TP de sécurité des systèmes embarqués

Hugues de Valon
Paul Luperini
Lucas Mahieu

23 janvier 2017

Table des matières

1 Introduction

De nos jours, les réseaux de neurones artificiels reprennent de plus en plus d'importance car la puissance de calculs disponible permet d'obtenir des résultats satisfaisant en temps raisonnable. Le traitement d'images, la reconnaissance vocale ou le traitements lexicaux sont des applications qui pourraient être intégrées dans des systèmes embarqués. Pour ce type d'application, il est possible d'implémenter sur des CPU ou GPU des algorithmes neuronales, mais la consommation et la vitesse de traitement deviendraient vite limitant.

Créer un composant électronique (ASIC ou une IP FPGA dans un premier temps) implémentant un réseau de neurones réduirait drastiquement sa consommation et améliorerait la vitesse du réseau par rapport à un CPU. De plus, étant donnée que l'IP serait spécialisé à cette application permettrait de rendre paramétrable dynamiquement le composant lui permettrait de s'adapter à de multiples applications.

Le projet "Réseau de neurones sur FPGA" s'inscrit dans ce cadre. Sous le tutorat de Frédéric Pétrot et Adrien Prost-Boucle, nous devons créer un tel composant, et tester ses performances en vue de le comparer à des systèmes existants tels que la puce Spinnaker ou TrueNorth d'IBM ou encore de systèmes en développement tel que les réseaux de neurones ternaires du laboratoire TIMA. Une fois implémenté et validé, nous utiliserons une carte FPGA Zedboard pour tester notre composant sur une application classique de reconnaissance de chiffres manuscrits, en utilisant la base de données MNIST.

2 TP 1

2.1 Quelle protections sont mises en place contre les attaques par fautes ?

Bien que l'algorithme de l'AES est incassable aujourd'hui, son implementation peut permettre de récupérer des données sensibles par de nombreux moyens. Dans ce TP, on s'intéresse à une potentielle attaque par injection de fautes et a une contre-mesure de cette attaque. Pour mener un attaque par faute dans ce module AES, nous avons tout d'abord analysé le circuit et tenté de comprendre comment le système

