Étude de méthodes de preuves de contre-mesures face aux attaques par canaux auxiliaires dans le Random Probing Model

Ghozlane Boukacem*[1,2]

[1]CryptoExperts – Sonia Belaïd, Mélissa Rossi – France
[2]LIP6 Sorbonne Université – Damien Vergnaud – France

Résumé

Les implémentations concrètes d'algorithmes cryptographiques sont souvent vulnérables à des attaques exploitant des fuites physiques, telles que la consommation d'énergie ou le temps d'exécution, appelées " attaques par canaux auxiliaires ". Pour y résister, une contre-mesure largement utilisée consiste à appliquer des techniques de masquage, où chaque donnée sensible est divisée en plusieurs parts aléatoires afin de rendre toute observation partielle inexploitables.
Cependant, prouver rigoureusement la sécurité de ces implémentations reste un défi majeur. Parmi les cadres formels existants, le Random Probing Model (RPM) s'est imposé comme un modèle réaliste, permettant de raisonner sur la probabilité qu'un attaquant observe certaines fuites tout en conservant un lien fort avec des modèles physiques plus concrets.

Le présent travail repose principalement sur la méthode des leakage diagrams, un formalisme graphique permettant de représenter les dépendances entre les variables internes d'un circuit et d'identifier les chemins critiques de fuites. Dans ce cadre, nous avons étudié deux gadgets réalisant des opérations fondamentales conçues spécifiquement pour le RPM : pRef (parallel Refresh), destiné à ré-randomiser les parts pour casser les corrélations, et Mult, qui réalise une multiplication sécurisée sur données masquées.

La sécurité de ces gadgets est quantifiée à l'aide d'une borne issue des travaux de la littérature. Nous avons cherché à affiner cette expression afin d'obtenir des estimations plus précises, en explorant plusieurs pistes combinatoires. Certaines se sont révélées prometteuses et ont été discutées avec l'un des auteurs du modèle étudié, mais les formalisations complètes restent à établir.
Ces travaux constituent une première étape vers une compréhension plus fine de la sécurité des circuits masqués et ouvrent la voie à des analyses plus précises dans le RPM. Ils s'inscrivent dans la continuité des recherches que je poursuis désormais dans le cadre de ma thèse au sein de CryptoExperts et de Sorbonne Université.

*Intervenant