Projet ANR-19-CE39-0008

ARCHI-SEC

[A Identification 2](#_Toc293389211)

[B Livrables et jalons 2](#_Toc293389212)

[C Rapport d’avancement 2](#_Toc293389213)

[C.1 Objectifs initiaux du projet 2](#_Toc293389214)

[C.2 Travaux effectués et résultats atteints sur la période concernée 2](#_Toc293389215)

[C.3 Difficultés rencontrées et solutions 2](#_Toc293389216)

[C.4 Faits et résultats marquants 3](#_Toc293389217)

[C.5 Travaux spécifiques aux entreprises (le cas échéant) 3](#_Toc293389218)

[C.6 Réunions du consortium (projets collaboratifs) 3](#_Toc293389219)

[C.7 Commentaires libres 3](#_Toc293389220)

[D Valorisation et impact du projet depuis le début 4](#_Toc293389221)

[D.1 Publications et communications 4](#_Toc293389222)

[D.2 Autres éléments de valorisation 4](#_Toc293389223)

[D.3 Pôles de compétitivité (projet labellisés) 5](#_Toc293389224)

[D.4 Personnels recrutés en CDD (hors stagiaires) 6](#_Toc293389225)

[D.5 État financier 6](#_Toc293389226)

[E Annexes éventuelles 6](#_Toc293389227)

Ce document est à remplir par le coordinateur en collaboration avec les partenaires du projet. Il doit être transmis par le coordinateur aux échéances prévues dans les actes attributifs :

1. à l’ANR
2. aux pôles de compétitivité ayant accordé leur label au projet.

L’ensemble des partenaires doit avoir une copie de la version transmise à l’ANR.

Il doit être accompagné d’un résumé public du projet mis à jour, conformément au modèle associé à ce document.

Ce modèle doit être utilisé uniquement pour le(s) compte(s)-rendu(s) intermédiaire(s) défini(s) dans les actes attributifs de financement, hors rapport T0+6 pour lequel il existe un modèle spécifique. Il existe également un modèle spécifique au compte-rendu final.

# Identification

|  |  |
| --- | --- |
| Acronyme du projet | ARCHISEC |
| Titre du projet | Etude de la sécurité au niveau micro-architecture |
| Coordinateur du projet (société/organisme) | Télécom Paris/LTCI |
| Date de début du projetDate de fin du projet | 1/10/201930/09/2023 |
| Labels et correspondants des pôles de compétitivité(pôle, nom et courriel du corresp.) |  |
| Site web du projet, le cas échéant | https://archi-sec.telecom-paristech.fr/ |

|  |
| --- |
| Rédacteur de ce rapport   |
| Civilité, prénom, nom | Mr Jean-Luc Danger |
| Téléphone | 06 82 03 59 57 |
| Courriel | Jean-luc.danger@telecom-paris.fr |
| Date de rédaction |  |
| Période faisant l’objet du rapport d’activité | 1/10/2019 \_ 30 /04/2021 |

# Livrables et jalons

Quand le projet en comporte, reproduire ici le tableau des jalons et livrables fourni au début du projet. Mentionner l’ensemble des livrables, y compris les éventuels livrables abandonnés, et ceux non prévus dans la liste initiale.

