COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

THÈSE DE DOCTORAT DE

NANTES UNIVERSITÉ

ÉCOLE DOCTORALE N° 641
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Électronique*

Par
Juliette Pottier

Protection microarchitecturale d'un cœur de processeur RISC-V

Thèse présentée et soutenue à Nantes Université, le 5 décembre 2025.
Unité de recherche : IETR UMR 6164

Rapporteurs avant soutenance :

M. BENOIT Pascal — Professeur des Universités, Université de Montpellier
Mme. HEYDEMANN Karine — Experte Sécurité/HDR, Thales DIS, Aix-en-Provence

Composition du Jury :

Examinateurs :	M. BENOIT Pascal	Professeur des Universités, Université de Montpellier
	M. BOSSUET Lilian	Professeur des Universités, Université Jean Monnet
	Mme. HEYDEMANN Karine	Experte Sécurité/HDR, Thales DIS, Aix-en-Provence
	M. MIGLIORE Vincent	Maître de Conférences, Université fédérale Toulouse Midi-Pyrénées
Dir. de thèse :	M. PILLEMENT Sébastien	Professeur des Universités, Nantes Université
Enc. de thèse :	Mme. MENDEZ REAL Maria	Maître de Conférences, Université Bretagne Sud

Invité(s) :

M. LE GAL Bertrand — Maître de Conférences, Université de Rennes

COLLEGE ED MATHEMATIQUES
DOCTORAL STIC
PAYS DE LA LOIRE

Nantes Université

Titre : Protection microarchitecturale d'un cœur de processeur RISC-V

Mot clés : Microarchitecture sécurisée, RISC-V, CSCA, attaques ROP, contre-mesures

Résumé : Ce manuscrit porte sur l'implémentation d'une microarchitecture sécurisée d'un cœur de processeur RISC-V contre les canaux auxiliaires sur les mémoires cache (CSCA). La solution proposée s'étend de la détection de contextes malveillants au déploiement dynamique de contre-mesures sur la mémoire cache. L'approche proposée repose sur l'intégration d'une unité de transformation du code dynamique matérielle basée sur une technique de micro-décodage afin de déployer les contre-mesures dynamiquement, tout en offrant une certaine flexibilité à l'échelle du matériel. En premier lieu, l'implémentation d'un système matériel d'observation de la microarchitecture, basé sur l'insertion dynamique d'instructions dans le flot d'exécution, est présenté. Une application de ce système à la détection d'attaques est également présentée ainsi que son évaluation. En outre, une stratégie de déploiement dynamique de contre-mesures sur la microarchitecture a été étudiée. Il s'agit de déployer au besoin, donc en cas de détection d'une menace, des contre-mesures. Deux solutions de sécurisation de la mémoire cache sont proposées : une technique basée sur l'ajout d'aléa sur l'adressage du cache et l'implémentation d'une hiérarchie mémoire hybride incluant une mémoire auxiliaire en parallèle du cache pour sécuriser l'accès aux données sensibles à l'exécution.

Title: Microarchitectural protection for a RISC-V processor core

Keywords: Secure microarchitecture, RISC-V, CSCA, ROP attacks, countermeasures

Abstract: This manuscript focuses on the implementation of a secure microarchitecture for a RISC-V processor core against side-channel attacks on cache memories (CSCA). The proposed solution ranges from the detection of malicious contexts to the dynamic deployment of countermeasures on the cache memory. The proposed approach is based on the integration of a hardware dynamic code transformation unit based on a micro-decoding technique in order to deploy countermeasures dynamically, while offering a certain degree of flexibility at the hardware level. First, the implementation of a hardware microarchitecture observation system, based on the dynamic insertion of instructions into the execution flow, is presented. An application of this system to attack detection is also presented, along with its evaluation. In addition, a strategy for the dynamic deployment of countermeasures on the microarchitecture has been studied. This involves deploying countermeasures as needed, i.e., when a threat is detected. Two solutions for securing the cache memory are proposed: a technique based on adding randomness to cache addressing and the implementation of a hybrid memory hierarchy including auxiliary memory in parallel with the cache to secure access to sensitive data during execution.