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.

Cryptanalyse de schémas multivariés

Type de stage : Recherche & Développement

Contacts : renaud.dubois@thalesgroup.com, olivier.bernard2@thalesgroup.com et sylvain.lachartre@thalesgroup.com

Contexte

Dans le cadre de l'appel à propositions du NIST pour la standardisation de cryptographie post-quantique, des schémas reposant sur des problèmes basés sur des polynômes multivariés vont être proposés. La difficulté dans la conception de tels cryptosystèmes est de trouver un système central que l'on sache exprimer en terme de polynômes multivariés quadratiques dans lequel on puisse insérer une trapdoor facile à inverser. Plusieurs constructions ont été proposées, qui tombent essentiellement dans deux catégories : les schémas à corps unique tel que le schéma UOV [4], et les schémas à corps mixés tels que C*, HFE, HMFEv-[3], ABC [1]. Une partie du stage consistera à recenser ces propositions, récupérer les implémentations disponibles et les comparer. On étudiera les outils algorithmiques nécessaires à leur implémentation, les voies d'optimisations ainsi que les caractéristiques spécifiques et génériques que l'on pourrait envisager pour le développement d'accélarateurs matériels. Un des principaux outils de cryptanalyse de ces schémas sont les bases de Gröbner [2]. La compréhension des différences d'efficacité de cet outil vis-à-vis des différents schémas est une des voies de recherche de ce stage.

Description du stage

1. Dans un premier temps une étude bibliographique des différents schémas soumis au NIST sera réalisée, ainsi qu'un rassemblement des sources disponibles.
2. Dans un second temps, une analyse de l'implémentation des schémas sera réalisée, ainsi qu'une synthèse sur les performances relatives des différents schémas sur différentes architectures.
3. Dans un dernier temps on retiendra un sous ensemble réduit de schéma afin de réaliser une analyse de sécurité incrémentale de ceux-ci. On réduira tout d'abord le schéma à un exemple jouet, puis on se donnera une succession de dimensionnement sur lesquels on analysera l'efficacité de différents outils de cryptanalyse. Le but de l'analyse est de se donner un modèle du niveau de sécurité de ces schémas et de (in)valider les propositions faites par les concepteurs.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[1] Chengdong Tao et al., Simple Matrix Scheme for Encryption, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013.

[2] J-C. Faugère et A. Joux, Algebraic cryptanalysis of hidden field equation (HFE), CRYPTO 2003.

[3] A. Petzoldt, M. Chen, J. Ding et B. Yang, HMFEv - An Efficient Multivariate Signature Scheme, 8th International Workshop, PQCrypto 2017.

[4] A. Kipnis, J. Patarin, L. Goubin, Unbalanced Oil and Vinegar signature schemes. EUROCRYPT' 99.