DE LA RECHERCHE À L'INDUSTRIE

www.cea.fr

Stage n° 3 du LCE : Accélération matériel pour la cryptographie homomorphe

Le Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA) est un acteur majeur en matière de recherche, de développement et d'innovation. Cet organisme de recherche technologique intervient dans trois grands domaines : l'énergie, les technologies pour l'information et la santé et la défense. Reconnu comme un expert dans ses domaines de compétences, le CEA est pleinement inséré dans l'espace européen de la recherche et exerce une présence croissante au niveau international. Situé en île de France sud (Saclay), le Laboratoire d'Intégration des Systèmes et des Technologies (LIST) a notamment pour mission de contribuer au transfert de technologies et de favoriser l'innovation dans le domaine des systèmes embarqués.

La sécurité dans les systèmes embarqués est aujourd'hui un enjeu de premier ordre qui requiert des avancées théoriques majeures. En 2009, un premier crypto-système capable de faire des calculs sur des informations chiffrées sans avoir besoin de les déchiffrer a été réalisé. Ceci constitue encore aujourd'hui une avancée sans précédent pour la cryptographie moderne. Ces systèmes encore appelés homomorphes ouvrent de nombreuses perspectives industrielles et de recherche. Cependant, malgré les progrès récents, de nombreuses limitations demeurent comme le manque de performance ou les besoins en mémoire trop importants. Ainsi, il est nécessaire d'envisager la conception d'accélérateurs matériels pour augmenter le champ d'application de cette nouvelle technologie.

L'objectif de ce stage consiste dans un premier temps à comprendre et à analyser différentes approches algorithmiques qui existent pour permettre le crypto-calcul homomorphe, et de sélectionner celle qui offrira l'accélération matérielle la plus importante. Ensuite, dans un deuxième temps, il faudra proposer une architecture matérielle spécifique capable d'accélérer très significativement les performances obtenues actuellement sur x86. Ce stage constitue une étude originale au niveau international et pourra faire l'objet d'une publication. Le candidat au stage pourra par ailleurs candidater à une thèse pour continuer ces travaux.

Niveau demandé : Master recherche, diplôme ingénieur (BAC+5) – étudiant intéressé pour poursuivre en thèse

Durée : 6 mois

Compétences : VHDL, architecture des calculateurs, synthèse ASIC/FPGA, bonne maîtrise de l'anglais

Pièces à fournir : CV + lettre de motivation + classements

Contact :

Nom : Nicolas Ventroux
Téléphone : 01.69.08.55.43
Email : nicolas.ventroux@cea.fr