Université de Rennes

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2025

~~Contrats doctoraux «Ordinaires»~~ (ARED)

ECOLE DOCTORALE : SPIN **POLE DE RECHERCHE : Mathématiques-Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA

Equipe : OCIF

Encadrement

Directeur de thèse : Hélène Le Bouder **Unité de recherche** : IRISA

Employeur/Établissement d'origine : IMT Atlantique

HDR : • oui **Nb de thèses en cours** : 1

Mail : helene.le-bouder@imt-atlantique.fr **Tél**. : **02 99 12 24 04**

Co-directeur de thèse : Vianney Lapôtre **Unité de recherche** : Labsticc

Employeur/Établissement d'origine : Université Bretagne Sud

HDR : • oui **Nb de thèses en cours** : 4

Mail : vianney.lapotre@univ-ubs.fr **Tél.** : 02 97 87 45 68

Encadrant de thèse : Gaël Thomas **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Ministère des Armées - DGA-MI

HDR : • non **Nb de thèses en cours** : 0

Mail : gael.thomas@intradef.gouv.fr **Tél.** : 02 90 89 84 72

Sujet

Titre : **Cryptographie à faible latence pour garantir l'intégrité des instructions face aux attaques par injections de fautes — Hardware Integrity for Instructions (HIFI)**

Mots clés : **Intégrité, cryptographie à faible latence, cryptographie à bas coût, protection des instructions, composants électroniques, composant matériel, attaques physiques, injection de fautes.**

Cotutelle internationale : non **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Le nombre de circuits présents dans notre quotidien est en constante augmentation. Utilisés dans tous types de domaines, y compris critiques, garantir leur sécurité est devenue une nécessité. De nombreux systèmes embarquent des fonctions de sécurité tels une vérification de code PIN ou un algorithme cryptographique. Néanmoins, si ces fonctions sont conçues théoriquement sures, il est toujours possible d'attaquer leur implémentation matérielle. Les attaques par injection de fautes permettent de les outrepasser. Pour contrer ces attaques, de nombreuses contremesures existent, mais elles sont spécifiques à chaque algorithme.
Dans notre projet, nous portons l'idée d'une contremesure pour protéger l'intégrité des instructions d'un processeur avec un schéma de randomisation des instructions s'appuyant sur un MAC (Message Authentication Code). Dans la littérature, de premiers travaux ont montré l'intérêt de la randomisation des instructions, technique consistant à encoder les programmes à la compilation et à les décoder à la volée lors de l'exécution. Néanmoins, ces propositions sont inefficaces, car elles se basent sur des algorithmes non adaptés, notamment avec une latence trop élevée. Nous

souhaitons développer une solution pour protéger les instructions contre les attaques par injections de fautes avec un MAC à faible latence.
Un MAC est un outil cryptographique garantissant l'intégrité des données qui lui sont passées en entrée. Il se compose d'une primitive traitant des données de taille fixe et d'un mode permettant de gérer le cas des tailles arbitraires. Le mode bénéficie d'une réduction de sécurité vers la primitive, tandis que la sécurité de cette dernière ne repose en général que sur la cryptanalyse.
La·le doctorant·e devra proposer une ou plusieurs primitives de type chiffrement par bloc à paramètre (ou tweakable block cipher) avec une faible latence et sûr face à l'état de l'art de la cryptanalyse.

Dans le but de mener à bien ces travaux de thèses, les étapes suivantes ont été identifiées.
— Étudier l'état de l'art des primitives cryptographiques à faible latence.
— Proposer une solution originale permettant de répondre aux contraintes de latence et de coût considérées dans le projet. Ainsi le rôle d'encadrant de Gaël Thomas cryptologue à la DGA-MI est primordial.
— Proposer une implémentation matérielle sur cible FPGA de la solution proposée. La solution sera intégrée à un cœur RISC-V de la famille OpenHW Group 2 déjà mis en œuvre dans le cadre de projets de recherches menés au sein de l'équipe ARCAD du laboratoire Lab-STICC à Lorient dont Vianney Lapôtre, co-directeur de la thèse, est membre.
— Évaluer la solution proposée en termes de performance, de surface et de sécurité. Pour réaliser des évaluations de sécurité face à des attaques physiques par perturbation, le doctorant recruté aura accès au Laboratoire Haute Sécurité (LHS) de Rennes dont sa directrice de thèse Hélène Le Bouder est une membre active.