| **N°** | **Intitulé** | **Nature\***  | **Date de fourniture** | **Partenaires** (souligner le responsable) |
| --- | --- | --- | --- | --- |
| Prévue initialement | Replanifiée | Livrée |
| D1.1 | Version initiale de la plate-forme virtuelle Gem5 | Plate-forme | T0+12 |  |  | TPT |
| D1.2 | Plateforme Gme5 avec gestion de la cohérence cache et nouvelles mémoires | Plate-forme | T0+24 |  |  | TPT |
| D1.3 | Plate-forme Gem5 avec exécution sécurisée | Plate-forme | T0+36 |  |  | TPT |
| D2.1 | Détection des vulnérabilités et attaque sur le cache | rapport | T0+36 |  |  | CRISTAL |
| D2.2 | Evaluation des contremesures | rapport | T0+42 |  |  | CRISTAL |
| D3.1 | Statistiques d’ évaluation des fuites au niveau du cache | rapport | T0+12 |  |  | SIC |
| D3.2 | Calcul du taux de succès pour différentes conditions | rapport | T0+36 |  |  | SIC |
| D4.1 | Attaque sur le cache par l’accélérateur matériel | rapport | T0+24 |  |  | LHC |
| D4.2 | Sécurité de l’unité de gestion de consommation | rapport | T0+30 |  |  | LHC |
| D4.3 | Extension Trustzone pour un SoC hétérogène | rapport | T0+42 |  |  | LHC |
| D5.1 | Attaque « Rowhammer » sur la plate-forme Gem5 | rapport | T0+24 |  |  | LIRMM |
| D5.2 | Attaque « Cold Boot » sur la plate-forme Gem5 | rapport | T0+30 |  |  | LIRMM |
| D5.3 | Attaque et contremesures sur les mémoires non-volatiles émergentes | rapport | T0+42 |  |  | LIRMM |

\* jalon, rapport, logiciel, prototype, données, …

# Rapport d’avancement

## Objectifs initiaux du projet

Maximum 10 à 20 lignes.

|  |
| --- |
| Le défi technique général de ce projet est d’analyser la sécurité et les vulnérabilités des interactions complexes entre différents composants micro-architecturaux des processeurs, de leurs périphériques et des composants logiciels. Nous prévoyons de résoudre ce problème en utilisant et modifiant l’outil de simulation d'architecture gem5.Un des objectifs est de trouver le compromis optimal entre vitesse et précision de simulation pour évaluer les problèmes de sécurité. Nous prévoyons d'utiliser différents modes pour une même classe de problèmes de sécurité. Nous limiterions notre étude aux SoC basés sur ARM et les SoC basés sur RISC-V.Pour les logiciels, nous limitons notre portée à Linux en tant que système d'exploitation et OPTEE (Open Trusted Execution Environment).Un autre objectif est d’étudier les SoCs hétérogènes intégrant des GPU, FPGA, unités de gestion de cohérence de cache,… Pour rendre les modèles HDL utilisables dans Gem5, nous utiliserons le niveau de transaction modélisation (SystemC TLM II) pour les blocs FPGA. Un autre défi majeur est d'incorporer des modèles d'exécution de confiance (TEE) dans gem5. Nous limitons notre portée à un hyperviseur sécurisé open source OPTEE (OpenTrusted Execution Environment) qui repose sur la technologie ARM Trustzone. Notre ultime défi scientifique est de concilier performance et sécurité. Les vulnérabilités au niveau micro-architecture conduisent à des attaques sur la mémoire cache dont le but est d’augmenter les performances. Nous essaierons donc de trouver un compromis performance/sécurité.  |

## Travaux effectués et résultats atteints sur la période concernée

Maximum 1 page. Travaux et résultats obtenus pendant la période concernée, conformité de l’avancement des travaux avec le plan initialement prévu. Prévision de travaux pour la (les) prochaine(s) période(s).

|  |
| --- |
| …Nous avons apporté la preuve de faisabilité des attaques par analyse temporelle de cache à partir d’un accélérateur matériel en ciblant un logiciel s’exécutant sur un cœur ARM (WP4.1). Sur la plateforme GEM5, nous proposons une méthode pour détecter les miss du cache et une méthode pour evicter une donnée du cache depuis l’IP matérielle. Cette contribution a fait l’objet d’une soumission à la conférence internationale IEEE VLSI-SOC 2021.Nous avons simulé avec GEM5 la réalisation de communication sur un canal dérobé exploitant le composant DVFS de gestion de l’énergie du SoC (WP4.2).Nous prévoyons de travailler durant les deux prochaines années à la proposition de protection contre les attaques internes au SoC à l’interface entre le matériel et le logiciel (WP4.3).  |

