Demande n°3870 - ARED

Acronyme :MPCLat

Identification

Identification

N°	3870
Année	2025
Statut	Soumis à l'établissement
Date de création	29/01/2025
Date de modification	29/01/2025
Date de soumission	29/01/2025
Acronyme	MPCLat
Intitulé du projet	MPC in the Head signature
Dispositif	ARED
Civilité du porteur	Monsieur
Nom du porteur	FOUQUE
Prénom du porteur	Pierre-Alain
Courriel	pierre-alain.fouque@irisa.fr

Priorité régionale

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
Axe transversal : transitions climatique et écologique	Adaptation au changement climatique
Axe transversal : cohésion et inclusion sociale	Dialogue science / société

Organisme de tutelle

Organisme de tutelle

Etablissement	UNIVERSITE RENNES 1
Commune	RENNES
Civilité	Monsieur
Nom	LE GOUGUEC
Prénom	Fabrice

Unité de recherche

Unité de recherche

Nom de l'unité	IRISA (UMR 6074)
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume
Tél.	0299847402
Courriel	guig@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA)	UMR 6074
Le cas échéant, nom de l'équipe de recherche	Capsule (equipe IRISA / Centre Inria de l'Université de Rennes)
Le cas échéant, nom du responsable de l'équipe de recherche	Pierre-Alain Fouque
Activités de recherche et points forts de l'équipe	- cryptographie symétrique - cryptographie post-quantique - sécurité des implémentations contre les attaques matérielles et logicielles
Si implication dans un/plusieurs programmes européens ou internationaux, préciser	

Co-directeur de thèse

Description

Description du projet

Libellé	Valeur
Résumé synthétique du projet (2000 caractères max)	Le but de cette thèse est d'étudier une nouvelle construction de schéma de signature post-quantique qui repose sur du calcul distribué sécurisé. Au dernier appel à contribution, un tiers des soumissions utilisait ce type de signature. Il reste des problèmes à résoudre comme comprendre pourquoi les signatures reposant sur les réseaux ne sont pas assez efficace actuellement, construire des signatures avancées notamment pour l'identité numérique et enfin, comprendre la sécurité de ce type de signature contre les attaques par canaux auxiliaires.
Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2025 -2000 car. max)	Ce projet est intéressant car il permettrait d'étudier les protocoles de calcul multi-party et les signatures. Les protocoles multi-parties sont actuellement important car le NIST va ouvrir un nouvel appel sur les signatures à seuil qui

	ont des applications dans les blockchains. Plusieurs personnes de l'équipe sont intéressées par travailler sur ce sujet qui couvre à la fois les aspects théoriques et les aspects implémentations.
Porteur du projet : date d'obtention de l'HDR ou dérogation	Pierre-Alain Fouque (HDR: ENS en Décembre 2010)
Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.)	Dans le cadre de ce projet, j'aimerai travailler avec l'entreprise PQShield, qui se trouve à la fois en France et en Angleterre. PQShiield est une entreprise qui s'intéresse aux algorithmes post-quantiques. Nous sommes en train de regarder pour un partenariat avec cette entreprise et l'équipe Capsule.
Si DIS identifié, préciser l'adéquation du projet avec le DIS (2000 car. maximum)	cybersécurité: il s'agit d'un sujet de cryptographie
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)	non
Cotutelle financière internationale (oui/non)	non
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	pas de cofinanceur
Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE	Pas de cofinancement entreprise
État du cofinancement (indiquer "acquis" ou "demandé")	pas de cofinanceur
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	Masculin
Nationalité	Française

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
29/01/2025	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.	cvfouque-hdr.pdf	Non traité	

29/01/2025	ARED - Dépôt - Avis directeur·rice d'unité	Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger"		Non traité	
29/01/2025	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
29/01/2025	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
29/01/2025	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
29/01/2025	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
29/01/2025	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	
29/01/2025	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
29/01/2025	ARED - Versement 2 - CV doctorant.e	Pour versement tranche 2	CV_PaulD_2025_01_29.pdf	Non traité	
29/01/2025	ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 2		Non traité	
29/01/2025	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
29/01/2025	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
29/01/2025	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
29/01/2025	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
29/01/2025	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
29/01/2025	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3		Non traité	

Université de Rennes 1 - INRIA Rennes
Campus de Beaulieu
35042 RENNES Cedex
☎ *+33.2.99.84.75.58*
✉ *Pierre-Alain.Fouque@inria.fr*
Français, né le 25 mars 1974 (50 ans),
PACSE, 2 enfants (18 et 21 ans)
`http://www.di.ens.fr/~fouque`

Pierre-Alain Fouque

Fonctions exercées

Depuis 2023 **Responsable équipe CAPSULE**, *IRISA (UMR 6074) / Inria Université de Rennes*, Sécurité embarqué et Cryptographie, 7 permanents (1 Prof., 2 MCF et 4 CR Inria). `http://www.irisa.fr/capsule/`, **Resp. du projet PQ-TLS du PEPR Quantique**

Depuis 2023 **Membre Senior de l'IUF (Institut Universitaire de France)**.

