Intership proposal

Proposed modifications to a processor architecture to improve its security and encryption performance

Application to classical and post-quantum encryption on a RISC-V target

The aim of this project is to propose different approaches for extending a generic processor architecture (GP-CPU) in order to improve its level of security and performance.
During this intership, the student will study already some existing GP-CPU performance, in particular by proposing dedicated instruction kits for error-correction codes. This type of kit has shown that for a RISC-V architecture, it is possible to obtain a significant improvement in performance (i.e. latency, throughput, power consumption, memory cost) for a minimal hardware overhead. The proximity of error-correctorection codes to certain encryption algorithms opens the door to the use of such dedicated kits.

Initially, the work will involve acquiring a minimum knowledge of existing kits and their implementation in the context of an open-source RISC-V architecture.

Subsequently, a selection of classical and post-quantum encryption algorithms will be made in consultation with the supervisor. The performance of these codes will have to be precisely evaluated in order to determine the most relevant candidate operations for inclusion in the new kit.

Finally, the trainee will propose a strategy for integrating this instructions kit into a RISC-V core (e.g. ISA extension), and will study the impact of this kit on the encryption performance of the final architecture.

Nota bene: mastery of the RISC-V design flow is a prerequisite, so (if needed) the trainee will need to take some training at the start of the intership.

Project scheduling

- Study and familiarization with RISC-V architecture
- Bibliographical research on encryption techniques, in particular post-quantum encryption and proposal of comparison metrics
- Performance analysis of these algorithms according to the selected metrics
- Code analysis to extract "candidate instructions" for the kit
- Test campaign and analysis of results

Contact

CHAVET Cyrille
Maître de Conférences – Associate professor
TIMA
Tel. : (+33)4-76-57-49-88
Mail : cyrille.chavet@univ-grenoble-alpes.fr

Proposition de stage PFE

Proposition de modifications d'une architecture de processeur pour en améliorer la sécurité et les performances de chiffrement

Application à des chiffrements classiques et post-quantiques sur cible RISC-V

L'objectif de ce projets est de proposer différentes approches pour améliorer/étendre une architecture de processeur générique (GP-CPU) pour en améliorer le niveau de sécurité et les performances.
Des travaux existent déjà concernant l'amélioration des performances de GP-CPU, via notamment la proposition de kits d'instructions dédiées pour des codes correcteurs d'erreurs. Ce type de kits a montré que pour une architecture RISC-V, il est possible d'obtenir une amélioration importante des performances (*i.e.* latence, débits, consommation, coût mémoire) pour un surcoût matériel minime. La proximité des codes correcteurs avec certains algorithmes de chiffrement ouvre la porte à l'utilisation de kits dédiés pour ces derniers.

Les travaux consisteront dans un premier temps, à acquérir les connaissances minimales concernant les kits existants et leur mise en œuvre dans le cadre d'une architecture open-source RISC-V.

Par la suite, une sélection d'algorithmes de chiffrement classique et post-quantiques, sera effectuée en concertation avec l'encadrant. Les performances de ces codes devront être évaluées précisément pour déterminer les opérations candidates les plus pertinentes pour intégrer le nouveau kit.

Enfin, le stagiaire proposera une stratégie pour intégrer ce kit d'instructions dans un coeur RISC-V (*e.g.* extension de l'ISA), et pourra ainsi étudier l'impact de ce kit sur les performances de chiffrement de l'architecture finale.

Nota bene : la maîtrise du flot de conception RISC-V étant nécessaire il faudra, si besoin, que le stagiaire se forme en début de stage.

Déroulement du projet :

- Etude et prise en main d'une architecture RISC-V
- Recherche de bibliographique des techniques de chiffrement et en particulier des chiffrement post-quantiques et proposition de métriques de comparaison
- Analyse de performances de ces algorithmes selon les métriques sélectionnées
- Analyse des codes pour en extraire les « instructions candidates »
- Campagne de test et analyse des résultats

Contact

CHAVET Cyrille
Maître de Conférences
TIMA
Tel. : (+33)4-76-57-49-88
Mail : cyrille.chavet@univ-grenoble-alpes.fr