Titre	Protection d'un processeur avec DIFT contre des attaques physiques
Contexte	À l'heure de l'Internet des objets (IoT), les systèmes embarqués se répandent massivement dans des infrastructures critiques comme l'industrie, les villes intelligentes, les dispositifs bio-médicaux, etc. Ils contribuent à un meilleur contrôle et une plus grande optimisation des infrastructures pour à la fois augmenter leur efficacité et leur usage mais aussi répondre à des défis sociétaux tels que le changement climatique ou la santé. Malheureusement, ils participent malgré eux à l'augmentation de la surface d'attaque globale des systèmes d'information ce qui représente une menace sans précédent. Il est donc essentiel de garantir le meilleur niveau de protection pour de tels systèmes ayant généralement un processeur à basse consommation d'énergie comme principal composant. Ce dernier manipule des données sensibles lors de tâches de sécurité. Du fait de la connectivité réseau et de la proximité physique avec l'attaquant, il fait face à la fois à des attaques logicielles et à des attaques physiques. Prendre en compte simultanément ces deux types d'attaques lors de la conception du processeur est donc essentiel bien que cette problématique soit encore insuffisamment appréhendée par la communauté scientifique. En effet, les travaux publiés dans la littérature se concentrent essentiellement sur un seul de ces types de menace. De plus l'intégration de protections développées pour contrer des attaques logicielles peut favoriser certaines attaques physiques (par exemple en augmentant l'activité électrique liée à certaines instructions sensibles). Les techniques de DIFT (Dynamic Information Flow Tracking) permettent de détecter diverses attaques logicielles en attachant et en propageant, à l'exécution, des étiquettes à des conteneurs d'information (registres, zones mémoire, etc.). Associées à une politique de gestion de flux d'information, elles permettent de détecter des violations de la politique de sécurité instanciée par le programmeur (p. ex. accès à une zone mémoire non autorisée, transmission de données non autorisées). Le sujet proposé vise à concevoir et à évaluer un mécanisme de protection de type DIFT qui soit robuste à des attaques physiques exploitant des canaux auxiliaires et des injections de fautes. Ce dispositif sera développé et intégré dans un processeur embarqué en tenant compte de contraintes de surface de circuit, de performance et d'énergie consommée. Ce sujet de thèse s'inscrit dans une ambition plus large visant à développer un processeur faible consommation résistant à une large gamme d'attaques logicielles et matérielles. Ainsi, les travaux en cours de Noura Ait Manssour (2019-2022) participent à cette ambition et porte sur la protection contre certaines attaques physiques de mécanismes simples d'intégrité du flot d'instructions via des techniques du type rejeu d'instructions. Le sujet proposé couvre une autre dimension du problème afin d'aboutir à une solution plus globale. Les travaux de thèse seront encadrés par Vianney LAPOTRE, Maître de Conférences, qui travaille dans la sécurité matérielle, et dirigés par Guy GOGNIAT, Professeur des Universités, apportant une expérience de près de vingt ans dans le domaine de la sécurité des systèmes embarqués. Vianney LAPOTRE co-encadre actuellement la thèse de Noura Ait Manssour (2019-2022) et la thèse de Ghita Harcha qui sera soutenue début 2021 sur la protection d'une architecture matérielle de chiffrement AES pour IIoT contre des attaques par canaux auxiliaires. Vianney LAPOTRE souhaite soutenir sont Habilitation à Diriger des Recherches vers la fin de cette thèse. Cela permettra de renforcer l'activité de recherche au sein de l'équipe ARCAD avec une plus grande capacité à encadrer des travaux.
Objectifs identifiés	Au regard de la croissance importante du nombre de systèmes embarqués dans notre vie quotidienne, le développement de processeurs sécurisés est un enjeu de souveraineté nationale et européenne. L'architecture de processeur libre RISC-V offre l'opportunité de développer et de partager des travaux de recherche originaux en s'appuyant sur une base commune. C'est dans cet esprit que s'inscrivent nos travaux qui s'appuieront sur le RISC-V. Dans cette thèse, nous nous focaliserons sur la protection du flux d'information au sein du cœur du processeur. Nous nous intéresserons particulièrement aux mécanismes DIFT à grain fin travaillant sur des conteneurs d'information physiques : registres, zones mémoire, interfaces d'entrées/sorties. Dans le but d'intégrer des protections développées durant ces travaux, la micro-architecture du processeur cible sera modifiée et étendue dans une approche « secure by design ». Les protections proposées seront évaluées en terme de performance, de surface de circuit, de consommation d'énergie et de sécurité sur cible FPGA. Pour cela, nous utiliserons la plateforme dévaluation de sécurité A2C2P2 de composants électroniques contre des attaques physiques (développée au Lab-STICC à Lorient dans le cadre du CPER CyberSSI 2015-2020). Pour l'évaluation des protections contre des attaques logicielles, nous nous appuierons principalement sur des benchmarks existants (p. ex. RIPE) et des codes sources développés lors de précédents projets (Labex HardBlare 2015-2019). Ces travaux se dérouleront au sein de l'équipe ARCAD du Lab-STICC à Lorient qui possède une forte expertise dans le domaine de la sécurité matérielle, ce qui favorisera les interactions avec les autres doctorants et chercheurs du laboratoire. La première étape du travail consistera à évaluer la sensibilité aux attaques physiques d'un ensemble de travaux proposés pour le DIFT dans l'état de l'art. Pour cela, nous intégrerons certaines de ces techniques comme par exemple [1] ou [2] à un processeur RISC-V disponible en libre accès (p. ex. le

