

Proposition de sujet de thèse à pourvoir

Année 2026-2027

Titre : Conception de circuits numériques pour la sûreté et la sécurité de systèmes 2.5D/3D basés sur des chiplets

Title: Design of digital circuits for reliability, safety and security of 2.5D/3D systems based on chiplets

Spécialité : Nano Electronique et Nano Technologies (NENT)

Laboratoire d'accueil : TIMA, Equipe AMfoRS

Direction de thèse (et contact) : Régis LEVEUGLE

Regis.Leveugle@univ-grenoble-alpes.fr

Résumé

Un nombre croissant d'applications, dans de nombreux domaines, demande aujourd'hui de satisfaire à la fois des exigences de fiabilité, sûreté/innocuité et sécurité. Pour être de confiance, ces applications doivent pouvoir compter sur des systèmes intégrés conçus pour satisfaire ces contraintes. Par ailleurs, les systèmes les plus complexes sont aujourd'hui basés sur des chiplets, interconnectés dans des structures à 2,5 voire 3 dimensions ce qui fait émerger de nouvelles problématiques. Le sujet de la thèse concerne la conception de systèmes intégrés numériques optimisés dans ce contexte et capables de résister aussi bien à des perturbations (naturelles ou intentionnelles) qu'à des attaques malveillantes par espionnage de canaux auxiliaires (consommation, émissions électromagnétiques directes, émissions électromagnétiques couplées ou conduites ...). Les mécanismes de protection contre les perturbations ne devront donc pas augmenter les risques d'observations malveillantes. De plus, il sera nécessaire de prendre en compte des problématiques de communication inappropriée (en émission ou en réception) entre chiplets, que ce soit avec un chiplet espion ou attaquant, ou simplement par des effets de couplage non maîtrisés pouvant créer des canaux cachés télécom (ou "screaming channels"). Les contraintes usuelles de compatibilité électromagnétique (émissivité, susceptibilité) seront donc aussi à reconsidérer dans la méthodologie proposée.

Abstract

A growing number of applications in many fields today require satisfying reliability, safety, and security requirements. To be trustworthy, these applications must rely on integrated systems designed to satisfy these constraints. Furthermore, the most complex systems today are based on chiplets, interconnected in 2.5- or even 3-dimensional structures, which gives rise to new challenges. This thesis focuses on the design of optimized digital integrated systems in this context, capable of withstanding both disturbances (natural or intentional) and malicious attacks through eavesdropping on side channels (power consumption, direct electromagnetic emissions, coupled or conducted electromagnetic emissions, etc.). The mechanisms for protection against disturbances must therefore not increase the risk of malicious observation. Furthermore, it will be necessary to consider issues of inappropriate communication (transmission or reception) between chiplets, whether with a spying or attacking chiplet, or simply due to uncontrolled coupling effects that can create hidden telecom channels (or "screaming channels"). The usual electromagnetic compatibility constraints (emissivity, susceptibility) will therefore also need to be reconsidered in the proposed methodology.



Laboratoire TIMA

46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE

Tél : 04 76 57 50 79

E-mail : tima-direction@univ-grenoble-alpes.fr

Web : <http://tima.univ-grenoble-alpes.fr>

TIMA Laboratory

46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE

Tel: (+33) (0) 476 57 50 79

E-mail: tima-direction@univ-grenoble-alpes.fr

Website: <http://tima.univ-grenoble-alpes.fr>

Profil et compétences recherchées

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. Des compétences en traitement du signal (analyse temps-fréquence, analyse de densité spectrale de puissance, ...) seraient également appréciées.

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.

Les candidatures doivent être compatibles avec les exigences d'une enquête FSD (travail en zone à accès restreint réglementé ZRR).

Profile and skills required

Candidates must hold a Master diploma in a discipline with a strong component related to the design of digital integrated systems (FPGA and/or ASIC). They must be able to demonstrate significant skills and experience acquired in projects and/or internships on this type of activity, including practice of the main description levels and tools of the design flow. Good experience in programming (C, Python, etc.) and scripting languages is highly desirable. Knowledge of robust design or hardware security aspects will be appreciated but is not required. Skills in signal processing (time-frequency analysis, power spectral density analysis, etc.) would also be appreciated.

Interpersonal skills, motivation, dynamism, rigor and the ability to work in a team will be appreciated.

Candidates must have a good level of oral and written English (at least B2 strongly desirable), with good writing skills. A minimum level in French is also desirable, at least for everyday technical communication.

Applications must be compatible with FSD requirements (work in restricted access area).

Description brève du contexte et des objectifs

Ce sujet concerne la conception de systèmes numériques intégrés pour des applications nécessitant de fortes exigences en terme de fiabilité, sûreté/innocuité et sécurité matérielle.

Le contexte principal est le besoin fortement croissant de satisfaire simultanément des exigences de robustesse face à des événements fortuits (problématique de fiabilité et innocuité des systèmes numériques) et des exigences de sécurité incluant la résilience face aux attaques dites matérielles (attaques en fautes et attaques par canaux auxiliaires SCA).

