# Demande n°4276 - ARED

# Acronyme :HardRocq

## Identification

### Identification

| | |
|---|---|
| **N°** | 4276 |
| **Année** | 2026 |
| **Statut** | Soumis à l'établissement |
| **Date de création** | 28/01/2026 |
| **Date de modification** | 28/01/2026 |
| **Date de soumission** | 28/01/2026 |
| **Acronyme** | HardRocq |
| **Intitulé du projet / thèse** | Implémentation et vérification formelle d'enclaves et de capacités dans un processeur RISC-V |
| **Dispositif** | ARED |

## Priorité régionale

### Priorité régionale

| | |
|---|---|
| **Priorité régionale** | 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 (DIS) principal** | Économie numérique sécurisée et responsable |
| **Levier thématique associé au DIS principal** | Cybersécurité |
| **Axe transversal : transitions climatique et écologique** | Non concerné |
| **Axe transversal : cohésion et inclusion sociale** | Non concerné |

## Organisme de tutelle

### Organisme de tutelle

| | |
|---|---|
| **Établissement** | UNIVERSITE RENNES |
| **Commune** | RENNES |
| **Civilité** | Monsieur |
| **Nom** | Barais |
| **Prénom** | Olivier |

# Unité de recherche

## Unité de recherche

| | |
|---|---|
| **Nom de l'unité** | IRISA |
| **Civilité** | Monsieur |
| **Nom** | Barais |
| **Prénom** | Olivier |
| **Courriel** | olivier.barais@irisa.fr |

## Données complémentaires de l'unité de recherche

| Libellé | Valeur |
|---|---|
| Statut et numéro de l'unité de recherche (UMR, USR, EA) | UMR IRISA |
| Le cas échéant, nom de l'équipe de recherche | Epicure et SUSHI |
| Le cas échéant, nom du responsable de l'équipe de recherche | Thomas Jensen (Epicure) et Guillaume Hiet (SUSHI) |
| Activités de recherche et points forts de l'équipe | L'équipe EPICURE apportera son expertise dans la vérification formelle, en particulier dans le domaine de la compilation. L'équipe SUSHI apportera son expertise dans le développement et la preuve de mécanismes de sécurité matériels,. |
| 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) | Dans le cadre du développement de systèmes critiques, des composants de différents niveaux de confiance et de différentes provenances (industrielle, militaire, etc.) peuvent s'exécuter sur un même processeur. Plusieurs approches permettent l'isolation de différents domaines sur une même machine. L'objectif de cette thèse est d'explorer différents mécanismes d'isolation, comme les enclaves ou les capacités (e.g. CHERI), et d'évaluer la mise en œuvre de ces mécanismes en termes de coûts (impact sur le temps d'exécution, l'occupation mémoire, la complexité du circuit, etc.) et de sécurité.<br>Par ailleurs, l'utilisation de produits de sécurité dans un contexte gouvernemental ou militaire passe par une évaluation de la sécurité de ces produits, typiquement une évaluation Critères Communs à un haut d'assurance (EAL7). Ce niveau d'assurance nécessite le développement d'une preuve formelle de la sûreté et de la sécurité du système. Nous proposons donc de développer des approches permettant de formaliser et prouver ces mécanismes d'isolation qui nécessitent un support à la fois du matériel et du compilateur.<br><br>Un premier objectif de cette thèse est d'implémenter, au sein d'un processeur RISC-V, des mécanismes de sécurité matériels, qui permettent d'une part à plusieurs entités ne se faisant pas confiance de s'exécuter simultanément sur un même processeur, et d'autre part de garantir la sûreté des programmes exécutés. Nous proposons de nous focaliser sur deux mécanismes complémentaires : les enclaves et les capacités.<br>Au-delà de l'implémentation matérielle de ces mécanismes de sécurité, un second objectif est de fournir une preuve formelle de la correction de ces mécanismes de sécurité, par exemple |

