Demande n°3166 - ARED

Acronyme :LOTR

Identification

Identification

N°	3166
Année	2023
Statut	Brouillon
Date de création	30/01/2023
Date de modification	01/02/2023
Date de soumission	01/02/2023
Acronyme	LOTR
Intitulé du projet	Lord Of The RISCV
Dispositif	ARED
Civilité du porteur	
Nom du porteur	Derrien
Prénom du porteur	Steven
Courriel	steven.derrien@irisa.fr

Priorité régionale

Stratégie régionale de recherche et d’innovation (S3)

Stratégie régionale de recherche et d’innovation (S3)

Axe transversal	Transitions numérique et industrielle
Domaine d'innovation stratégique	Économie numérique sécurisée et responsable
Domaine d'innovation stratégique	.
Levier thématique	Cybersécurité
Domaine d'innovation statégique Secondaire	Hors DIS
Domaine d'innovation statégique Secondaire	.

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	UMR IRISA
Civilité	Monsieur
Nom	Gravier
Prénom	Guillaume
Courriel	guillaume.gravier@irisa.fr

Données complémentaires de l'unité de recherche

Libellé	Valeur
Statut et numéro de l'unité de recherche (UMR, USR, EA?)	6074
Le cas échéant, nom de l'équipe de recherche	Équipe TARAN
Le cas échéant, nom du responsable de l'équipe de recherche	Olivier Sentieys
Activités de recherche et points forts de l'équipe	L'équipe CAIRN mène des activités de recherches sur thème des outils d'aide à la conception de circuits et de processeurs. Elle regroupe à la fois des chercheurs en informatique et en électronique, ce qui lui permet de disposer d'une expertise unique.
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)	La grande majorité des plates-formes automobiles et Internet des Objets s'appuient sur des unités de microcontrôleur basse consommation, dont la micro-architecture et les ensembles d'instructions sont fortement spécialisés. Ces processeurs personnalisés sont conçus à la main à l'aide de langages de description de matériel. Concevoir un pipeline de processeur à ce niveau d'abstraction est très fastidieux et extrêmement chronophage. La possibilité de déduire automatiquement une micro-architecture (ou un ensemble de microarchitectures) à partir d'une représentation plus abstraite (par exemple un modèle comportemental du processeur en C/C++) peut être une réponse à ces problèmes. Elle permettrait de rationaliser le processus de conception tout en permettant une exploration précoce de l'espace de conception.

