ECOLE DOCTORALE EEATS

Electronique, Electrotechnique, Automatique, Traitement du Signal

Proposition de sujet de thèse à pourvoir avec un contrat doctoral
Pour l'année 2025-2026

(information à renseigner obligatoirement)*

Titre de la thèse* : Méthodologie de conception optimisée pour systèmes intégrés numériques sûrs et sécurisés

Spécialité de la thèse* : Nano Electronique et Nano Technologies (NENT)

Laboratoire d'accueil* : TIMA

Date de début de la thèse* : 01/10/2025

Date limite de candidature* : 30/05/2025 à 23h59

****

Direction de thèse* : Régis LEVEUGLE, Regis.Leveugle@univ-grenoble-alpes.fr, encadrement 100%, Equipe AMfoRS

Co-encadrants éventuels* : ***Noms, Emails, Quotité d'encadrement envisagé, laboratoires et équipes de recherche***

****

Contexte et thématique de recherche :

Le domaine de la sûreté de fonctionnement en informatique et dans les systèmes numériques s'est développé historiquement pour pallier le très faible niveau de fiabilité des premiers composants, puis les perturbations induites par l'environnement, en commençant par le domaine spatial, puis avionique, nucléaire … et aujourd'hui jusqu'aux applications quotidiennes exploitées au niveau de la mer en atmosphère standard. Les objectifs visés sont essentiellement la fiabilité (service correct continu), l'innocuité (absence de conséquences catastrophiques en cas de défaillance) et dans certains cas la disponibilité (pourcentage de temps où le service attendu peut être obtenu).
Avec l'importance croissante de l'informatique dans de très nombreux domaines, la sécurité informatique ou cybersécurité s'est développée indépendamment, au sein de communautés différentes, et en considérant des menaces très différentes (intentionnelles et essentiellement liées à des programmes, au lieu de impromptues et dues à des perturbations essentiellement physiques).
Depuis le début du siècle, les deux domaines ont vu croître leur intersection pour deux raisons. Tout d'abord, le nombre de systèmes concernés à la fois par les menaces naturelles et les attaques malveillantes a considérablement augmenté. Ensuite, des attaques dites matérielles ont été développées, certaines exploitant des perturbations proches des perturbations naturelles ("attaques en fautes"). Malgré cette