| Libellé | Valeur |
|---|---|
| | de la correction de ces mécanismes de sécurité, par exemple dans l'assistant de preuve Rocq, avec l'aide d'un solveur SMT. Un troisième objectif est de prouver des propriétés de sécurité (sûreté mémoire, isolation, etc.) sur un système logiciel/matériel où le compilateur tire parti des mécanismes fournis par le matériel.<br>Ces objectifs de preuve mécanisée à l'interface logiciel/matériel font l'originalité de cette thèse. |
| Caractère structurant/stratégique du projet (descriptif/ex. : art.5 Rglmt ARED 2026 -2000 car. max) | Cette thèse sera co-encadrée par Sandrine Blazy (équipe Epicure), Pierre Wilke et G.Hiet (équipe SUSHI). Il s'agira de poursuivre une collaboration récente initiée dans le cadre du projet SecurEval du PEPR Cybersécurité auquel participent nos deux équipes appartenant à deux départements de l'IRISA.<br><br>Cette thèse s'inscrit dans le Domaine d'Innovation Stratégique (DIS) 3.3 "Économie numérique sécurisée et responsable", en particulier le levier Cybersécurité. Les mécanismes d'enclave et les capacités CHERI devraient intéresser les équipes de DGA-MI car ils ont vocation à être intégrés dans les systèmes militaires. Cet intérêt a d'ailleurs été marqué lors de la visite de Robert Watson et Carl Shaw (Codasip) qui développent le projet CHERI lors du séminaire SoSySec / SemSecuElec du 12 septembre 2025.Par ailleurs, le développement de mécanismes pour l'architecture RISC-V répond à l'enjeu de souveraineté nationale et européenne. Ce choix technologique est d'ailleurs poussé par des industriels dont Thales. |
| Porteur du projet : date d'obtention de l'HDR ou dérogation | Sandrine Blazy HDR obtenue en octobre 2008 |
| Collaborations scientifiques (nature/pays) et partenariat socio-économique envisagé (3000 car. max.) | L'équipe EPICURE apportera son expertise dans la vérification formelle, en particulier dans le domaine de la compilation. L'équipe SUSHI apportera son expertise dans le développement et la preuve de mécanismes de sécurité matériels, notamment la maîtrise du langage Kôika et son écosystème. Nous envisageons de collaborer avec Jan-Tobias Muehlberg (Université Libre de Bruxelles), qui a participé au développement du processeur Sancus, qui intègre un mécanisme d'enclaves offrant des garanties de disponibilité (Aion), mais dont la preuve n'est pas mécanisée. |
| 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 2026) | |
| Cotutelle financière internationale (oui/non) | non |
| Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s) | DGA Creach Labs |
| Si cofinancement industriel, justifier le choix du dispositif ARED au lieu du dispositif CIFRE | |
| État du cofinancement (indiquer "acquis" ou "demandé") | demandé |
| Si demandé, date prévisionnelle de réponse du cofinanceur | 5/6/2026 |
| Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s) | |
| Si reversement prévu, préciser (partenaire, montant) | |

## Candidat

## Collaboration internationale

### Collaboration internationale

| | |
|---|---|
| **Pays** | |
| **Etablissement partenaire à l'étranger** | |

## Pièces jointes

| Date de mi | Type de pièce | Commentaire | Document | Valide | Commentaire |
|---|---|---|---|---|---|
| 28/01/2026 | 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. | cv-2p.pdf | Non traité | |
| 28/01/2026 | ARED - Dépôt - Avis directeur·rice d'unité | Obligatoire - Voir le modèle à suivre dans l'onglet "Documents à télécharger" | | Non traité | |
| 28/01/2026 | ARED - Dépôt - Justificatif cofinancement | Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti... | | Non traité | |
| 28/01/2026 | ARED - Dépôt - Lettre partenaire étranger | Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale | | Non traité | |
| 28/01/2026 | ARED - Dépôt - Pièce complémentaire | Facultatif | | Non traité | |
| 28/01/2026 | ARED - Dépôt - Pièce complémentaire | Facultatif | | Non traité | |
| 28/01/2026 | 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 | |
| 28/01/2026 | ARED - Versement - Convention de partenariat | Le cas échéant (si autorisation de reversement) | | Non traité | |
| 28/01/2026 | ARED - Versement 2 - CV doctorant.e | Pour versement tranche 2 | | Non traité | |
| 28/01/2026 | ARED - Versement 2 - Copie du contrat doctoral (ou CDD ou attestation)) | Pour versement tranche 2 | | Non traité | |
| 28/01/2026 | ARED - Versement 2 - Attestation bon déroulement travaux année 1 | Pour versement tranche 2 | | Non traité | |
| 28/01/2026 | ARED - Versement 2 - Bilan financier année 1 | Pour versement tranche 2 ARED | | Non traité | |
| 28/01/2026 | ARED - Versement 3 - Attestation bon déroulement travaux année 2 | Pour versement 50% tranche 3 ARED | | Non traité | |
| 28/01/2026 | ARED - Versement 3 - Bilan financier année 2 | Pour versement 50% tranche 3 ARED | | Non traité | |
| 28/01/2026 | ARED - Versement 4 - Bilan financier année 3 | Pour versement solde année 3 ARED | | Non traité | |
| 28/01/2026 | ARED - Versement 4 - Certificat administratif précisant statut thèse | Pour versement du solde de la tranche 3 | | Non traité | |

# Sandrine Blazy

sandrine.blazy@irisa.fr
http://people.irisa.fr/Sandrine.Blazy




## Professional activities

2009 – · · · · **Full professor of Computer Science.** University of Rennes, IRISA laboratory.
Member of Epicure, a joint team with Inria, CNRS, University of Rennes and ENS Rennes

2020 – · · · · **Member of the GDR GPL scientific committee**

2015 – · · · · **Member of the IFIP group "W.G. 1.9/2.15 on verified software"**

**Member of the IFIP group "W.G. 2.11 on program generation"**

2024 – · · · · **Member of the editorial board of the LMCS journal**

2026 – · · · · **Chair of GDR GPL's PhD thesis award committee**

## Awards

2023 **CNRS Silver Medal**

**Lucas award from FME board** for a highly influential paper published at FM 2006 with Z.Dargaye and X.Leroy

2022 **ACM SIGPLAN Programming Languages Software Award**, with X. Leroy, Z. Dargaye, J.H. Jourdan, M.Schmidt, B. Schommer, and J.B. Tristan for the development of the CompCert verified compiler