Libellé	Valeur
	Malheureusement, les outils capables de traduire du C/C++ sous la forme de circuits sont incapables de traiter efficacement ce type de modèle, parce qu'ils n'ont pas la capacité d'exploiter des techniques de spéculation. Des résultats de recherche récents issus de l'IRISA ont cependant montré que cette limitation pouvait être levée et qu'il était possible de générer automatiquement des pipelines de processeurs dont les performances et le coût surfacique étaient comparables à des conceptions manuelles. De nouvelles problématiques de conception émergent cependant : en plus des contraintes de performances et d'énergie, les plateformes matérielles IoT doivent désormais également intégrer des garanties de sécurité et de prévisibilité. De telles garanties sont très difficiles à appliquer, car elles impliquent une compréhension approfondie de la micro-architecture sous-jacente ainsi que des modifications souvent subtiles (et ad hoc) de la conception HDL. Elles ne peuvent donc être mise en œuvre que par des experts du domaine, et seulement au prix d'importants efforts de conception supplémentaires. Ces garanties non fonctionnelles ont également souvent un impact négatif sur les performances et le coût du matériel. Par conséquent, le choix de la meilleure conception implique un compromis entre des exigences contradictoires, et les contraintes de temps de conception obligent souvent les concepteurs à opter pour des solutions sous-optimales. L'objectif du projet est de proposer de nouvelles techniques de synthèse micro-architecturale, dans lesquelles les propriétés non fonctionnelles sont soutenues par une analyse spécifique à un domaine (pour la prévisibilité) et des transformations (pour la sécurité). En raison de sa licence ouverte et de sa popularité croissante, le projet se concentrera sur le jeu d'instruction open-source RISC-V.
Porteur du projet : date d'obtention de l'HDR ou dérogation	HDR obtenue en 2011
Hypothèses, questions posées, points de blocage, approche méthodologique, technique (4000 car. max)	L'objectif de la thèse est d'étudier et de proposer de nouvelles techniques de synthèse micro-architecturale, dans lesquelles les propriétés non fonctionnelles sont gérées au travers d'analyse spécifique et de transformations appliquées sur un modèle abstrait de micro architecture. En raison de sa licence open-source et de sa popularité croissante, le projet se concentrera sur le jeu d'instruction RISC-V.
Environnement scientifique, positionnement dans contexte régional/national/international (2000 car.)	La thèse se déroulera au sein de l'IRISA, dans l'équipe CAIRN (équipe commune INRIA/IRISA). - LIRISA (Institut de Recherche en Informatique et Systèmes Aléatoires) est aujourd'hui l'un des plus grands laboratoires de recherche français (+ de 850 personnes) dans le domaine de l'informatique et des nouvelles technologies de l'information. - Le centre de recherche INRIA Rennes-Bretagne Atlantique a été crée en 1980. Il regroupe 630 personnes de 47 nationalités différentes dans 31 équipes de recherche et 8 services dappui. - Les activités de l'équipe TARAN dans domaine de la synthèse de matériel spécialisé sont reconnues au niveau international, et l'équipe dispose de plus de 25 ans d'expertise sur ce domaine.
Collaborations scientifiques (nature/partenariat/pays) et partenariat socio-économique envisagé	
Adéquation du projet avec le DIS de rattachement (3000 caractères maximum)	Le projet se rattache naturellement au DIS 3 "ECONOMIE NUMERIQUE SECURISEE ET RESPONSABLE". De plus, et comme expliqué en détail ci-après, la méthodologie qui y sera développée a vocation à répondre à des enjeux spécifiques aux domaines de la cybersécurité. Le cœur d'un objet connecté consiste en un processeur conçu pour offrir un maximum de performance pour une enveloppe de coût énergétique très faible. Développer ce type de circuits ex-nihilo représente un effort de conception et de vérification gigantesque, qui est hors de portée des industriels du secteur. Les plateformes matérielles actuelles sont donc contraintes de reposer sur des solutions "sur étagères" basées sur des jeux

	d'instructions propriétaires (exemple : jeux d'instruction ARM). Ces approches limitent de fait les possibilités de différenciation et de "customisation" que ce soit au niveau du jeu d'instruction ou de l'architecture matérielle en tant que telle. L'émergence du jeu d'instruction libre RISC-V (www.riscv.org) et sa popularité croissante dans le domaine de l'Internet des Objets offre de nouvelles opportunités : il devient possible d'enrichir le jeu d'instruction et/ou d'ajouter des mécanismes matériels spécifiques à un processeur, en fonction des besoins, et sans les contraintes de propriété intellectuelle d'un jeu d'instructions propriétaire. Par exemple, dans un contexte cybersécurité, il rend possible la définition de nouvelles instructions dédiées au traitement cryptographique (crypto-processeurs), et/ou l'introduction de mécanismes de contre-mesures (ex : vérification d'intégrité du flot de contrôle, des données ou du temps d'exécution). Cette possibilité reste cependant difficile à exploiter à cause de l'effort de conception associé. S'il existe des outils logiciels d'aide à la conception de processeurs, leurs fonctionnalités sont très limitées et n'ont que peut évoluées depuis la fin des années 90. Cet état de fait est d'autant plus surprenant étant donné les progrès colossaux réalisés dans des domaines connexe (par exemple la synthèse automatique d'accélérateur matériels via les techniques de synthèse de haut-niveau). L'objectif du projet est donc de proposer une nouvelle génération d'outil d'aide à la conception de processeurs, en revisitant les approches existantes à l'aune de nombreux résultats récents, dont ceux issus des recherches de l'équipe TARAN de l'IRISA sur la synthèse automatique d'architectures spéculatives. Ces outils seront évalués et validés sur des études de cas issues de la cybersécurité (contrôle d'intégrité en matériel) .
Si priorité régionale, préciser (200 caractères maximum)	
Cotutelle internationale (indiquer "oui" ou "non"; si oui, préciser le pays et l'établissement)	
Nom(s) du(des) cofinanceur(s) envisagé(s) ou confirmé(s)	Université de Rennes
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	
Si cofinancement refusé, autre(s) source(s) de cofinancement identifiée(s)	
Si reversement prévu, préciser (partenaire, montant)	

