Injection de fautes par impulsion électromagnétique sur microcontrôleur

Nicolas Moro, Amine Dehbaoui, Bruno Robisson, Emmanuelle Encrenaz, Karine Heydemann

Mars 2013

Résumé

Ce travail présente un ensemble de résultats expérimentaux visant à définir un modèle de fautes pour les attaques par injection électromagnétiques sur un microcontrôleur 32 bits. Notre approche vise à mieux comprendre les effets d'une injection électromagnétique à différents niveaux d'abstraction.

1 Introduction

Les circuits intégrés exécutant des fonctions cryptographiques peuvent faire l'objet d'attaques physiques, en visant ainsi non pas l'algorithme lui-même mais son implémentation. Parmi ces attaques physiques, les attaques par injection de faute peuvent permettre à un attaquant de retrouver des clés cryptographiques à l'aide d'un nombre très faible de couples composés d'un chiffré et d'un chiffré fauté. Les attaques par injection de faute se basent sur un modèle des fautes réalisables physiquement par l'attaquant. Notre travail vise à définir un tel modèle dans le cas d'une injection de fautes par impulsion électromagnétique sur un microcontrôleur.

2 Généralités sur l'injection électromagnétique

Nous utilisons une injection électromagnétique pulsée comme moyen d'injection de fautes. Celle-ci a d'abord été étudiée sur des architectures matérielles mais ses effets précis sur des circuits complexes sont mal maîtrisés. Sur microcontrôleur, ce procédé a pour l'instant été utilisé avec succès pour empêcher l'appel de sous-routine d'un programme. Nous présenterons donc les principes généraux de l'injection électromagnétique pulsée et introduirons notre montage expérimental.

3 Approche pour évaluer les effets obtenus

L'utilisation d'un microcontrôleur réel pose un certain nombre de problèmes pour pouvoir déterminer les effets obtenus sans avoir accès à l'ensemble des signaux internes de la puce. Nous proposons donc une approche qui permet d'évaluer au mieux les effets d'une injection de fautes sur l'exécution d'un programme embarqué. Une observation de l'état interne du microcontrôleur couplée à une simulation pour différents modèles de faute nous permettent d'observer plus finement les conséquences de .

4 Présentation des résultats expérimentaux

L'approche que nous proposons est ensuite appliquée au montage expérimental de façon à pouvoir mieux observer les effets obtenus et comprendre les fautes observées expérimentalement. Nous isolons les différents paramètres expérimentaux et étudions leur effet sur le type des fautes générées.

5 Vers la génération d'un modèle de fautes

Les différentes expérimentations menées nous permettent de construire un modèle de fautes au niveau transfert de registres (RTL) et de construire une abstraction simplifiée de ce modèle au niveau assembleur. La possibilité d'avoir une vue assembleur de ce modèle de fautes permet de faciliter la simulation d'une injection de fautes par un attaquant et ainsi de réfléchir à la conception d'éventuelles contre-mesures logicielles.