## Difficultés rencontrées et solutions

Maximum 10 à 20 lignes. Difficultés éventuelles rencontrées et solutions de remplacement envisagées ex : impasse technique, abandon d’un prestataire, maîtrise des délais, maîtrise des budgets. Faut-il revoir le contenu du projet ? Faut-il revoir le calendrier du projet ?

|  |
| --- |
| * La mutation de Clémentine Maurice de IRISA vers CRISTAL a décalé l’embauche d’un postdoc
* Le transfert budgétaire de IRISA à CRISTAL n’a pas été effectué en mai 2021
* Le PhD de Télécom Paris a été recruté un an après le T0
* Suite au départ du 1er post-doc embauché sur le projet (partie vers un CDI dans le privée), le Lab. H. Curien rencontre d’importantes difficultés pour le recrutement d’un nouveau post-doc du aux contraintes conjointes de la crise sanitaire et des refus d’autorisations à sa ZRR.
 |

## Faits et résultats marquants

En quelques lignes pour chaque fait ou résultat marquant. Cet élément pourrait donner lieu à communication, après accord du coordinateur du projet.

|  |
| --- |
| … |

## Travaux spécifiques aux entreprises (le cas échéant)

Entreprise xxx

Maximum 10 à 20 lignes par entreprise. Pour chaque entreprise du consortium, décrire les activités dans le projet, en se concentrant sur les apports, collaborations et perspectives liés au projet. Préciser notamment les perspectives d’application industrielle ou technologique, de potentiel économique et commercial, d’intégration dans l’activité industrielle, etc.

|  |  |
| --- | --- |
| Entreprise | Secure-IC |
| Rédacteur (nom + adresse mél) |  |
| … |

## Réunions du consortium (projets collaboratifs)

| **Date** | **Lieu** | **Partenaires présents** | **Thème de la réunion** |
| --- | --- | --- | --- |
| 8 octobre 2019 | Paris | tous | plénière |
| 10 décembre 2019 | téléphonique | tous | plénière |
| 11 février 2020 | téléphonique | tous | plénière |
| 31 mars 2020 | virtuel | tous | plénière |
| 27 mai 2020 | virtuel | tous | plénière |
| 25 août 2020 | virtuel | tous | plénière |
| 8 septembre 2020 | virtuel | tous | plénière |
| 29 septembre 2020 | virtuel | tous | technique |
| 18 décembre 2020 | virtuel | tous | plénière |
| 4 mars 2021 | virtuel | tous | plénière |
| 6 Mai 2021 | virtuel | tous | plénière |

## Commentaires libres

Commentaires du coordinateur

Commentaire général à l’appréciation du coordinateur, sur l’état d’avancement du projet, les interactions entre les différents partenaires…

|  |
| --- |
|  |

Commentaires des autres partenaires

Éventuellement, commentaires libres des autres partenaires

|  |
| --- |
| … |

Question(s) posée(s) à l’ANR

Éventuellement, question(s) posée(s) à l’ANR…

|  |
| --- |
| … |

# Valorisation et impact du projet depuis le début

Cette partie rassemble des éléments cumulés depuis le début du projet qui seront suivis tout au long de son avancée, et repris dans son bilan final.

## Publications et communications

Citer les publications résultant du projet en utilisant les normes habituelles du domaine. Si la publication est accessible en ligne, préciser l’adresse. L’ANR encourage, dans le respect des droits des co-auteurs et des éditeurs, à publier les articles résultant des projets qu’elle finance dans l’archive ouverte pluridisciplinaire HAL : <http://hal.archives-ouvertes.fr/>

**Attention** : éviter une inflation artificielle des publications, mentionner uniquement celles qui résultent directement du projet (postérieures à son démarrage, et qui citent le soutien de l’ANR et la référence du projet).

