THALES

Thales Communications & Security, CRISTAL, Gennevilliers (92)

Propositions de Stage 2018

Ce document comporte 1 sujets de stage.

Présent dans 56 pays et employant 69.000 collaborateurs, THALES est leader mondial des systèmes d'information critiques sur les marchés de l'aéronautique et de l'espace, de la défense et de la sécurité. Le laboratoire Chiffre est en charge de l'intégration des mécanismes cryptographiques dans les systèmes et équipements THALES.

Les stages proposés débuteront vers avril 2018 et se dérouleront sur une période de 6 mois sur le site de CRISTAL, Thales Communications & Security à Gennevilliers, au sein du laboratoire chiffre LCH.

Le profil recherché est celui d'étudiant motivé par le travail au sein d'une équipe de R&D dans un grand groupe, avec de bonnes compétences en mathématiques complétées par des compétences en programmation.

La rémunération mensuelle est, à titre indicatif, d'environ 1250 euros brut. Toute candidature devra être faite par email en transmettant au format pdf:

- Un CV indiquant les mentions obtenues pour les diplômes
- Une lettre de motivation en rapport avec le(s) sujet(s) visé(s)

Lors de l'entretien, *le candidat devra avoir lu les articles mis en référence* dans le sujet de stage. Il devra être capable de répondre aux questions de compréhension posées sur le sujet du stage.

Amélioration d'un schéma de signature post-quantique

Type de stage : Recherche et développement

Contact :`thomas.prest@thalesgroup.com` et `olivier.bernard2@thalesgroup.com`.

Contexte

En raison de la menace croissante que représentent les ordinateurs quantiques pour la cryptographie à clef publique actuellement déployée, des efforts de standardisation de cryptographie dite "post-quantique" ont été lancés, le plus notable étant l'appel à propositions du NIST [NIST16].

Avec d'autres partenaires (IBM, IRISA, etc.), Thales compte soumettre un schéma de signature basé sur les réseaux euclidiens : Falcon [Falcon17]. Le but de ce stage est l'amélioration au sens large de ce schéma. En particulier, deux techniques algorithmiques y sont utilisées, et liées à :

- la résolution d'équation du type $fG - gF = 1 \bmod \phi$ où f, g, ϕ sont donnés en entrée et $f, g, F, G, \phi \in \mathbb{Z}[x]$ [HGGPW03].
- l'utilisation de samplers Gaussiens sur les réseaux [GPV08, DP16].

La première technique nécessite l'utilisation de très grands entiers. Pour la deuxième, il est fait un usage intensif d'arithmétique en point flottant. Dans les deux cas, cela rend leur mise en oeuvre complexe, notamment sur systèmes embarqués.

Description du stage

Le déroulement du stage s'effectuera comme décrit ci-après :

1. Dans un premier temps, le ou la stagiaire réalisera une étude bibliographique de Falcon et de ses "ancêtres" [HGGPW03, GPV08, DP16].
2. Ensuite, son but sera de développer des algorithmes qui ne souffrent pas des limitations énoncées plus haut, c'est-à-dire :
   (a) un algorithme permettant de résoudre l'équation $fg - gF = 1 \bmod \phi$ sans utiliser de grands entiers ;
   (b) un sampler Gaussien n'utilisant pas de point flottant ;
   (c) de manière générale, toute proposition d'amélioration qui rendrait le schéma plus efficace (en temps et/ou mémoire), plus sûr ou plus simple à implémenter sera prise en considération.

Nous recherchons des candidats possédant de solides compétences en algèbre, en algorithmique et un fort esprit d'initiative. Des notions correctes en probabilités et la maîtrise d'un langage de programmation seront aussi appréciées. Enfin, le candidat devra faire preuve de bonnes capacités de travail en équipe.

Durée des travaux

La durée prévue pour ce stage est 6 mois.

Références

[NIST16] NIST. ≪Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process≫

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardizatio
Call-for-Proposals

[DP16] L. Ducas and T. Prest. ≪Fast Fourier Orthogonalization≫
ISSAC 2016
https://eprint.iacr.org/2015/1014

[Falcon17] The Falcon team ≪Falcon : Fast-Fourier Lattice-based Compact Signatures over NTRU≫
http://www.di.ens.fr/~prest/Publications/falcon.pdf

[GPV08] C. Gentry, C. Peikert and V. Vaikuntanathan ≪Trapdoors for Hard Lattices and New Cryptographic Constructions≫
STOC 2008
https://eprint.iacr.org/2007/432

[HGGPW03] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman and W. Whyte ≪NTRUSign : Digital Signatures Using the NTRU Lattice≫
CR-RSA 2003
www.math.brown.edu/~jpipher/NTRUSign_RSA.pdf