2021 **ACM Software System Award**, with X. Leroy, Z. Dargaye, J.H. Jourdan, M. Schmidt, B. Schommer, and J.B. Tristan

2011 **La Recherche award in Information Sciences**, La Recherche magazine, with X.Leroy, Z.Dargaye and J.B. Tristan

## Past professional activities

2021 – 2025 **Deputy Director of IRISA** (CNRS UMR 6074)

2016 – 2021 **Member of the national committee for scientific research** (CoNRS)

2015 – 2018 **Co-head of the LTP group** (Languages, Types, Proofs) of the GDR GPL

2013 – 2017 **Co-head of the research master in computer science** at the University of Rennes, shared by 9 Breton universities and engineering schools

2012 – 2013 **Scientific director of the languages and software engineering department** of IRISA

2009 – 2013 **Head of the Information Systems Security track** of the computer science Master's degree

2004 – 2006 **Sabbatical,** Inria Paris

1994 – 2009 **Lecturer,** ENSIIE

## Education

2008 **Habilitation to supervise research,** University of Évry Val d'Essonne, *"Formal semantics"*

1993 **Ph.D.,** CNAM, *"Program specialisation as an aid to the understanding of Fortran programs"*

1990 **M.Sc. in computer science,** Sorbonne University

**Engineering degree in computer science**, ENSIIE

## Research interests

Keywords formal semantics of programming languages, deductive verification, verified compilation, static analysis, software security

## Advising

| | |
|---|---|
| 2023 – · · · · | Clément Chavanon, *"Refinement of formal specification for trusted secure environments"* (with F.Besson) |
| 2022 – · · · · | Tony Law, *"Verified compilation for high-level synthesis"* (with D.Demange) |
| 2022 – 2025 | Sophia La Spina, *"Formal verification of weak topological orderings and data-flow analysis"* (with D.Demange) |
| 2019 – 2022 | Aurèle Barrière, *"Formal verification of just-in-time compilation"* (with D.Pichardie) **EAPLS PhD award** |
| 2018 – 2021 | Rémi Hutin, *"Verified secure compilation against timing side-channels"* (with D.Pichardie) |
| · · · · – 2018 | Supervised 7 PhD students who graduated in 2018, 2017, 2016, 2015, 2015, 2014 and 2010 |
| | Supervised 26 Master's students |

## Recent professional service

### Conference organisation

| | |
|---|---|
| 2026 | **POPL** general chair |
| 2024, 2025 | **CPP** conference co-chair |
| 2013, 2015, 2017 | **CoqPL'17** workshop co-chair, **ITP'13** and **SAS'15** conference co-chair |
| 2016 | **VSTTE** conference co-chair, and **PLMW**@SPLASH mentoring workshop co-chair |

### Program committee member

| | |
|---|---|
| 2021 – | ICFP, PriSC, FMTea, Types, ESOP, POPL, ECOOP, Types, ITP, FM, ProLaLa |
| 2019 – 2020 | GPCE, TyDe, ICFP (ERC), PriSC, POPL, APLAS, ITP |
| 2017 – 2018 | CoqPL, CPP, IFL, SRC@PLDI, TFP, VSTTE, GPCE, LOPSTR, ICFP, Euro S&P |

### Jury member

| | |
|---|---|
| 2023 | **French Open Science award for free research software** chair of the jury |
| 2022 – 2024 | **ACM SIGPLAN Robin Milner Young Researcher Award** member of the jury |

## Recent selected invited talks

| | |
|---|---|
| 2025 | **Trusting compilers and more: mechanized semantics to the rescue**, ECRTS |
| 2024 | **Form mechanized semantics to verified compilation**, ETAPS unifying keynote |
| 2023 | **CompCert: a journey through the landscape of mechanized semantics for verified compilation**, CPP |
| 2022 | **Obfuscation du logiciel : brouiller le code pour protéger les programmes**, Collège de France |
| 2021 | **A tutorial on teaching deductive verification with Why3**, Tutorial Series of the FME Teaching Committee |
| 2020 | **From Verified Compilation to Secure Compilation: a Semantic Approach**, PLAS |
| 2019 | **Formal Verification of a Constant-Time Preserving C Compiler**, Verified software workshop, Newton institute |

## Publications

| | |
|---|---|
| Journals | Co-author of 16 articles, including Journal on Automated Reasoning (JAR) |
| Conferences | Co-author of 50 peer-reviewed papers, incl. POPL, ICFP, OOPSLA, ESOP, ITP, IJCAR, LCTES, CSF, CPP |
| Books | Co-author of a book chapter |
| Proceedings | Co-editor of a special issue of JAR, and of 5 conference proceedings (ACM and LNCS) |

## Recent lecturing

| | |
|---|---|
| Current | software foundations (M1), deductive verification (L3) |
| Previously | software vulnerabilities (M2), static analysis (M1), functional programming (L3) |