|  |
| --- |
| **Liste des publications multipartenaires (résultant d’un travail mené en commun)** |
| **International** | **Revues à comité de lecture** |  |
| **Ouvrages ou chapitres d’ouvrage** | 1.
 |
| **Communications (conférence)** | 1.
 |
| **France** | **Revues à comité de lecture** | 1.
 |
| **Ouvrages ou chapitres d’ouvrage** | 1.
 |
| **Communications (conférence)** | 1.
 |
| **Actions de diffusion** | **Articles de vulgarisation** | 1.
 |
| **Conférences de vulgarisation** | 1.
 |
| **Autres** | 1.
 |

|  |
| --- |
| **Liste des publications monopartenaires (impliquant un seul partenaire)** |
| **International** | **Revues à comité de lecture** | 1.
 |
| **Ouvrages ou chapitres d’ouvrage** | 1.
 |
| **Communications (conférence)** | 1. Pierre Ayoub, Clémentine Maurice"Reproducing Spectre Attack with gem5: How To Do It Right? “,, 14th European Workshop on Systems Security
2. Loïc France, Maria Mushtaq, Florent Bruguier, David Novo and Pascal Benoit "Vulnerability Assessment of the Rowhammer Attack Using Machine Learning and the gem5 Simulator — Work in Progress" ACM SaT-CPS '21 conference
 |
| **France** | **Revues à comité de lecture** | 1.
 |
| **Ouvrages ou chapitres d’ouvrage** | 1.
 |
| **Communications (conférence)** | 1.
 |
| **Actions de diffusion** | **Articles de vulgarisation** | 1.
 |
| **Conférences de vulgarisation** | 1.
 |
| **Autres** | 1.
 |

## Autres éléments de valorisation

Les éléments de valorisation sont les retombées autres que les publications. On détaillera notamment :

* brevets nationaux et internationaux, licences, et autres éléments de propriété intellectuelle consécutifs au projet.
* logiciels et tout autre prototype
* actions de normalisation
* lancement de produit ou service, nouveau projet, contrat,…
* le développement d’un nouveau partenariat,
* la création d’une plate-forme à la disposition d’une communauté
* création d’entreprise, essaimage, levées de fonds
* autres (ouverture internationale,..).

Ce tableau détaille les brevets nationaux et internationaux, licences, et autres éléments de valorisation consécutifs au projet, du savoir-faire, des retombées diverses en précisant les partenariats éventuels. Voir en particulier celles annoncées dans l’annexe technique.

|  |
| --- |
| **Liste des éléments. Préciser les titres, années et commentaires** |
| **Brevets internationaux obtenus** | 1.
 |
| **Brevet internationaux en cours d’obtention** | 1.
 |
| **Brevets nationaux obtenus** | 1.
 |
| **Brevet nationaux en cours d’obtention** | 1.
 |
| **Licences d’exploitation (obtention / cession)** | 1.
 |
| **Créations d’entreprises ou essaimage** | 1.
 |
| **Nouveaux projets collaboratifs** | 1.
 |
| **Colloques scientifiques** | 1.
 |
| **Autres (préciser)** | 1.
 |

## Pôles de compétitivité (projet labellisés)

Pour les projets labellisés par un ou plusieurs pôles de compétitivité,

Collaboration du projet avec le(s) pôle(s) ayant labellisé

Quelles collaborations y a-t-il eu entre votre projet et le(s) pôle(s) de compétitivité l’ayant labellisé ?

|  |
| --- |
| … |

 Activités financées par le complément de pôle (laboratoires publics uniquement)

Détailler les activités réalisées par les laboratoires publics avec le complément de financement accordé au titre de la labellisation. Préciser notamment les partenaires impliqués et la collaboration menée avec le ou les pôles.