2.2 Quelles sont les faiblesses de cette sécurité ?

2.3 Implémentation de l'attaque par faute

2.4 Embarcation du code

3 TP 2

3.1 Introduction

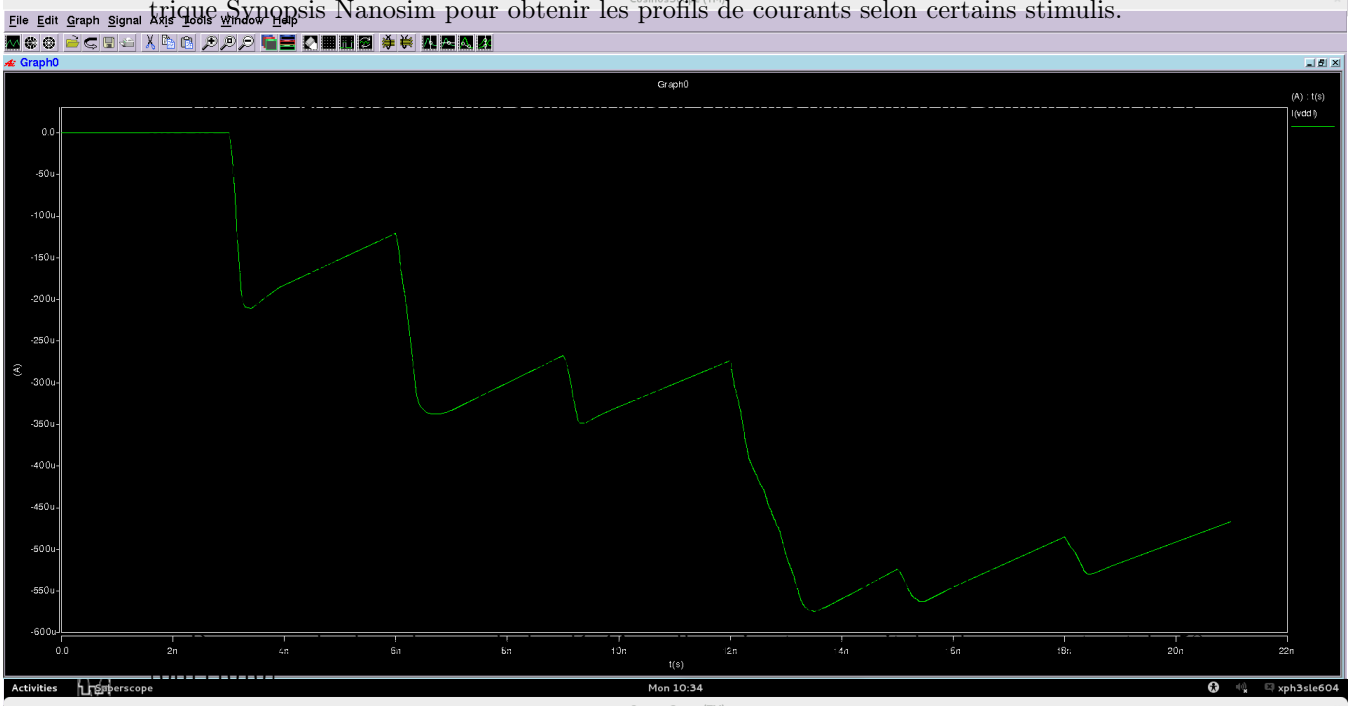
Dans cette partie nous allons effectuer une attaque par canaux auxiliaires sur un chiffrement AES. Cette attaque s'appelle Differential Power Analysis ou DPA, et consiste à étudier la consommation électrique du système visé sur de multiples exécutions et d'en déduire par des procédés statistiques l'information visée, ici la clé de chiffrement.

3.2 Théorie

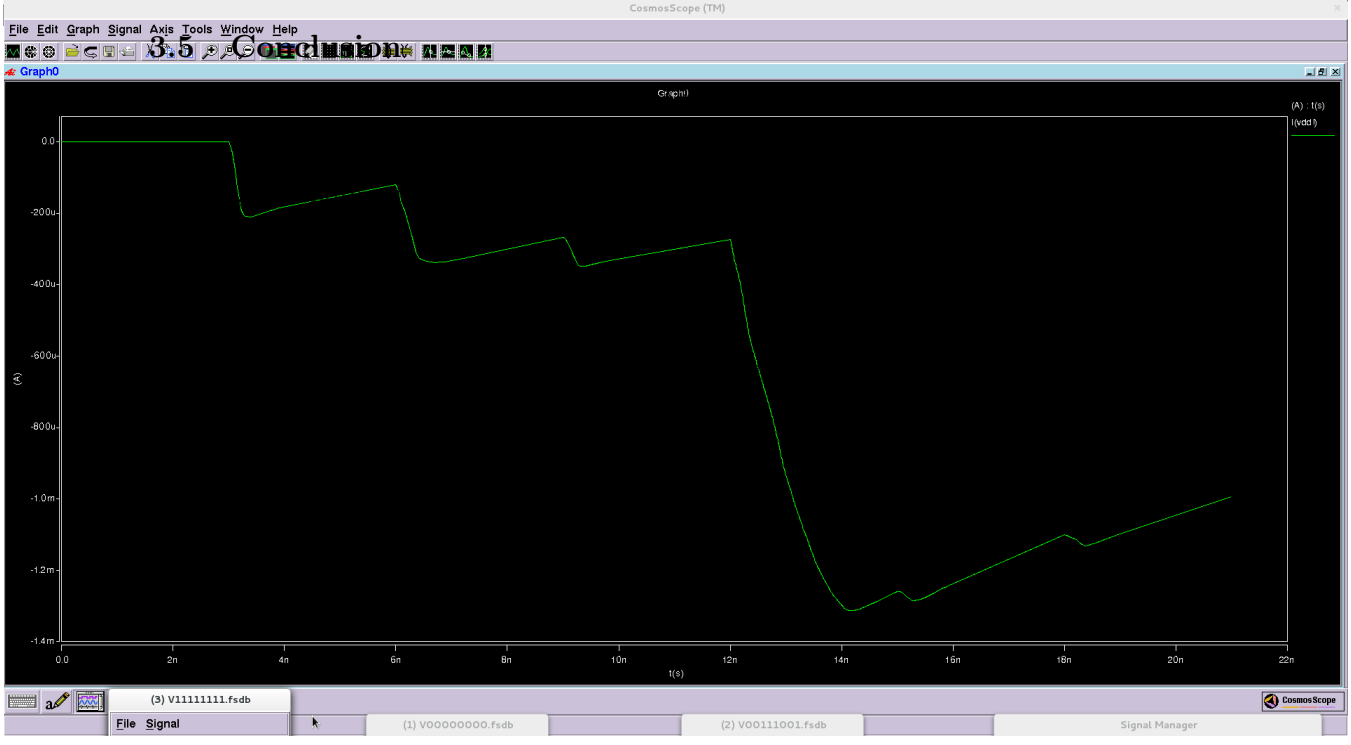
La sécurité d'un système de chiffrement dépend de l'algorithme employé et de son implémentation sur circuit électronique. Dans le cas de la DPA, nous allons utiliser des faiblesses d'implémentations pour en déduire la clé de chiffrement employée.

