SORBONNE UNIVERSITÉ

Proposition de stage M2

Sécurité des architectures FPGA : évaluation de l'implémentation d'oscillateurs en anneaux sur différentes architectures FPGA et impact sur une attaque par canal distant (remote side-chanel attack)

Contexte

Depuis leur introduction, il y a environ quarante ans, les FPGA (Field Programmable Gate Arrays) ont eu une évolution technologique rapide qui s'est accélérée ces dix dernières années [1]. Ils ont vu leurs capacités d'intégration multipliées par 10 000 et leurs performances par 100. La consommation énergétique et le coût de ces dispositifs ont diminués d'un facteur de plus de 1000. Ces progrès ont été rendus possibles par les avancées dans les technologies de fabrication et d'intégration, mais aussi par l'évolution de leur architecture.

Avec l'expansion des capacités des FPGA est apparue l'hétérogénéité du grain de reconfiguration au sein de ces circuits. Chaque fabricant a intégré de nouveaux nœuds de calcul et de mémorisation. Au sein des FPGA modernes, il n'y a plus seulement des LUTs (Look-Up-Table) configurés à grain fin, mais aussi des blocs de mémoires distribués, des opérateurs à grain moyen, appelés blocs DSPs (Digital Signal Processing), pour arriver aujourd'hui à du gros grain avec les SoC (System-on-Chip) où les architectures reconfigurables cohabitent, sur silicium, avec des processeurs en dur paramétrables (nombre de cœurs, fréquence d'horloge système, interfaces dédiées et bus système) i.e. le Zynq de chez Xilinx [2]. Récemment Xilinx a développé une nouvelle famille d'architecture reconfigurable, les ACAP (Adaptive Compute Acceleration Platform) qui intègrent en plus dans le SoC des accélérateurs dédiés à l'IA (Intelligence Artificielle) [3].

Cette hétérogénéité a permis la mise en œuvre de nouvelles applications en nous amenant dans l'âge de l'accélération où les FPGA sont au cœur de l'optimisation et de l'accélération matérielle des algorithmes, tant au niveau "edge" - systèmes embarqués (faible consommation énergétique, temps réel), que au niveau "cloud" pour des systèmes informatiques comme les serveurs de calcul hautes-performances.

Cette évolution architecturale et cette croissance en terme de ressources matérielles reconfigurables ont permis le développement de différentes méthodes d'utilisation du même circuit avec le paradigme de la reconfiguration partielle et dynamique. La définition des ZDR (Zones de Reconfiguration) permet le déploiement de différents IPs (Intellectual Property) au sein du même circuit mais à différents instants.

L'accès distant de ces ressources et leur utilisation partagée posent différents problèmes liées à leur sécurité. La principale étant l'impossibilité actuelle de partager par plusieurs utilisateurs le même FPGA (multitenant), car la structure qui permet la reconfiguration des ressources empêche une isolation logique complète. Un IP d'un utilisateur pourrait être perturbé ou espionné par la présence d'un IP d'un autre utilisateur. On parle dans ce cas d'un attaque par canal distant et qui exploite les caractéristiques intrinsèques architecturales des FPGAs. Ceci s'inscrit dans un contexte

qui demande la possibilité de reconfigurer partiellement une zone du FPGA (ZDR).

Mais pour que l'attaque puisse s'accomplir une mesure est nécessaire, les questions sont alors : que mesurer ? et comment ?
La mesure des fluctuations de la tension, liée au temps de propagation d'un signal, est un moyen utilisé à la fois pour perturber le bon fonctionnement d'une IP, que pour extraire la valeur d'un signal (clé d'un algorithme AES-Advanced Encryption Standard par exemple). Les oscillateurs en anneaux (Ring Oscillator (RO)) [4] sont la brique de base qui permet de faire cette mesure. Plusieurs architectures ont étés développées pour améliorer la sensibilité des RO.

Dans ce stage l'objectif est alors d'évaluer d'une part le risque d'implémenter des RO dans un FPGA, et de voir l'influence de l'architecture du FPGA sur ce risque (et donc sur l'efficacité du RO malveillant). Pour ce faire nous prendrons en considération comme architecture de départ les travaux de J. Gravellier et al. [5] et nous utiliseront un IP AES comme élément à attaquer par SPA (Simple Power Analysis [6]). Cet ensemble d'évaluation sera alors porté et implémenté sur différentes architectures de FPGA. Idéalement de premières expérimentations utilisant la reconfiguration dynamique seront alors menées pour voir l'impact de ce paradigme sur la sécurité du circuit.

Liste de publications en lien avec le stage

[1] Russell Tessier, Kenneth Pocek, and Andre DeHon. Reconfigurable computing architectures. Proceedings of the IEEE, 103(3):332–354, 2015.

[2] Zynq System-on-Chip architecture, Xilinx.

[3] Versal ACAP architecture, Xilinx.

[4] Kenneth M. Zick and John P. Hayes. Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems. ACM Transactions on Reconfigurable Technology and Systems, 5(1):1–26, 2012.

[5] J. Gravellier, J.-M. Dutertre, Y. Teglia, et P. Loubet-Moundi, High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs, in 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), Cancun, Mexico, déc. 2019, p. 1-8. doi: 10.1109/ReConFig48160.2019.8994789.

[6] Paul C Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In CRYPTO '96. 1996.

Objectif

A partir de l'implémentation d'une architecture de mesure du temps de propagation à base de RO (attaquant) et d'une IP de calcul (victime), i.e. AES, sur différentes ZDR, évaluer l'impact des différents architectures FPGA (virtuelle - OpenFPGA-VTR) ou physique (Ultrascale+ Virtrex-

Zynq) sur l'efficacité d'une attaque par canal distant.
Un objectif secondaire sera d'évaluer sur une architecture FPGA donnée l'impact des différents scénarios possibles pour la définition des ZDR (hétérogène versus homogène).

Environnement de travail
Les outils de conception seront à la fois des logiciels libres, comme VPR et OPENFPGA, qui permettent une libre exploration architecturale, et à la fois avec les outils de développement Xilinx - Vitis. Trois cartes seront utilisées, une Zedboard, une Xilinx Ultrascale+ Zynq et une Xilinx UltraScale+ Virtex.

Compétences requises
Connaissance des architectures FPGA, des architectures ARM, des langages VHDL, Verilog et C. Une connaissance des outils de conception Xilinx sera également apprécie.

Durée 6 mois

Laboratoire d'accueil
Ce stage sera effectué au laboratoire LIP6, à la Faculté de Sciences et il s'inscrit dans une collaboration scientifique entre le LIP6 (Andréa Pinna) et le laboratoire IETR (Sébastien Pillement).

Contact

Andrea Pinna
andrea.pinna@sorbonne-universite.fr
Sébastien Pillement
sebastien.pillement@univ-nantes.fr