Journée thématique GDR SoC2 et GDR sécurité informatique :

# Sécurité matérielle et calcul en mémoire

**Date** : 12 octobre 2022

**Lieu :** Laboratoire LIP6, Paris Sorbonne Université, Paris, France

---

**Organisateurs :**

- Romain Wacquez (CEA Leti, Mines Saint-Etienne, Gardanne)
- Cédric Marchand (École Centrale de Lyon – INL)

## Contexte :

Les architectures de calcul en mémoire ou proche mémoire occupent un intérêt croissant dans la conception de systèmes afin de proposer des alternatives aux architectures de Von-Neumann. En effet, ces dernières ont l'inconvénient de créer un goulot d'étranglement entre la partie mémoire et la partie calcul dans les systèmes de traitement de l'information. Si l'on prend en compte l'utilisations en forte croissance de l'internet des objets et de l'intelligence artificielle, le nombre de données collectées est aujourd'hui très important et continue d'augmenter. Cela implique la nécessité de trouver de nouvelles solutions afin d'améliorer l'efficacité des futures architectures de calcul.

Si les données ne sortent pas ou très peu de la mémoire afin que certains calculs soient effectués dessus, la question de la sécurité des ces données se pose. De même, on peut se demander qu'elles sont les opportunités, les forces et les faiblesses de ce type d'architectures pour des fonctions de bases de sécurité (cryptographique, fonctions physique non-clonale et générateurs de nombres aléatoires notamment). On pourra aussi solliciter les propriétés spécifiques des mémoires microélectroniques émergentes pour la spécification et la sécurisation de ces nouvelles architectures.

Le but de cette journée est d'échanger sur la mise en place de fonctions liées à la sécurité matérielle des systèmes de calcul dans ou proche de la mémoire mais aussi de faire le point sur la sécurité de telle mécanisme du point de vue matériel.

## Programme (provisoire) :

| | |
|---|---|
| 09 :30 – 10 :00 | Accueil |
| 10 :00 – 10 :45 | Jean-Philippe Noël → Implémentation cryptographique in memory avec SRAM |
| 10 :45 – 11 :00 | pause café |
| 11 :00 – 11 :30 | Nathan Roussel → Implémentation cryptographique avec STT-MRAM |
| 11 :30 – 12 :15 | Cédric Marchand → Transistor Ferroélectrique et implémentation cryptographique |
| 12 :15 – 14 :00 | Repas |
| 14 :00 – 14 :45 | Raphaël Viera → *caractérisation de la sécurité sur mémoire flash* |
| 14 :45 – 15 :30 | *Giorgio Di Natale → Difficultés avec la sécurité et l'approche calcul en mémoire* |
| 15 :30 – 16 :00 | Discussion et fin (pause café) |

Les présentations (slides) de la journée qui sont publiques sont disponible sur la page internet de l'événement : https://gdr-securite.irisa.fr/journee-thematique-gt-ssm-securite-materielle-et-calcul-en-memoire/

## Participants :

La journée a rencontré un certain succès au près de la communauté travail sur les architectures de calcul en mémoire avec un peu plus de trente d'inscriptions. Environ la moitié des personnes inscrites ont pu finalement faire le déplacement à Paris. En revanche, personne n'ayant demandé d'accès à distance, aucun moyen hybride n'a été mis en place.

**Nombre d'inscrits :** 36

**Nombre de participants :** 17

| Nom | Prénom | Affiliation |
|---|---|---|
| Ammoura | Lila | lirmm |
| Catinaud | Margot | Université Paris Saclay |
| Charrat | Bruno | CEA |
| Courousse | Damien | CEA |
| Di Natale | Giorgio | TIMA |
| Ducousso | Rieul | LIP6 |
| Flottes | Marie-Lise | LIRMM |
| Georget | Lucas | Stagiaire cybersécurité chez EDF |
| HEYDEMANN | Karine | Sorbonne Université |
| Kühne | Ulrich | Télécom Paris, Institut polytechnique de Paris |
| Marchand | Cédric | Ecole centrale de Lyon, INL |
| Noel | Jean-Philippe | CEA |
| Roussel | Nathan | Mines Saint-Etienne |
| Stratigopoulos | Haralampos | Sorbonne Université, CNRS, LIP6 |
| Valea | Emanuele | CEA-LIST |
| VIERA | Raphael | Mines-Saint Etienne |
| Wacquez | Romain | CEA Leti |

## Bilan de la journée :

Lors de cette journée, les échanges entre les orateurs et les participants ont été très riches et intéressants. Il y a eu beaucoup de questions pour chaque présentation et les pauses café et le repas ont permis d'aller plus loin dans les discussions. Le retour général des participants a été très positif et ils ont trouvés l'ensembles des présentations très intéressantes. Ils espèrent que d'autres journées en présentiel seront organisées.

La journée a mis en évidence que la sécurité des architectures de calcul en mémoire est un sujet encore très émergent avec beaucoup plus de questions que de certitudes, notamment autour des technologies émergentes qui ne sont pas nécessairement plus robuste que les technologies conventionnelles.