Demande n°3860 - ARED

Acronyme :HIFI

Identification

Identification

N°	3860
Année	2025
Statut	Brouillon
Date de création	28/01/2025
Date de modification	28/01/2025
Date de soumission	28/01/2025
Acronyme	HIFI
Intitulé du projet	Hardware Integrity for Instructions
Dispositif	ARED
Civilité du porteur	Madame
Nom du porteur	Le Bouder
Prénom du porteur	Hélène
Courriel	helene.le-bouder@imt-atlantique.fr

Priorité régionale

Priorité régionale

Priorité régionale	Lien avec une politique publique de la Région (Cybersécurité, Agroécologie, Mer, Mobilités, Ports, Langues de Bretagne)
Regional priority	Lien avec une politique publique de la Région (Cybersécurité, Agroécologie, Mer, Mobilités, Ports, Langues de Bretagne...)

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Domaine d'innovation stratégique principal	Économie numérique sécurisée et responsable
Domaine d'innovation stratégique	.
Levier thématique associé au DIS principal	Cybersécurité

Organisme de tutelle

Organisme de tutelle

Etablissement	IMT Atlantique
Commune	BREST
Civilité	Madame
Nom	DUMUR
Prénom	Bétrice

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA)	
Le cas échéant, nom de l'équipe de recherche	OCIF
Le cas échéant, nom du responsable de l'équipe de recherche	Georgios Papadopoulos
Activités de recherche et points forts de l'équipe	sécurité IoT et système embarqué
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Co-directeur de thèse

Civilité	Monsieur
Nom	Lapôtre
Prénom	Vianney
Unité de recherche	LAbsticc

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	Le nombre de circuits présents dans notre quotidien est en constante augmentation. Utilisés dans tous types de domaines, y compris critiques, garantir leur sécurité est devenue une nécessité. De nombreux systèmes embarquent des fonctions de sécurité tels une vérification de code PIN ou un algorithme cryptographique. Néanmoins, si ces fonctions sont conçues théoriquement sures, il est toujours possible d’attaquer leur

Libellé	Valeur
	théoriquement sures, il est toujours possible d'attaquer leur implémentation matérielle. Les attaques par injection de fautes permettent de les outrepasser. Pour contrer ces attaques, de nombreuses contremesures existent, mais elles sont spécifiques à chaque algorithme. Dans notre projet, nous portons l'idée d'une contremesure pour protéger l'intégrité des instructions d'un processeur avec un schéma de randomisation des instructions s'appuyant sur un MAC (Message Authentication Code). Dans la littérature, de premiers travaux ont montré l'intérêt de la randomisation des instructions, technique consistant à encoder les programmes à la compilation et à les décoder à la volée lors de l'exécution. Néanmoins, ces propositions sont inefficaces, car elles se basent sur des algorithmes non adaptés, notamment avec une latence trop élevée. Nous souhaitons développer une solution pour protéger les instructions contre les attaques par injections de fautes avec un MAC à faible latence. Un MAC est un outil cryptographique garantissant l'intégrité des données qui lui sont passées en entrée. Il se compose d'une primitive traitant des données de taille fixe et d'un mode permettant de gérer le cas des tailles arbitraires. Le mode bénéficie d'une réduction de sécurité vers la primitive, tandis que la sécurité de cette dernière ne repose en général que sur la cryptanalyse. La·le doctorant·e devra proposer une ou plusieurs primitives de type chiffrement par bloc à paramètre (ou tweakable block cipher) avec une faible latence et sûr face à l'état de l'art de la cryptanalyse.
Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2025 -2000 car. max)	Dans le but de mener à bien ces travaux de thèses, les étapes suivantes ont été identifiées. — Étudier l'état de l'art des primitives cryptographiques à faible latence. — Proposer une solution originale permettant de répondre aux contraintes de latence et de coût considérées dans le projet. — Proposer une implémentation matérielle sur cible FPGA de la solution proposée. La solution sera intégrée à un cœur RISC-V. — Évaluer la solution proposée en termes de performance, de surface et de sécurité. Pour réaliser des évaluations de sécurité face à des attaques physiques par perturbation, le doctorant recruté aura accès au Laboratoire Haute Sécurité (LHS) de Rennes.
Porteur du projet : date d'obtention de l'HDR ou dérogation	octobre 2023
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	encadrement : IMT Atlantique, Université de Bretagne sud et DGA MI
Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	
Si priorité régionale cochée, préciser en quoi le projet s'y rattache effectivement (2000 car.max.)	
Si priorité régionale "Politique publique Région", préciser (voir liste au point 4, Règlement 2025)	Cybersécurité
Cotutelle financière internationale (oui/non)	non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	
État du cofinancement (indiquer "acquis" ou "demandé")	demandé Creach Labs
Si demandé, date prévisionnelle de réponse du cofinanceur	
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	
Si reversement prévu, préciser (partenaire, montant)	

Candidat

Candidat

Genre	Féminin
Nationalité	marocaine

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
	ARED - Dépôt - CV du porteur	Obligatoire - Le CV doit préciser si le porteur est titulaire de l'HDR et, le cas échéant, depuis quand, et mentionner la liste des doctorant·e·s déjà encadré·e·s et des publications associées.		Non traité	
	ARED - Dépôt - Avis directeur·rice d'unité	Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger"		Non traité	
	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
	ARED - Instruction - Lettre de saisine	Lettre de l'établissement à transmettre à la Région (utiliser le modèle disponible dans la rubrique "Documents à télécharger")		Non traité	
	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
	ARED - Versement 2 - CV doctorant.e	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	

	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3		Non traité	