Institut d'ingénierie et de management de l'Université Grenoble Alpes

HR EXCELLENCE IN RESEARCH

Grenoble INP - UGA est membre de **réseaux internationaux** de formation et recherche en ingénierie et management. Il est reconnu dans les classements nationaux et internationaux.

8 écoles + **39** laboratoires
8300 étudiantes et étudiants
1 300 personnels enseignants-chercheurs, administratifs et techniques

Grand établissement public d'enseignement supérieur, pôle de recherche reconnu, élément fondateur de l'écosystème grenoblois : Grenoble INP-UGA, institut d'ingénierie et de management de l'Université Grenoble Alpes, occupe une place de premier plan dans la communauté scientifique et industrielle.

Doctorat en conception numérique

Référence de l'offre	2024-PHDDIGITALENG-LCIS
Champ de recherche	Digital design engineering
Laboratoire	Laboratoire de conception et d'intégration des systèmes (Grenoble-INP, UGA) https://lcis.fr/
Profil	M.Sc./M.Eng. Degree in Telecommunication, digital design Engineering, or a closely related field in Electronic and Electrical
Localisation	Valence
Date de recrutement / durée du contrat	01/05/2024 (36 mois)
Contact métier	romain.siragusa@grenoble-inp.fr

Grenoble INP - UGA, grand établissement public, labellisé Initiative d'Excellence, propose des formations aux métiers d'ingénierie et de management avec un contenu scientifique solide et une haute spécialisation en lien avec les enjeux des transitions digitales, industrielles, organisationnelles, environnementales et énergétiques ainsi qu'une internationalisation importante de ses cursus. L'institut d'ingénierie et de management de l'Université Grenoble Alpes réunit ainsi plus de 1 300 personnels (enseignement, recherche, soutien administratif et technique) et 9 000 étudiantes et étudiants répartis entre ses 8 écoles (Grenoble INP - Ense3, Grenoble INP - Ensimag, Grenoble INP - Esisar, Grenoble INP - Génie industriel, Grenoble INP - Pagora, Grenoble INP - Phelma, Polytech Grenoble, Grenoble IAE) et La Prépa des INP. Grenoble INP est reconnu dans les classements nationaux comme un des leaders en ingénierie et en management avec une visibilité internationale certaine et est membre de différents réseaux internationaux académiques ainsi que de l'université européenne UNITE!
Au sein de l'Université Grenoble Alpes, Grenoble INP est tutelle associée de 40 laboratoires de recherche, dont certains internationaux, et de plateformes technologiques où sont menées des recherches de pointe valorisées auprès de ses partenaires socio-économiques et transférées à ses étudiantes et étudiants. Grenoble INP se positionne au cœur des axes scientifiques suivants : physique, énergie, mécanique et matériaux ; numérique ; micronano-électronique, systèmes embarqués ; industrie du futur, systèmes de production, environnement ; sciences de gestion et management.
Grenoble INP - UGA s'engage en matière de soutenabilité, promeut l'égalité des chances en matière d'emploi et affirme les valeurs d'équité, d'inclusion et de diversité. Toute candidature qualifiée pour un emploi sera considérée sans discrimination d'aucune sorte.

Recherche

***Laboratoire LCIS** :*

Le LCIS est un laboratoire de recherche public, équipe d'accueil de l'Université Grenoble Alpes associée à Grenoble-INP sur le campus UGA Valence.

Le LCIS rassemble plus de 60 chercheurs en informatique, électronique et automatique autour des systèmes embarqués et communicants.

Les thématiques abordées concernent la sûreté et la sécurité des systèmes embarqués et distribués, la modélisation, l'analyse et la supervision des systèmes complexes ouverts et les systèmes radiofréquences sans fil communicants.

Le laboratoire travaille sur des domaines d'application variés : internet des objets, systèmes cyber-physiques, environnements connectés naturels ou artificiels, RFID, etc.

