Formalisme des attaques physiques

Hélène Le Bouder
encadrée par Bruno Robisson, dirigée par Assia Tria

3 avril 2013

Un algorithme cryptographique peut être prouvé sécurisé mathématiquement, en le ramenant à un problème juger difficile. Cependant, une fois implémenté dans un circuit, on peut attaquer les failles de ce dernier. On parle alors d'attaques physiques. Les attaques physiques s'opposent à la cryptanalyse classique. Elles ne permettent pas d'attaquer l'algorithme en soit mais son implémentation matérielle.

Il existe deux grandes familles d'attaques physiques différentes : canaux auxiliaires et injection de fautes. Les attaques par canaux auxiliaires se basent sur l'observation du circuit en cours de fonctionnement. Les attaques par injection de fautes analysent l'effet d'une perturbation intentionnelle sur le fonctionnement du circuit. Bien que leur principes semblent différents, nous montrons l'existence d'un formalisme qui permet d'unifier toutes ces attaques. Ce formalisme permet de simplifier les données d'une attaque. En effet malgré leur différences elles reposent sur le même principe. De nombreux formalismes existent déjà pour regrouper les attaques en fautes ou les attaques en canaux auxiliaires. Notre formalisme réuni toutes les attaques physiques, et non une sous classe uniquement.

Par ailleurs dans ce formalisme nous cherchons à unifier également les attaques classiques de recherche de clé et les attaques en rétro-conception. Cela peut être par exemple des s-box d'un algorithme. Nous montrons que rechercher une clé ou une partie d'un algorithme ne change pas fondamentalement la construction d'une attaque. Seule la cible change.

Le but de ce formalisme est de se rapprocher au maximum de la cryptanalyse classique ; afin de comparer et combiner plus facilement les attaques, mieux choisir l'attaque en fonction du circuit et revoir la pertinence des contre-mesures existantes. Au final nous espérons que ce formalisme permettra de trouver de nouvelles attaques et de nouvelles contre-mesures.

Les attaques physiques fonctionnent toujours de la même manière.

Une attaque se réalise en trois phases : une phase de collecte de données observables, une phase de prédiction de données en fonction des hypothèses sur la cible et les modèles sélectionnés et une phase de comparaison des données observées avec les données prédites afin de retrouver le secret.

Il faut savoir ce que l'on attaque, quelle est la cible. La cible est le secret, l'information que l'on cherche à récupérer. Pour commencer, l'attaquant va collecter des mesures ou observables. Les observables sont reliées à la cible par une relation dite exploitable. Une relation exploitable dépend d'une fonction physique qui n'a pas forcément d'écriture mathématique.

La deuxième étape consiste alors à faire des hypothèses sur la cible. La fonction physique doit être expliquée par un modèle. Différents modèles peuvent être utilisés. Certains modèles sont plus probant que d'autre. A l'aide des hypothèses et du modèle, on veut construire des données approchant les mesures.

Pour finir, il faut mettre en évidence l'hypothèse correcte, en confrontant mesures et prédictions. Pour cela on utilise un outil statistique appelé distingueur.