L'objectif principal est la proposition et la validation d'une méthodologie de conception permettant de répondre de manière holistique à l'ensemble des préoccupations en terme de fiabilité, innocuité et sécurité matérielle au lieu de juxtaposer des protections strictement focalisées chacune sur une partie de



Laboratoire TIMA

46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE

Tél : 04 76 57 50 79

E-mail : tima-direction@univ-grenoble-alpes.fr

Web : <http://tima.univ-grenoble-alpes.fr>



TIMA Laboratory

46 avenue Félix Viallet - 38031 GRENOBLE – FRANCE

Tel: (+33) (0) 476 57 50 79

E-mail: tima-direction@univ-grenoble-alpes.fr

Website: <http://tima.univ-grenoble-alpes.fr>



la problématique et ayant parfois des effets contre-productifs par rapport aux objectifs globaux. Les mécanismes de protection face aux différents types d'évènements pouvant créer des fautes dans le circuit devront être compatibles avec une bonne protection face aux attaques par canaux auxiliaires (SCA). Le niveau global de sécurité et de sûreté sera évalué en tenant compte des problématiques de compatibilité électromagnétique (CEM), notamment dans un contexte d'assemblage 3D.

Le travail visera à proposer des méthodes de conception et architectures innovantes pour protéger les principales fonctions élémentaires d'un système numérique, de façon à satisfaire simultanément les contraintes de sûreté et de sécurité matérielle malgré les antagonismes potentiels, tout en minimisant les surcoûts et en tenant compte des nouvelles problématiques liées aux assemblages de chiplets. Les propositions seront évaluées dans le cadre d'applications concrètes pouvant inclure des systèmes avec coprocesseurs de chiffrement, des implantations matérielles de réseaux de neurones ou d'accélérateurs pour l'IA ou encore des coeurs de processeurs open-source (typiquement RISC V). Les contraintes à prendre en compte sur les différentes étapes du flot de conception seront également identifiées précisément.

L'utilisation d'approches émergentes comme le calcul approché fait partie des pistes pour atteindre de meilleurs compromis entre le niveau de redondance fonctionnelle et le niveau de redondance en terme de ressources et de consommation.

Après validation fonctionnelle, l'évaluation de l'efficacité des approches proposées sera multi-critères, tenant compte notamment du nombre de ressources pour l'implantation, du surcoût en consommation, de la robustesse en présence de fautes, des caractéristiques en courant dans l'optique d'une potentielle attaque SCA par analyse de la consommation (du type DPA ou CPA) ou par analyse électromagnétique, et des niveaux de susceptibilité et d'émissivité dans un contexte CEM. Pour cela des prototypes de fonctions protégées seront implantés et ces démonstrateurs seront caractérisés en menant des campagnes d'attaques et de mesures.

Référence bibliographique sur le lien entre sûreté et sécurité

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

Plus de détails sur la thématique, le domaine, le contexte et les objectifs peuvent être obtenus en contactant l'auteur de la proposition.

Conditions scientifiques matérielles (conditions de sécurité spécifiques) et financières du projet de recherche

Pas de conditions de sécurité spécifiques concernant le travail à réaliser mais obligation de satisfaire à une enquête FSD (accès en zone à accès réglementé ZRR).

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 2026 est de 2300€ (source : site ministériel).

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

Plusieurs collaborations sont en cours sur la thématique de la thèse, que ce soit au niveau académique ou industriel. Selon le financement qui sera activé pour soutenir l'activité de la thèse, des échanges plus étroits auront lieu avec certains partenaires. Par ailleurs, les nombreux contacts existant entre l'équipe et des laboratoires ou industriels, au niveau national ou international, pourront donner lieu à des collaborations ponctuelles en fonction des intérêts mutuels, voire à la définition de nouvelles études communes à moyen terme.

Objectifs de valorisation des travaux de recherche du doctorant : diffusion, publication et confidentialité, droit à la propriété intellectuelle,...:

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

Candidature

Toute candidature doit être faite par courrier électronique à Regis.Leveugle@univ-grenoble-alpes.fr et être accompagnée d'un CV, d'une lettre de motivation, et des relevés de résultats académiques des dernières années. Des pièces complémentaires peuvent être indiquées comme disponibles si judicieuses par rapport au profil demandé (rapports de stage non confidentiels, rapports de projets, lettres de recommandation ...). Certaines peuvent aussi être jointes mais attention à la taille totale des messages envoyés ...

Application

Applications must be submitted by email to Regis.Leveugle@univ-grenoble-alpes.fr and include a CV, a cover letter, and academic transcripts from recent years. Additional documents may be indicated as available if relevant to the required profile (non-confidential internship reports, project reports, letters of recommendation, etc.). Some documents may also be attached, but please be mindful of the total email size.