Candidat

Candidat

Genre	Masculin
Nationalité	Français

Collaboration internationale

Collaboration internationale

Pays	
Etablissement partenaire à l'étranger	

Pièces jointes

Date de mi	Type de pièce	Commentaire	Document	Valide	Commentaire
01/02/2023	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_ARED_23.pdf	Non traité	
01/02/2023	ARED - Dépôt - Avis directeur·rice d'unité	15 lignes maximum		Non traité	
01/02/2023	ARED - Dépôt - Justificatif cofinancement	Facultatif - Dépôt de demande, justificatif d'obtention, courrier du cofinanceur pressenti...		Non traité	
01/02/2023	ARED - Dépôt - Lettre partenaire étranger	Facultatif - Lettre d'engagement de l'établissement partenaire étranger en cas de cotutelle internationale		Non traité	
01/02/2023	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
01/02/2023	ARED - Dépôt - Pièce complémentaire	Facultatif		Non traité	
01/02/2023	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	
01/02/2023	ARED - Versement - Convention de partenariat	Le cas échéant (si autorisation de reversement)		Non traité	
01/02/2023	ARED - Versement 1/2 - CV doctorant.e	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	
01/02/2023	ARED - Versement 1/2 - Copie du contrat doctoral (ou CDD ou attestation))	Pour versement tranche 1 (cohortes jusqu'en 2018) Pour versement tranche 2 (cohortes à partir de 2019)		Non traité	
01/02/2023	ARED - Versement 1 - Lettre d'approbation école doctorale	Pour versement tranche 1 (cohortes jusqu'en 2018)		Non traité	
01/02/2023	ARED - Versement 2 - Attestation bon déroulement travaux année 1	Pour versement tranche 2		Non traité	
01/02/2023	ARED - Versement 2 - Bilan financier année 1	Pour versement tranche 2 ARED		Non traité	
01/02/2023	ARED - Versement 3 - Attestation bon déroulement travaux année 2	Pour versement 50% tranche 3 ARED		Non traité	
01/02/2023	ARED - Versement 3 - Bilan financier année 2	Pour versement 50% tranche 3 ARED		Non traité	
01/02/2023	ARED - Versement 4 - Bilan financier année 3	Pour versement solde année 3 ARED		Non traité	
01/02/2023	ARED - Versement 4 - Certificat administratif précisant statut thèse	Pour versement du solde de la tranche 3 (à accompagner des pièces justificatives correspondantes pour les cohortes jusqu?en 2018 : avis du jury, attestation de réinscription en ED, justificatif de prolongation ou d'abandon)		Non traité	

		d'abandon)			
01/02/2023	ARED - Versement 4 - Avis du jury si thèse soutenue	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
01/02/2023	ARED - Versement 4 - Attestation de réinscription en ED	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
01/02/2023	ARED - Versement 4 - Justificatif de prolongation	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	
	ARED - Versement 4 - Justificatif d'abandon de thèse	Pour versement solde tranche 3 ARED (cohortes jusqu'en 2018)		Non traité	