT 2021) and (ASIACRYPT 2021). In particular, the best practical instantiation of the compiler yet reaches a complexity of $\mathcal{O}(\kappa^{3.9})$, for a κ-bit security, while tolerating a leakage probability of $p = 2^{7.5}$. Some generalized constructions improve on the asymptotic complexity of the compiler to achieve quasi-linear asymptotic complexity with an increasing number of shares. Thanks to the promising potential of this expansion strategy and its limitations exhibited in these works, it has opened the door for many open questions and room for improvements.