intersection, les rapprochements entre les deux communautés restent limités et les équipes de chercheurs ou de développement industriel spécialistes des deux thématiques sont souvent séparées.
Pour se focaliser ici uniquement sur la problématique des attaques en fautes, l'essentiel de la littérature présuppose que les méthodes de protection (ou méthodes de "durcissement par conception") utilisées pour des objectifs de fiabilité ou d'innocuité répondent aussi directement aux besoins de protection contre les attaques en fautes et donc plus généralement à des exigences d'amélioration du niveau de sécurité. Toutefois, il a été montré que le problème est plus complexe car (1) une bonne protection contre les menaces naturelles n'est pas forcément suffisante pour s'opposer à un attaquant [1] et (2) une bonne protection contre les attaques en fautes peut dans certains cas augmenter la sensibilité à d'autres types d'attaques, facilitant la tâche de l'attaquant et réduisant de facto le niveau global de sécurité.
La possibilité d'un impact contre-productif au niveau sécurité d'une protection contre les fautes a été étudiée dans le cadre de la conception VLSI en analysant les effets de la redondance matérielle ou de la redondance d'information (codage des données) sur la consommation des circuits. Cette consommation, comme d'autres caractéristiques physiques, peut être exploitée par des attaques matérielles dites "par canaux auxiliaires" (SCA).
La première étude connue sur cette thématique au niveau international, ayant lancé la problématique sur ce sujet, a été réalisée dans notre équipe et publiée en 2006 [2]. Ces travaux ont été étendus [3-4], ce qui a notamment conduit à une partie de la thèse de Vincent Maingot, préparée sous ma direction et soutenue en 2009. Ils ont été repris et développés par un consortium international (Universités d'Amherst, USA, Lugano, Suisse, Milan, Italie, Ruhr à Bochum, Allemagne et EPFL à Lausanne, Suisse) dès 2007 [5]. D'autres équipes internationales ont depuis effectué quelques travaux sur cette thématique, à l'Université du Connecticut, à celle de Boston et à celle du New Hampshire aux USA [6-8], puis plus récemment, à Prague en République tchèque [9] et à Tallinn en Estonie [10]. En deux décennies, les travaux restent toutefois très peu nombreux, alors que la problématique devient de plus en plus critique pour de nombreuses applications quotidiennes, telles que l'automobile, le contrôle industriel et les nombreux dispositifs de l'Internet des objets, incluant ceux en lien avec la santé ou la défense.
Bien que des équipes renommées travaillent en France sur la sécurité matérielle et/ou la robustesse des systèmes intégrés (bien sûr à Grenoble, mais aussi, sans être exhaustif, Valence, Gardanne, Montpellier, St Etienne, Rennes, Lorient, Paris, …) le besoin de considérer globalement les contraintes de sécurité lors de la protection contre les fautes reste peu pris en compte malgré la demande croissante. Cet intérêt croissant est illustré par la présentation invitée qui m'a été demandée lors de la conférence BITFLIP by DGA en 2023 [11]. Depuis, j'ai été invité à présenter plusieurs tutoriaux sur cette thématique dans des conférences internationales (LATS25, NEWCAS25, SBCCI25). J'ai aussi été invité sur le même thème comme orateur pour le discours d'ouverture de la seconde édition de BITFLIP by DGA au sein de la European Cyber Week organisée en novembre 2025. Ces invitations, et différents contacts industriels ou institutionnels, montrent l'importance de développer aujourd'hui de nouveaux travaux sur ce sujet, en tenant compte des évolutions considérables du contexte au cours des vingt dernières années.

[1] N. Wiersma, R. Pareja, "Safety != Security: on the resilience of ASIL-D certified microcontrollers against fault injection attacks," IEEE FDTC, 2017
[2] R. Leveugle, V. Maingot, "On the use of information redundancy when designing secure chips," IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2006, pp. 141-142
[3] V. Maingot, R. Leveugle, "On the use of error correcting and detecting codes in secured circuits", IEEE Conf. on Ph.D. Research in Microelectronics and Electronics (PRIME), 2007, pp. 245-248
[4] V. Maingot, R. Leveugle, "Influence of error detecting or correcting codes on the sensitivity to DPA of an AES S-Box," Int. Conf. on Signals, Circuits & Systems (SCS), 2009
[5] L. Breveglieri, I. Koren, P. Maistri, "An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers," IEEE Trans. on Computers, vol. 56, no. 5, May 2007, pp. 635-649
[6] J. Dai, L. Wang, "A Study of Side-Channel Effects in Reliability-Enhancing Techniques," IEEE DFTS, 2009, pp. 236-244
[7] P. Luo et al., "Side-channel power analysis of different protection schemes against fault attacks on AES," IEEE ReConFig, 2014

[8] J. Dofe, H. Pahlevanzadeh, Q. Yu, "A comprehensive FPGA-based assessment on fault-resistant AES against correlation power analysis attack," Journal of Electronic Testing, 32, 611-624, 2016
[9] J. Ríha et al., "Influence of Fault-Tolerance Techniques on Power-Analysis Resistance of Cryptographic Design," Euromicro Conference on Digital System Design (DSD), 2017, pp. 260-267
[10] F. Almeida et al., "Side-Channel Attacks on Triple Modular Redun-dancy Schemes," IEEE Asian Test Symposium (ATS), 2021, pp. 79-84
[11] R. Leveugle, "Hardening by design: methods and perspectives", 8th European Cyber Week, Seminar BITFLIP by DGA, Rennes, France, November 22-23, 2023 (Invited presentation)

Description de la problématique de recherche :

Comme indiqué dans le résumé du contexte, sécuriser un système en ajoutant juste différents types de protections conçus indépendamment pour lutter contre chaque type d'attaque n'est pas efficace. Considérer qu'un système durci dans un but de fiabilité ou d'innocuité est aussi protégé contre les attaques en fautes n'est pas non plus réaliste. Et pourtant, cet axe de recherche reste encore aujourd'hui largement sous-exploré.