2015-2020 **co-responsable équipe EMSEC**, *IRISA*, Sécurité embarqué et Cryptographie, 8 permanents (2 Prof., 2 MCF et 4 CNRS), `http://www.irisa.fr/emsec/`.

Depuis 2012 **Professeur des Universités**, *Université de Rennes 1, Unité de formation et de recherche en Informatique et en Électronique (ISTIC)*, **Responsable de l'EUR Cyberschool**.

2003 – 2012 **Maître de Conférences en Informatique**, *École normale supérieure*, Paris, Délégation INRIA dans l'équipe Celtique (Rennes) 2011–2012.

2001 - 2003 **Chercheur en Cryptographie**, *Laboratoire de Cryptographie de la DCSSI*, Paris.

Diplômes

Déc. 2010 **Thèse d'Habilitation à Diriger des Recherches**, *Sur Quelques Méthodes Algébriques et Statistiques en Cryptanalyse*, Sous la Direction de Jacques Stern, École normale supérieure (ENS).

Oct. 2001 **Thèse de Doctorat**, *Le partage de clés Cryptographiques: Théorie et Pratique*, Sous la Direction de Jacques Stern, Université de Paris 7. Thèse effectuée à l'ENS.

Encadrements

Thèses Soutenues

S. Zimmer Mécanismes cryptographiques pour la génération de clefs et l'authentification (soutenue en septembre 2008). Co-encadrement avec David Pointcheval (50%)

G. Macario-Rat Cryptanalyse de schémas multivariés (soutenance le 28 Juin 2010). Thèse effectuée au sein d'Orange Labs. Co-encadrement avec Jacques Stern (50%)

G. Leurent Cryptanalyse de fonctions de hachage (soutenue le 30 septembre 2010). Encadrement officieusement avec David Pointcheval.

C. Bouillaguet Modes opératoires pour les fonctions de hachage et cryptanalyse multivariée (soutenue le 26 septembre 2011)

D. Masgana-Leresteux Injection de fautes et de logiciels sur les implémentations cryptographiques (soutenue le 10 Juillet 2012)

J. Jean Cryptanalyse de primitives symétriques basées sur le chiffrement AES (soutenue en 2013).

P. Derbez	Attaques par rencontre par le milieu sur l'AES (depuis septembre 2010).
J.C. Zapalowicz	Sécurité des générateurs pseudo-aléatoires et des implémentations de schémas de signature à clé publique (soutenue en 2014).
S. Belaïd	Security of cryptosystems against power-analysis attacks (soutenue en 2015).
B. Minaud	Analyse de primitives cryptographiques récentes (soutenue en 2016).
B. Richard	Étude des protocoles d'authentification et de dérivation de clés en 3 parties (soutenue en 2017).
P. Lestringant	Identification d'algorithmes cryptographiques dans du code natif (soutenue en 2017).
R. Bost	Algorithmes de recherche sur bases de données chiffrées (soutenue en 2018).
C. Delaplace	Algorithmes d'algèbre linéaire pour la cryptographie (soutenue en 2018).
Q. Chen	Lossy trapdoor primitives, zero-knowledge proofs and applications (soutenue en 2019).
B. Lambin	Optimization of core components of block ciphers (soutenue en 2019).
P. Bert	Signatures reposant sur les réseaux euclidiens: de la construction à l'implémentation (soutenue en 2019).
A. Siffer	New Statistical methods for data mining, contributions to anomaly detection and unimodality testing (soutenue en 2019).
T. Espitau	Algorithmic aspects of algebraic lattices (soutenue en 2020).
A. Bossuat	Provable security of real world protocols (soutenue en 2020).
K. Boudgoust	Theoretical hardness of algebraically structured learning with errors (soutenue en 2021).
C. Duguey	On the security of instant messaging: towards solutions for multi-device and group applications (soutenue en 2021).
V. Mollimard	Algorithmes pour la cryptanalyse différentielle (soutenue en 2022).
A. Nedelcu	A cryptographic approach to preventing unauthorized access (soutenue en 2022).
D. De Almeida Braga	Cryptography in the wild: the security of cryptographic implementations (soutenue en 2022).
D.P. Pham	Leveraging side-channel signals for IoT malware classification and rootkit detection (soutenue en 2022).
L. Prabel	Trapdoors in lattice-based cryptography: applications and implementation (soutenue en 2023).
G. Patat	Bust the trust: dissect and analyze the security and privacy impacts of the widewine DRM (soutenue en 2023).
A. Cheriere	Side-channel resistance of cryptographic primitives based on error-correcting codes (soutenue en 2022).
O. Bernard	Algebraic cryptanalysis of the shortest vector problem in ideal lattices (soutenue en 2022).
C. Jeudy	Design of advanced post-quantum signature schemes (soutenue en 2024).