Description de l'offre :

Les systèmes d'aujourd'hui sont de plus en plus interconnectés. Depuis l'avènement de l'internet des objets (IoT), tout capteur peut être interfacé avec un réseau local ou l'internet. Ce déploiement massif a engendré de nombreux problèmes de sécurité et des solutions associées. La sécurité de la communication peut être assurée grâce à la cryptographie. Cependant, la complexité de la solution ne la rend pas forcément compatible avec des systèmes à très faible coût comme on peut en trouver dans un réseau de capteurs. Une autre faille de sécurité étudiée concerne les attaques matérielles. En effet, l'analyse de canaux secrets, comme l'analyse de l'alimentation électrique, ou les attaques par injection de fautes, comme l'envoi d'impulsions électromagnétiques, peuvent copier le fonctionnement d'un appareil afin d'ajouter un objet tiers dans le réseau ou de le rendre inopérant. Ces attaques peuvent également perturber la génération des clés de chiffrement des données en s'attaquant au générateur de nombres aléatoires de la puce. Pour les éviter, il est possible de blinder les puces pour éviter tout rayonnement ou d'utiliser des codes correcteurs d'erreurs. Cependant, les solutions sont souvent lourdes à mettre en œuvre dans un appareil IoT.

La thèse fera partie d'un projet européen sur la création d'une puce sécurisée pour les systèmes IoT. L'objectif principal de la thèse est de concevoir un lien sans fil bas débit sans utiliser de composant analogique et d'associer des outils permettant d'identifier un module IoT et de détecter des attaques matérielles en temps réel pendant la communication. Au cours du projet, ces modules seront émulés par des cartes FPGA RF conçues au début du projet. Le premier objectif du projet sera donc de proposer une liaison sans fil à très bas coût sans composants analogiques utilisant une simple modulation numérique dans les bandes de fréquences ISM en ajoutant simplement une antenne au composant FPGA. Lors d'un précédent travail, notre équipe a montré qu'il était possible d'utiliser des composants FPGA à des fréquences RF (autour de 600 MHz) pour réaliser des liaisons sans fil OOK (On-Off Keying) sur plusieurs mètres à l'aide d'un amplificateur. L'innovation de ce premier objectif réside dans la possibilité d'opérer dans les bandes ISM sans aucun composant analogique (gain de place, de coût, de consommation). Un travail particulier sur le FPGA tel que l'étude des oscillateurs en anneau (RO) utilisés pour la porteuse sera réalisé afin de permettre une montée en fréquence. La liaison sera alors entièrement caractérisée en termes de débit, de portée et de taux d'erreur sur les bits. Le deuxième objectif est d'ajouter des fonctionnalités permettant d'identifier un module de réseau et de détecter des attaques matérielles sur celui-ci en utilisant la liaison sans fil développée. En effet, les signaux porteurs de communication sont générés par des RO.

Ce type de résonateur, utilisé notamment dans les générateurs de nombres aléatoires, a la particularité d'être très sensible aux caractéristiques de la puce : tension de seuil, tension d'alimentation, températures, etc. Deux résonateurs identiques implantés à deux endroits différents d'un FPGA auront donc une fréquence légèrement différente. Cette propriété a été utilisée pour authentifier les FPGA dans le cadre du projet Protect. En utilisant ces RO pour communiquer, dont la fréquence sera spécifique à l'appareil, il est possible de définir un identifiant associé à sa fréquence. Il sera également possible de détecter une attaque en surveillant les variations de fréquence des oscillateurs à la réception car ils sont très sensibles à toute variation de l'environnement. Le module de surveillance sera développé au niveau logique, le plus proche possible du matériel. Plus nous travaillerons à bas niveau, plus nous aurons un contrôle fin sur le système. Nous travaillerons sur le nombre de résonateurs par module pour rendre l'identification et la surveillance aussi fiables que possible.

Résumé du projet :

La thèse fait partie d'un projet européen KDT JU sur la création d'une puce sécurisée pour les systèmes IoT.

Objectifs principaux :

Les principaux objectifs sont de développer une communication sans fil à faible coût en utilisant un FPGA basse fréquence et de définir des outils de sécurité matérielle basés sur cette communication.

Mots-clés : FPGA, Internet des objets, communication sans fil, sécurité matérielle.

Logiciel : Programmation FPGA en VHLD ou Verilog.

Spécificités et contraintes particulières

Particularité du poste

Poste affecté dans une zone à régime restrictif : non

Processus de recrutement

Les candidatures (CV et lettre de motivation) doivent être transmises à : romain.siragusa@grenoble-inp.fr

Date de fin de candidature : 19/04/24