La problématique considérée ici est donc la nécessité de développer une approche plus holistique de la conception de systèmes numériques pour prendre en compte simultanément la dimension fiabilité/innocuité et l'ensemble de la dimension sécurité matérielle. Cette dernière recouvre de nombreux aspects en lien avec la conception de systèmes intégrés, incluant la robustesse face aux attaques en fautes et par canaux auxiliaires, mais aussi les attaques micro-architecturales, et d'autres composantes comme l'impact de la variabilité sur les fonctions de sécurité ou la prise en compte des contraintes sur le test, la lutte contre la contrefaçon, les chevaux de Troie … Dans le cadre de cette thèse, l'accent sera mis principalement sur le durcissement par conception en prenant en compte à la fois les protections nécessaires face aux fautes naturelles, dans un objectif de fiabilité et d'innocuité, et l'impact ou les limitations de ces protections du point de vue des contraintes de sécurité. L'objectif sera de proposer et valider des solutions efficaces maximisant la robustesse face aux fautes de toutes origines, tout en maximisant la résilience face aux autres types d'attaques matérielles et en minimisant les surcoûts. Les exigences à prendre en compte pour l'implantation de ces solutions seront identifiées précisément à chaque étape du flot de conception, depuis la spécification jusqu'au placement-routage final du système intégré sur FPGA ou sur ASIC.

Pour entrer davantage dans les détails, satisfaire des contraintes de sûreté (au sens innocuité et/ou fiabilité) s'appuie sur l'ajout de mécanismes permettant de détecter ou tolérer des disfonctionnements avant d'aboutir à des déviations inacceptables du service perceptible par l'utilisateur. De nombreuses méthodes existent, appliquées au niveau de la conception matérielle ou lors du développement du logiciel, y compris le logiciel directement embarqué dans des systèmes sur puce (SoC). Quelle que soit la méthode retenue, une protection induit des surcoûts et des modifications des caractéristiques du système intégré. Actuellement, le choix d'une méthode de protection contre les fautes reste guidé par les compromis en termes de ressources (ou surface), puissance de calcul (fréquence d'horloge, nombre de cycles), puissance ou énergie consommée et probabilité d'éviter des conséquences inacceptables suite à une liste prédéfinie d'évènements (typiquement, probabilité de détection ou de tolérance d'un ou plusieurs modèles de fautes représentatifs des évènements physiques redoutés). Lorsqu'un circuit doit satisfaire des contraintes de sécurité en plus des contraintes de sûreté, ce raisonnement n'est pas suffisant. D'une part, les modèles de fautes doivent être étendus pour tenir compte des capacités de nuisance réelles d'un attaquant. Ensuite, il est nécessaire d"ajouter dans les critères de sélection l'impact de la redondance sur les caractéristiques physiques du circuit comme la consommation électrique ou les émissions électromagnétiques. Comme indiqué précédemment, ces caractéristiques constituent ce qui est appelé en sécurité des canaux auxiliaires, porteurs d'informations sur les données manipulées par le circuit. Ces canaux peuvent être exploités par des attaquants pour extraire des informations secrètes comme par exemple des clés de chiffrement, donnant ensuite à l'attaquant un contrôle complet sur le système, ses actions et les informations qu'il contient. Sans détailler ici le fonctionnement exact de ces attaques, il suffit de

