Implémentation d'algorithmes cryptographiques dans une mémoire intelligente et caractérisation contre les attaques par canaux auxiliaires sur la consommation

Référence	CYBERINSTITUTE-INT-20003
Description	Contexte : CEA Tech est le leader mondial de la recherche technologique. Les équipes d'ingénieurs chercheurs sont mobilisées pour bâtir et transférer à des partenaires industriels des portefeuilles de technologies répondant aux besoins des filières technologiques dans les domaines de l'information, de la communication, de l'énergie et de la santé. Le Leti, un des instituts de CEA Tech, concentre son activité sur les micro et nano technologies et leurs applications aux systèmes et composants de communication sans fil, à la biologie et la santé, à l'imagerie, et aux Micro-Nano Systèmes (MNS). Au sein du Département d'Architecture, Conception et Logiciel Embarqué (DACLE), le laboratoire LISAN (Laboratoire Intégration des Systèmes et Architecture Numériques) conçoit et réalise des circuits intégrés digitaux basés sur des architectures à haute efficacité énergétique, couvrant un large spectre applicatif depuis l'internet des objets jusqu'aux systèmes sur puce complexes pour calcul intensif. http://www.leti-cea.fr/cea-tech/leti Le Grenoble Alpes Cybersecurity Institute regroupe environ 150 chercheurs - experts en informatique, cryptographie, micro-électronique mais également en droit international, politique et économie - issus de 16 laboratoires de l'Univ. Grenoble Alpes et travaillant dans les domaines de la cybersécurité et de la protection de la vie privée. Ses principaux axes de recherche sont les éléments sécurisés à bas coût, les infrastructures critiques sécurisées et leur gestion en terme de cycle de vie, l'analyse de vulnérabilité et les défis globaux en termes d'analyse des risques et de validation des grands systèmes, incluant la résilience pratique dans l'industrie et la société. En prenant en compte l'impact sociétal de la cybersécurité, cette approche – dite holistique – permet d'intégrer la recherche fondamentale dans un contexte plus large, donc plus pertinent (https://cybersecurity.univ-grenoble-alpes.fr). Sujet : Le laboratoire LISAN (Laboratoire Intégration Silicium et Architecture Numérique) développe et conçoit des systèmes sur puces (SoC) innovants à base d'architectures multicœurs ainsi que des architectures basse consommation dédiées à l'Internet des Objets (Internet of Things - IoT). Le domaine de l'IoT remet à plat de nombreux prérequis, notamment au niveau de la sécurité des objets connectés autonomes en énergie. Les nouvelles architectures se veulent les plus économes en énergie possible. L'implémentation de la sécurité dans l'IoT doit donc elle aussi être guidée par l'énergie disponible, sans pour autant mener à des failles de sécurité. Une mémoire intelligente, appelée C-SRAM, permettant de faire des calculs en mémoire a été conçue au sein du laboratoire. L'objectif du stage est d'étudier l'implémentation d'un algorithme de chiffrement connu comme l'AES (Advanced Encryption Standard) au sein de cette mémoire et de caractériser sa robustesse par rapport aux attaques par canaux auxiliaires sur la consommation. De premières implémentations d'AES, sur un modèle précédent de la mémoire C-SRAM, ont déjà été réalisées au niveau RTL et au niveau C et pourront servir de base pour la nouvelle implémentation qui utilisera le dernier modèle de mémoire embarquant plus d'opérations logiques. Un environnement d'attaques, sous Python, est d'ores et déjà disponible au sein du laboratoire. Deux doctorants étudient actuellement à d'autres niveaux la C-SRAM et ce stage vient compléter leur étude sur l'aspect sécurité. Ce stage s'inscrit dans le cadre de travaux sur l'étude de techniques de sécurisation d'algorithmes de cryptographie implémentés en mémoire. Travail Demandé : Le travail se décomposera en plusieurs étapes : • Prise en main du flot de conception ASIC numérique du laboratoire (simulation sous Modelsim/Questasim, synthèse sous Design Compiler, implémentation physique sous Innovus et génération des traces de consommation sous PrimeTime power) • Prise en main de l'environnement d'attaques sous Python à partir de la mise en forme des traces de consommation (CPA et T-test) • Etude de l'implémentation d'un AES sur le nouveau modèle de C-SRAM ce qui implique un travail au niveau de l'algorithme pour tirer parti des nouvelles opérations disponibles et au niveau RTL (VHDL, Verilog ou System Verilog) • Caractérisation de l'implémentation par rapport aux attaques par canaux auxiliaires En fonction de l'avancement du stage, le/la stagiaire pourra également implémenter d'autres algorithmes et/ou d'autres attaques ou proposer des pistes d'optimisations.
Prérequis	Cette proposition est dédiée aux étudiants recherchant un stage au contenu technique ambitieux et désirant acquérir une expérience dans la recherche technologique.

GRENOBLE ALPES CYBERSECURITY INSTITUTE. **Office/Bureau** : Institut Fourier – Bureau 031C, 100 rue des Maths, 38610 Gières
Postal address/Adresse postale : Institut Fourier – Cybersecurity Institute, CS40700 38058 Grenoble CEDEX 09 – FRANCE
Contact : +33 6 37 81 22 94 / cyberalps-contact@univ-grenoble-alpes.fr / https://cybersecurity.univ-grenoble-alpes.fr
Twitter : @CyberAlps / **LinkedIn** : https://www.linkedin.com/company/grenoble-alpes-cybersecurity-institute

financed by
IDEX Université Grenoble Alpes

	L'étudiant devra présenter un niveau équivalent de dernière année d'école d'ingénieur (ou master 2) avec de préférence une spécialité en conception de circuits numériques. Des notions sur la sécurité des systèmes matériels, de la cryptographie en général serait un plus. La connaissance de la microélectronique et du flot de conception aidera le stagiaire à la réussite des objectifs. Enfin, l'étudiant devra présenter une bonne curiosité dans le domaine de la sécurité matérielle. Le sujet de stage offre la possibilité de continuer en thèse sur le sujet « Techniques de sécurisation matérielle d'algorithmes de cryptographie tirant partie du calcul en mémoire ». Les compétences suivantes sont recherchées : • VHDL ou Verilog ou System Verilog, • C • Scripting (Python, Perl, …) • Outils de simulation numériques (Modelsim/Questasim, ...), • Contrôle de révision (SVN, git, ...)

Encadrant(s)	Simone Bacles-Min
Candidature	Envoyer CV, lettre de motivation avec recommandation(s) de 1 ou 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) à cyberalps-contact@univ-grenoble-alpes.fr Pour plus d'information sur le stage, contacter [simone.bacles-min@cea.fr]
Localisation	CEA GRENOBLE 17 avenue des Martyrs 38054 Grenoble CEDEX 9
Date de début	A partir de février 2020
Durée	5 à 6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.