Université Gustave Eiffel

Offre de Stage M2

Optimisation et implémentation GPU de preuves à divulgation nulle de connaissance post-quantiques (ZK-STARKs)

Mots-clés : Cryptographie, Protection de la vie privée, ZKP, GPU, Parallélisme

Organisme d'accueil : Laboratoire COSYS-ERENA, Université Gustave Eiffel, Bordeaux, France

Encadrants :
- Frédéric Chatrie (frederic.chatrie@junia.com)
- Hasnaa Aniss (hasnaa.aniss@univ-eiffel.fr)

Profil attendu :
- Étudiant·e en Master 2 ou école d'ingénieur, filière informatique/maths appliquées
- Compétences souhaitées :
    - Bonnes bases en cryptographie ou forte motivation pour apprendre.
    - Maîtrise de la programmation C++/Rust et intérêt pour le GPU (CUDA/OpenCL).
    - Curiosité scientifique, capacité d'analyse et goût pour la recherche appliquée.
    - Maîtrise de l'anglais (oral et écrit).
- Un intérêt pour la sécurité post-quantique, le calcul parallèle ou les systèmes distribués est un plus.

Informations complémentaires :
- Durée : 5 à 6 mois
- Démarrage : Printemps 2026 (flexible)

Contexte

La protection de la vie privée est devenue un enjeu majeur dans un monde où la donnée est au cœur des applications numériques. Les preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs, ZKP) permettent de prouver la validité d'une information sans en révéler le contenu et s'imposent comme une technologie clé pour la sécurité et la confiance numérique.

Parmi elles, les ZK-STARKs [1] offrent des garanties de sécurité post-quantique et une bonne scalabilité, mais leur génération et vérification restent très coûteuses en calcul. Ce verrou constitue aujourd'hui un frein majeur à leur adoption à grande échelle dans des domaines comme l'intelligence artificielle, la finance, la santé ou le transport.

L'un des leviers les plus prometteurs pour franchir ce cap est l'accélération sur GPU avec des travaux tels que [2] ou BatchZK [3]. Leur capacité de parallélisation massive ouvre la voie à de nouvelles stratégies d'optimisation, notamment via le batching intelligent, permettant d'exécuter efficacement un grand nombre de preuves en parallèle.

Dans ce cadre, une première étape a déjà été franchie au laboratoire ERENA : l'implémentation GPU de briques fondamentales (hash, arbres de Merkle), en s'appuyant sur la bibliothèque de référence Winterfell. L'objectif du présent stage est d'aller plus loin, en implémentant les autres composantes de la chaîne STARK (FRI, trace, commitment, etc.), d'explorer des techniques d'optimisation avancées et de tendre vers une implémentation complète de bout en bout.

Ce stage constitue une opportunité unique d'acquérir une double expertise en cryptographie avancée et en programmation parallèle sur GPU, deux domaines en forte demande dans le monde

académique et industriel. Les résultats visent une publication scientifique, avec la possibilité éventuelle de poursuivre en thèse.

Missions

Le ou la stagiaire sera pleinement intégré·e au projet de recherche et aura pour missions principales :

1. Analyse et montée en compétence : 1) Étudier en profondeur les mécanismes des ZKP et en particulier les ZK-STARKs (FRI, trace, etc.) ; 2) S'approprier le code existant et comprendre les implémentations de référence (Winterfell) ; 3) Se former aux architectures GPU et aux modèles de programmation parallèle (CUDA/OpenCL).
2. Implémentation GPU : 1) Développer de nouvelles briques STARK (FRI, génération de trace, commitment) ; 2) Optimiser les briques existantes (hash, Merkle) en termes de mémoire et de calcul ; 3) Intégrer progressivement les différentes composantes vers une implémentation de bout en bout.
3. Optimisation et batching intelligent : 1) Explorer des stratégies de regroupement (batching) pour améliorer le débit de génération et de vérification de preuves ; 2) Concevoir des algorithmes d'ordonnancement optimisés conciliant latence et scalabilité.
4. Validation et évaluation : 1) Mettre en place un banc d'essai (Proof-of-Concept) pour tester différents scénarios (charge massive, temps réel) ; 2) Évaluer les performances selon plusieurs critères (latence, débit, scalabilité GPU) ; 3) Identifier les limites et proposer des pistes d'amélioration.
5. Valorisation scientifique : 1) Documenter l'architecture et les résultats obtenus ; 2) Contribuer à la conception d'un code propre et réutilisable ; 3) Préparer une publication scientifique en collaboration avec les encadrants.

Références

[1] https://www.cyfrin.io/blog/a-full-comparison-what-are-zk-snarks-and-zk-starks

[2] Ni, N., & Zhu, Y. (2023). Enabling zero knowledge proof by accelerating zk-SNARK kernels on GPU. *Journal of Parallel and Distributed Computing*, *173*, 20-31.

[3] Lu, T., Chen, Y., Wang, Z., Wang, X., Chen, W., & Zhang, J. (2025, March). BatchZK: A Fully Pipelined GPU-Accelerated System for Batch Generation of Zero-Knowledge Proofs. In *Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 1* (pp. 100-115).