La SBox (Substitution Box) est le composant non linéaire principal de l'AES. Il s'agit d'une substitution d'octets, cette opération est effectuée juste après l'ajout de la clé à la

trique Synopsis Nanosim pour obtenir les profils de courants selon certains stimulis.



3.5 Conclusion



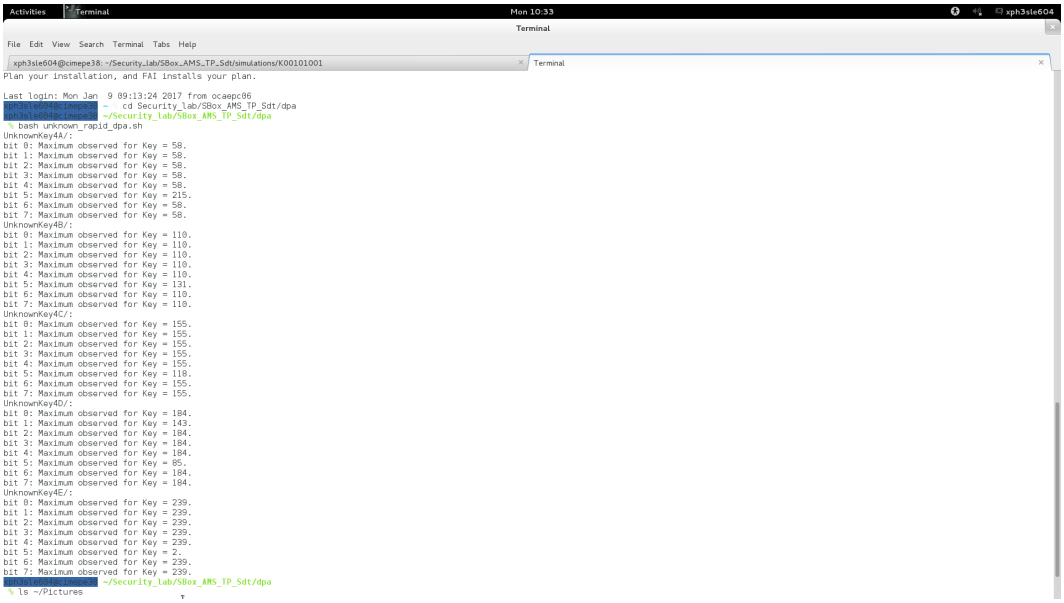


FIGURE 1 – Résultats de l'attaque DPA sur l'ensemble de données du groupe 4