comprendre que l'insertion de protections contre les fautes peut fragiliser la sécurité du système en facilitant des attaques par canaux auxiliaires et/ou en rendant moins efficaces les protections dédiées à ces attaques, implantées par ailleurs dans le système intégré.
En conséquence, le besoin aujourd'hui est de proposer et valider une méthodologie de conception permettant de garantir que le choix des techniques de durcissement est réellement efficace contre les attaques en fautes, sans créer un maillon faible en nuisant à la lutte contre les autres types d'attaques. Cette méthodologie doit prendre en compte les évolutions significatives de ces dernières années en terme de capacité de nuisance des attaquants, qui mettent en œuvre des techniques de plus en plus sophistiquées, que ce soit au niveau de la finesse d'analyse ou du matériel employé. Il faut noter en particulier que les types de fautes pouvant être injectés par un attaquant sont aujourd'hui beaucoup plus menaçants et plus difficiles à contrer que les fautes naturelles prises en compte habituellement dans le domaine de la sûreté. Il s'agit donc d'apporter une réponse globale à la hauteur des risques actuels, ce qui a un impact sur toutes les étapes du flot de conception d'un système intégré, comme brièvement illustré dans [12].

[12] R. Leveugle, "Embedded tutorial: Integrated system hardening seen from a security point of view: dream or nightmare?," IEEE Latin American Test Symposium (LATS), San Andrés Island, Colombia, March 11-14, 2025

Objectifs de la thèse :

Au début de la thèse, il s'agira pour l'étudiant.e de se familiariser avec l'état de l'art aussi bien en termes d'attaques et de menaces que de méthodes de protection. En parallèle, un environnement à base de FPGA sera pris en main afin de pouvoir réaliser des attaques par analyse de consommation. Les premières expérimentations seront réalisées à partir de manipulations existantes ou à adapter. Elles permettront à la fois d'asseoir la compréhension de l'état de l'art et de revisiter certaines conclusions parfois contradictoires présentées dans la littérature. L'environnement sera ensuite exploité et amélioré au fur et à mesure de l'avancée et des besoins pendant la thèse.

Sur la base des premiers résultats obtenus, les antagonismes entre protection contre les fautes et augmentation de la sécurité seront précisés. Des réponses seront alors apportées en proposant de nouvelles structures et architectures combinant maximisation de la robustesse globale, donc maximisation de la confiance dans le système, et minimisation des surcoûts. Pour cela, il sera possible d'explorer différentes pistes. Celles liées à la conception du matériel seront privilégiées avec différents types de redondances (spatial, temporel, d'information) ou différentes techniques alternatives (CFC, assertions, auto-tests …) mais l'étude d'optimisations du logiciel embarqué est envisageable. L'utilisation d'approches émergentes comme le calcul approché est aussi une piste pour atteindre de meilleurs compromis entre le niveau de redondance fonctionnelle et le niveau de redondance en terme de ressources et de consommation.

En fonction des avancées, les approches explorées pourront être appliquées dans différents contextes, en lien avec d'autres études menées au sein de l'équipe et selon les partenariats qui seront mis en place. L'augmentation de la sûreté et de la sécurité des implantations de réseaux de neurones (CNN, DNN, …) implantés dans les systèmes embarqués ("Edge AI") sera l'un des cas d'étude, en complément de contextes classiques comme les systèmes exploitant des dispositifs de chiffrement ou d'autres domaines applicatifs motivés par les collaborations.

La valorisation des résultats se fera par le biais de publications régulières dans des conférences et revues internationales reconnues dans le domaine, par la participation à des évènements nationaux (colloque ou journée du GdR SoC2 notamment) et selon les opportunités des transferts au niveau industriel avec potentiellement dépôt de brevet sont envisageables.