Publications scientifiques

140 publications dans des conférences internationales et 26 articles dans des revues internationales (dont 47 dans des conférences et journaux de rang A* et 48 dans des conférences et journaux de rang A). Dans les 25 premiers publiant dans des conférences majeures en cryptographie cf. `http://www.iacr.org/cryptodb/` et premier français.

PAUL DELHOM

Cryptology and Cybersecurity Engineer

paul.delhom0@gmail.com https://www.linkedin.com/in/paul-delhom/

PROFESSIONAL EXPERIENCE

CNRS Cryptography Research Engineer
at IRISA laboratory in CAPSULE team

Jan 2025 – Ongoing Rennes, France

- Research on side-channel aspect of Codes, skew Codes and MPCitH
- Supervised by Pierre-Alain Fouque in the ANR CROWD

Inria Cryptography Research Intern
at IRISA laboratory in CAPSULE team

May 2024 – Oct 2024 Rennes, France

- Research on MPCitH schemes involving Lattices
- Supervised by Pierre-Alain Fouque in the BPI RESQUE project

Software and Security Engineer Intern
at CYSEC, Decentralized Computing & Space Security

Mar 2023 – Aug 2023 Lausanne, Switzerland

- Rust development of SDLS protocol with its extended procedures (SDLS EP), SDLS secures space telecommunications on OSI layer 2
- Design engineering of parts of the SDLS EP library: ARCA SATLINK

Software and Security Engineer Intern
at NANO Corp, Network Traffic Analysis & Cybersecurity

Aug 2022 – Feb 2023 Paris, France

- Reverse Engineering of network protocols
- Rust development of protocol detection in the probe: n.Scope NDR

SKILLS & MASTER LEVEL COURSES

Cryptology

- Grasp of the state-of-the-art of Multi-Party Computation in the Head, Zero-Knowledge Proofs of Knowledge with Lattices and Codes schemes (in my last internship and my current research)
- Security proofs of cryptographic primitives (course from Pierre-Alain Fouque and Olivier Sanders, I am now the TA of the course)
- Secure cryptography implementation, side-channel and fault attacks (courses from Benoît Gérard, Damien Marion and Ronan Lashermes, partially from my internship at CYSEC and in my current research)
- Cryptanalysis (course from Patrick Derbez and cryptohack website)
- Mathematical foundations for modern cryptology: Algebra & Cryptology (course from Rémi Géraud-Stewart)

Cybersecurity

- Offensive: reverse engineering, memory attacks and pentesting
- Defensive: steganography, OS security and data privacy

Programming

- Professional level in Rust and Git
- Skilled in C, C++, SageMath, Python and OCaml
- Can code in R, Bash and Java

EDUCATION

MEng specialized in Cybersecurity ("Diplôme d'ingénieur") and BE
CentraleSupélec, Paris-Saclay University School of Engineering

Sept 2018 – Oct 2024

MSc in Computer Science Research (Master SIF)
University of Rennes

Sept 2023 – Oct 2024

ACTIVITIES

- Core Technical Staff of ViaRézo, IT and Network student association of CentraleSupélec from 2020 to 2022
- Member of the Jury at the TFJM² 2022 session of Île-de-France, a math competition for high school students
- Participation in CTFs: TRACS 2022-23-24, Insomni'hack 2023, FCSC 2024
- Cryptanalysis challenges on cryptohack website (top 1.2% of users with more than 105 challenges solved)
- Mathematics and Computer Science tutoring and presentations for high school students (2020-2024)
- Project for the French Ministry of the Interior and the Armed Forces on IoT security on networks (2022)

INTERESTS

Alpinism | Climbing | Hiking | Cybersecurity

PERSONALITY

Curious | Persistent | Teamwork Spirit | Adaptive

LANGUAGES

French
Native

English
Fluent
C1 level
100/120 TOEFL IbT Oct 2022