|  |  |
| --- | --- |
| **Montant du complément accordé par l’ANR (pour chaque labo public)** | * Partenaire XXX : xxx €
* Partenaire YYY : yyy €
 |

|  |  |  |
| --- | --- | --- |
| **Type d’action menée** | **Détails**(exemples non limitatifs) | **Dépenses complément de pôle\*** |
| **Actions contribuant à la réflexion stratégique et à la programmation scientifique du pôle** | Ex : Participation aux journées thématiques organisées par le pôle | Xxx : xxy €Yyy : yyy € |
| **Actions de communication scientifique et publique bénéficiant à la notoriété du pôle**  | Ex : colloque de projets | Xxx : xxy €Yyy : yyy € |
| **Développement de la recherche partenariale (recherche de partenaires, frais de gestion du partenariat, ingénierie de projets,...)** | Ex : accord de consortium, frais de formation à la propriété intellectuelle, à la gestion de projets, dépenses relatives au montage du projet | Xxx : xxy €Yyy : yyy € |
| **Valorisation de la recherche et transfert vers le monde industriel**  | Ex : étude de brevetabilité | Xxx : xxy €Yyy : yyy € |

\* Estimation des dépenses imputées sur le complément de financement accordé au titre de la labellisation par un pôle de compétitivité, partenaires publics seulement.

## Personnels recrutés en CDD (hors stagiaires)

Ce tableau dresse le bilan du projet en termes de recrutement de personnels non permanents sur CDD ou assimilé. Renseigner une ligne par personne embauchée sur le projet quand l’embauche a été financée partiellement ou en totalité par l’aide de l’ANR et quand la contribution au projet a été d’une durée au moins égale à 3 mois, tous contrats confondus, l’aide de l’ANR pouvant ne représenter qu’une partie de la rémunération de la personne sur la durée de sa participation au projet.

Les stagiaires bénéficiant d’une convention de stage avec un établissement d’enseignement ne doivent pas être mentionnés.

Des données complémentaires sur le devenir professionnel des personnes concernées seront demandées à la fin du projet. Elles pourront faire l’objet d’un suivi jusqu’à 5 ans après la fin du projet.

|  |  |  |
| --- | --- | --- |
| **Identification** | **Avant le recrutement sur le projet** | **Recrutement sur le projet** |
| Nom et prénom | SexeH/F | Adresse email (1) | Date des dernières nouvelles | Dernier diplôme obtenu au moment du recrutement | Lieu d'études (France, UE, hors UE) | Expérience prof. antérieure (ans) | Partenaire ayant embauché la personne | Poste dans le projet (2) | Date de recrutement  | Durée missions (mois) (3) |
| Benhani Mehdi | H | benhani.elmehdi@gmail.com | 12/03/2021 | Doctorat UJM | Saint-Etienne, France | 4 | Lab. H. Curien | Post-doc | 01/07/2020 | 7 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Aide pour le remplissage

**(1) Adresse email**: indiquer une adresse email la plus pérenne possible

**(2) Poste dans le projet** : post-doc, doctorant, ingénieur ou niveau ingénieur, technicien, vacataire, autre (préciser)

**(3) Durée missions** : indiquer en mois la durée totale des missions (y compris celles non financées par l’ANR) effectuées ou prévues sur le projet

Les informations personnelles recueillies feront l’objet d’un traitement de données informatisées pour les seuls besoins de l’étude anonymisée sur le devenir professionnel des personnes recrutées sur les projets ANR. Elles ne feront l’objet d’aucune cession et seront conservées par l'ANR pendant une durée maximale de 5 ans après la fin du projet concerné. Conformément à la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'Informatique, aux Fichiers et aux Libertés, les personnes concernées disposent d'un droit d'accès, de rectification et de suppression des données personnelles les concernant. Les personnes concernées seront informées directement de ce droit lorsque leurs coordonnées sont renseignées. Elles peuvent exercer ce droit en s'adressant l'ANR (http://www.agence-nationale-recherche.fr/Contact).

## État financier

Donner un état indicatif de la consommation des crédits par les partenaires. Indiquer la conformité par rapport aux prévisions et expliquer les écarts significatifs éventuels.

|  |  |  |
| --- | --- | --- |
| **Nom du partenaire** | **Crédits****consommés****(en %)** | **Commentaire éventuel** |
|  Lab. H. Curien – Université Jean Monnet | 29 % | Petit retard sur la consommation du budget en ressources humaines, mais un recrutement est en cours |
|  |  |  |
|  |  |  |

# Annexes éventuelles