Sujet thèse Lab-STICC 2019-2021

Complémentarités des architectures reconfigurables gros grains et des codes correcteurs d'erreurs pour la cryptographie post-quantique

Directeur de thèse : Pr. Philippe Coussy (Lab-STICC, UMR CNRS 6285)

Mots clés :
Cryptographie post-quantique, conception d'architectures sécurisées, architectures reconfigurables gros grains, optimisations de performances (mémoires, temps de traitement…), outils d'exploration automatique.

Sujet de thèse :
Le sujet que nous souhaitons explorer dans le cadre de cette thèse se trouve à la croisée de travaux menés depuis plusieurs années par les membres du laboratoire dans les domaines : des architectures sécurisées pour la cryptographie, les architectures avancées (type CGRA-*Coarse Grain Reconfigurable Architecture*) et les codes correcteurs d'erreurs.
En effet, l'objectif de cette thèse est de proposer un nouveau modèle de composant CGRA capable de transposer les excellentes performances de ces architectures (les CGRA) au monde des codes correcteurs et en particulier aux familles de codes dédiés au chiffrement post-quantique.

Comme la cryptographie à laquelle elles sont souvent associés, les architectures de sécurité constituent une brique de base indispensable à tout composants spécifiques qui vise à assurer un haut niveau de sécurité. Le principal défi des travaux de cette thèse est ainsi de mettre au point un composant capable de maintenir les excellentes performances des CGRAs dans un nouveau champ applicatif-*pour ce type d'architectures*.

Ainsi dans le cadre de cette thèse, il faudra mettre au point une architecture innovante capable de faire des traitements poussés, dans une enveloppe de puissance minimale, tout en étant capable de <u>bien</u> faire du chiffrement, et en l'espèce pour des algorithmes de chiffrements post-quantiques.

Pour ces derniers, plusieurs approches théoriques ont été proposées et font l'objet de nombreuses études par les experts du domaine : cryptographie basée sur des codes correcteurs d'erreurs, cryptographie à base de réseaux euclidiens, cryptographie multivariée… Le problème de toutes ces approches est que la taille des clés, la taille du chiffré et les temps de calculs sont énormes comparativement à ce que l'on peut obtenir avec un RSA, pour un même niveau de sécurité, ou avec des approches de chiffrement par courbes elliptiques (facteurs multiplicatifs de 10^2 à 10^6).
En conséquence, partie importante du travail de thèse sera de suivre, d'étudier et d'analyser les performances des différents modèles retenus dans la compétition organisée par le NIST (National Institute of Standards and Technology)[1].
Pour répondre à ces problèmes, le doctorant pourra notamment s'appuyer sur l'expérience accumulée dans le domaine des architectures sécurisés (avec l'expertise de Arnaud Tisserand, DR CNRS) et des architectures reconfigurables gros grains (ou CGRA pour Coarse Grain Reconfigurable Architecture) qui font l'objet de recherches approfondies au sein du laboratoire. Un CGRA est un modèle d'architecture, intégrant de multiple éléments de calcul basiques, capable d'atteindre des niveaux de performances largement au-dessus de l'état de l'art : accélération des calculs couplée à une minimisation de la consommation énergétique. Ces travaux sur les CGRA se déroulent dans le cadre d'une collaboration internationale avec l'Université de Bologne, Italie (Pr. Luca Benini). Les différents travaux dans ce domaine ont donné lieux à de nombreuses publications en collaboration (ASP-DAC 2017, Trans. On CAD 2018, DATE 2019…).
Toutefois, malgré les nombreux cas d'études ayant fait l'objet d'expérimentations, les code-correcteurs d'erreurs (ou ECC, pour Error Correcting Codes) n'ont pas été traités à ce jour. Ces codes sont à la base de tous les standards de communication numériques (GSM, DVB, EDGE, UMTS, LTE-4G, LTE-5G…). Or, il se trouve que ces mêmes code-correcteurs constituent un autre des domaines d'expertise de notre équipe. Si l'on s'en réfère seulement au dernières années, nos travaux ont débouchés sur plusieurs publications de niveau international : livre (eds. Springer 2015), revue (IEEE Trans. on SP 2013), brevets et dans les meilleurs conférences (ICASSP, DATE, ISCAS…)

[1] Un algorithme de chiffrement post-quantique est un algorithme de capable de résister à une tentative de décryptage par un ordinateur « quantique » ; à la différence des algorithmes actuels (RSA, AES, SHA, ECDH…) qui eux seraient « cassés » en quelques minutes. Même si à l'heure actuelle, l'arrivée à court terme d'une telle sur le marché est peu probable, les plus grandes agences mondiales (NIST, ETSI, ANSSI) se sont lancées dans la recherche d'algorithmes de chiffrement résistants.