Conditions scientifiques, matérielles et financières du projet de recherche :

L'étudiant.e travaillera dans l'équipe AMfoRS (Architectures and Methods for Resilient Systems) du laboratoire TIMA, qui a une grande expérience des problématiques de conception de systèmes intégrés pour la sûreté et la sécurité matérielle. Outre le directeur de thèse, l'étudiant.e sera en contact régulier avec des chercheurs seniors et aura de nombreuses interactions avec les autres doctorant.e.s de l'équipe, y compris dans le cadre d'activités spécifiques organisées avec l'ensemble des doctorant.e.s, permettant des échanges et partages entre les sujets scientifiques traités. L'étudiant.e pourra aussi être intégré.e, en fonction des intérêts communs et des opportunités, dans diverses collaborations (internes à l'équipe, inter-équipes dans le laboratoire ou plus largement avec des équipes extérieures au laboratoire).
L'étudiant.e bénéficiera de toute l'infrastructure de travail de TIMA : bureau, ordinateur, accès aux logiciels de CAO, services internet, etc. Une partie des budgets existants de l'équipe AMfoRS sera utilisée pour soutenir cette thèse, notamment pour financer l'accès aux services du CIME Nanotech (accès à des outils de CAO couramment utilisés dans l'industrie) et pour financer des missions.
La participation éventuelle à des activités d'enseignement pourra être discutée en fonction des motivations de l'étudiant.e et des opportunités.

Le montant brut des contrats doctoraux à compter du 1er janvier 2025 est de 2100€.
Un doctorant contractuel peut consacrer une partie de son temps de travail annuel à une autre activité rémunérée telle que l'enseignement ou l'expertise.
Remboursement partiel des titres de transport (domicile-travail) par l'employeur UGA.

Collaborations envisagées :

De nombreux contacts existent, que ce soit au niveau académique ou industriel, national ou international. Ces contacts pourront donner lieu à des collaborations ponctuelles en fonction des intérêts mutuels, voire à la définition de projets communs à moyen terme. Mais au moment où cette proposition de thèse est écrite, il n'y a pas de collaboration formelle engagée explicitement sur le sujet proposé pour la période correspondant à la thèse.

Compte tenu des contacts internationaux, il peut être envisagé une mobilité internationale pendant la préparation de la thèse, des aides pouvant être demandées auprès de l'UGA.

Profils et Compétences recherchés :

Les candidat.e.s doivent être titulaires d'un diplôme de niveau Master 2 dans une discipline comportant une composante marquée en conception de systèmes intégrés numériques (FPGA et/ou ASIC). Ils/elles devront pouvoir présenter des compétences et une expérience significatives acquises en projets et/ou stages sur ce type d'activité, incluant la mise en oeuvre des principales étapes et outils du flot de conception. Une bonne expérience en programmation (C, Python, …) et langages de script est fortement souhaitable. Des connaissances sur les aspects conception robuste ou sécurité matérielle seront appréciées mais ne sont pas exigées.

Les qualités relationnelles, la motivation, le dynamisme, la rigueur et la capacité à travailler en équipe seront appréciés.

Les candidat.e.s doivent avoir un bon niveau oral et écrit en anglais (B2 au moins fortement souhaité), avec de bonnes capacités rédactionnelles. Un niveau minimal en français est également souhaité, au moins dans le cadre des échanges techniques courants.

Notre équipe est très internationale et accueille des candidat.e.s avec des origines et des expériences variées. Notre laboratoire considère l'égalité des sexes et la diversité comme une force et un atout.

Pour plus amples informations sur le sujet :

Les références citées ci-dessus peuvent être consultées, notamment [12] qui peut être demandée à son auteur (e-mail ci-dessous).

Contact :

La candidature se fait en ligne via le lien suivant :
https://www.adum.fr/script/candidature/index.pl?site=edeeats

Un e-mail direct au contact ci-dessous est également souhaitable en cas de candidature.

Pour toute question supplémentaire concernant cette proposition :
Contact : **Régis LEVEUGLE, Regis.Leveugle@univ-grenoble-alpes.fr**, TIMA – 46 av. Felix Viallet – 38031 Grenoble Cedex