N° d'ordre : D -

THESE

présentée

devant l'Institut National des Sciences Appliquées de Rennes

en vue de l'obtention du

DOCTORAT

spécialité : Electronique

par Mme May Myat Thu

Intitulé : Exploitation of EM Emanations of a SoC-FPGA Bus to Eavesdrop the Internally Processed Images of a Deep Learning Accelerator

Directeur de Thèse : Philippe Besnier / Maxime PELCAT

Date, heure et lieu de soutenance : 26/02/2025, 10h à Rennes, Amphi GC

Membres du jury

Cédric KILLIAN	Professeur des universités, Université Jean Monnet, St-Etienne
Alexandre BOYER	Maitre de conférences HDR, INSA Toulouse
Nele MENTENS	Full Professor, Universiteit Leiden, Pays-Bas
Christophe JEGO	Professeur, ENSEIRB-MATMECA, Bordeaux
Gabriel ZAID Dr.	Ingénieur de recherche, Thales ITSEF, Toulouse, France
Philippe BESNIER	Directeur de Recherche, CNRS, Rennes
Maxime PELCAT	Professeur des universités, INSA Rennes
Maria MÉNDEZ REAL	Chaire de Professeur Junior, Université de Bretagne Sud, Lorient

RESUME DE LA THESE

Cette thèse étudie l'exploitation des fuites EM des bus de données pour récupérer des images d'entrée secrètes traitées par des accélérateurs de réseaux neuronaux mis en oeuvre sur des SoC-FPGA. Pendant l'inférence par réseau neuronal, les pixels de l'image d'entrée transmis à travers les bus internes émettent des émanations EM qui sont ensuite analysées pour reconstruire les images d'entrée originales du réseau neuronal. En tirant parti d'un accès physique au système, un adversaire peut déployer une sonde en champ proche, telle qu'un cheval de Troie matériel pour capturer ces traces EM émises par le bus SoC pendant la classification des images. Deux nouvelles méthodologies sont proposées pour interpréter les émanations EM en pixels d'entrée, tout en exposant les vulnérabilités matérielles critiques, y compris l'acheminement et le positionnement des fils de bus internes dans la puce. Pour valider les approches proposées, un classificateur d'images tiers, HD level difference et PSNR sont utilisés. Cette recherche met en évidence les risques de sécurité posés par les fuites de EM dans SoC-FPGAs. Les résultats soulignent la nécessité de développer des contre-mesures solides pour atténuer les risques de attaque et protéger les informations sensibles contre les accès non autorisés.