Concernant les cas d'études, cette thèse s'appuiera sur l'implantation de codes de chiffrement post-quantique identifiés comme prometteurs dans le cadre des derniers rounds du processus de normalisation du NIST [1]. Plusieurs algorithmes ont été identifiés comme pouvant être pertinent dans le cadre des travaux envisagés : LEDAcrypt [2][3], RQC [4] et QC-MDPC [5] basés sur des codes correcteurs ; EMBLEM [6], Titanium [7] et NTRU Prime [8] basés sur des matrices euclidiennes ; GeMSS [9] basé sur l'approche multivariée pour faire de la signature. Le doctorant devra suivre les dernières évolutions de cette compétition pour déterminer les meilleurs cas d'études, les implanter et mesurer les performances du système vis-à-vis de l'état de l'art.

Quelques références :

[1] https://www.safecrypto.eu/pqclounge

[2] M. BALDI, A. BARENGHI, F. CHIARALUCE, G. PELOSI, P. SANTINI, "*LEDApkc key encapsulation module, a post-quantum asymmetric cryptoscheme relying on Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes*"

[3] M. BALDI, A. BARENGHI, F. CHIARALUCE, G. PELOSI, P. SANTINI, "*LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes*"

[4] C. A. MELCHOR, N. ARAGON, S. BETTAIEB, L. BIDOUX, O. BLAZY, J.-C. DENEUVILLE, P. GABORIT, G. ZÉMOR, "*Rank Quasi-cyclic codes*"

[5] A. YAMADA, E. EATON, K. KALACH, P. LAFRANCE, A. PARENT, "*Quasi-Cyclic Moderate Density Parity-Check*"

[6] M. SEO, J. H. PARK, D. H. LEE, S., KIM, S.-J. LEE, "*Error-blocked Multi-Bit LWE based KEM*"

[7] R. STEINFELD, A. SAKZAD, R. K. ZHAO, "*Titanium: Post-Quantum Public-key Encryption and KEM Algorithms*"

[8] D. J. BERNSTEIN, C. CHUENGSATIANSUP, T. LANGE, C. VAN VREDENDAAL, "*NTRU prime*"

[9] A. CASANOVA, J. C. FAUGÈRE, G. MACARIO-RAT, J. PATARIN, L. PERRET, J. RYCKEGHEM, "*GeMSS: Multivariate Quadratic signature*"

[10] D. J. BERNSTEIN, J. FRIED, N. HENINGER, P. LOU, L. VALENTA, "*Post-Quantum RSA Encryption*"

Encadrement de la thèse et contacts

Directeur de thèse : Pr. Philippe Coussy (Lab-STICC, UMR CNRS 6285)
Co-Encadrant : Dr. Cyrille Chavet (Lab-STICC, UMR CNRS 6285)

Contacts :

Pr. Philippe Coussy (directeur de thèse)
eMail : PHILIPPE.COUSSY@UNIV-UBS.FR
Tel. pro. : 02.9787.45.65

Dr. Cyrille Chavet (encadrant)
eMail : CYRILLE.CHAVET@UNIV-UBS.FR
Tel. pro. : 02.9787.45.67

Procédure de candidature (impérative)

Date limite de candidature : 28 mai 2019 à minuit

Contactez par email : philippe.coussy@univ-ubs.fr et cyrille.chavet@univ-ubs.fr
avec les pièces suivantes (PDF uniquement)

- un CV détaillé
- une lettre de motivation

Les candidat(e)s retenu(e)s pour la pré-sélection seront invité(e)s à participer à une évaluation scientifique et technique sur place (ou en visio-conférence si besoin).

La sélection finale sera effectuée par les financeurs fin mai.