	cœur libre CV32E40P mis à disposition par l'OpenHW Group) et nous procéderons à des évaluations via des outils de simulation bit-près cycle-près et/ou via la plateforme A2C2P2. La seconde étape consistera à concevoir un nouveau mécanisme de DIFT offrant en plus d'une protection à des attaques logicielles de la robustesse contre certaines attaques physiques (p. ex. analyse de la consommation de puissance et perturbation électromagnétique). Pour cela, nous combinerons et intégrerons à la microarchitecture du processeur une large gamme de méthodes de protection afin de les évaluer de façon systématique : masquage, obscurcissement, ajout d'aléa pour augmenter la robustesse à des attaques par observation et redondance spatiale/temporelle, détection et correction d'erreurs pour augmenter la robustesse à des attaques par perturbation. Nous analyserons les meilleures combinaisons et configurations des protections existantes et proposerons de nouvelles protections.
Caractère novateur	Parmi les nouvelles contremesures que nous souhaitons étudier, la question de la propagation des tags de façon sécurisée nous paraît centrale, aussi nous explorerons la mise en œuvre d'étiquettes encodées (pour la détection d'erreurs) et masquées (pour la réduction des fuites par canaux auxiliaires). Une telle approche nécessite une arithmétique dédiée que nous étudierons également. Il est important de noter que les techniques d'attaques considérées dans ce projet sont bien maitrisées au sein de l'équipe et que nous avons également une expérience des techniques DIFT. Dans le cadre de ces travaux, les solutions proposées seront purement matérielles. Par conséquent, aucune modification de la chaîne de compilation n'est envisagée (sauf potentiellement l'ajout d'instructions de configuration). Les mécanismes de protections proposés seront intégrés à un processeur RISC-V, implémenté sur circuit FPGA afin de pouvoir prototyper et évaluer en terme de performance, de consommation d'énergie, de surface de circuit et de sécurité sur la plateforme A2C2P2 les solutions proposées.
Collaborations nationales et internationales	Dans le cadre de la thèse nous encouragerons la mobilité internationale. Nous pensons par exemple à l'équipe du Professeur Russell Tessier, College of Engineering, University of Massachusetts, Amherst, USA avec qui nous travaillons régulièrement. Nous avons d'autres partenaires potentiels, nous verrons l'équipe la plus pertinente en fonction des contributions que nous obtiendrons.
Retombées	Le sujet proposé s'inscrit pleinement dans la dynamique française et européenne autour du processeur RISC-V. En effet, la maitrise des architectures de processeur est un enjeu de souveraineté. C'est pourquoi, des communautés de chercheurs et d'industriels se sont organisées dans le but d'adresser les multiples challenges liés au RISC-V (IoT, calcul haute performance, télécommunication, sécurité, etc.). Les travaux proposés se positionnent sur la thématique de la sécurité des processeurs RISC-V. Au sein de la de la sécurité des processeurs RISC-V. Au sein de la communauté française, différents efforts sont actuellement menés. Par exemple, le projet ANR COFFI (https://anr.fr/Projet-ANR-18-CE39-0003) se concentre sur la résistance à des attaques physiques en injection de fautes et rassemble des partenaires du CEA, des laboratoires LIP6, LabHC et l'entreprise Invia ISSM. Un autre effort remarquable de la communauté académique est le projet ANR ARCHI-SEC sur la résistance de processeurs à des attaques sur la micro-architecture (p. ex. Spectre/Meltdown) et rassemble des partenaires des laboratoires LTCI, LIRMM, LabHC, IRISA et l'entreprise Secure-IC. L'originalité de notre sujet réside principalement dans la conception de mécanismes de protection contre des attaques logicielles et contre des attaques physiques. Il est donc complémentaire avec les efforts menés sur le territoire national et breton et vise à adresser la question fondamentale de la sécurité en profondeur. En effet, l'ajout de mécanismes de protection peut introduire des vulnérabilités croisées, aussi il est essentiel d'évaluer de façon systématique si une contremesure pour des attaques logicielles n'introduit pas de vulnérabilités pour des attaques physiques et inversement. Les travaux que nous menons depuis plusieurs années sur la protection des systèmes embarqués contre des attaques logicielles et physiques nous permettent de rassembler les compétences nécessaires pour mener à bien ce projet.

References

[1] M. Dalton, H. Kannan, and C. Kozyrakis. Raksha: A Flexible Information Flow Architecture for Software Security, in proc. of International Symposium on Computer Architecture (ISCA). 2007.

[2] C. Palmiero, G. Di Guglielmo, L. Lavagno and L. P. Carloni, Design and Implementation of a Dynamic Information Flow Tracking Architecture to Secure a RISCV Core for IoT Applications, in proc. of IEEE High Performance extreme Computing Conference (HPEC), 2018.