THALES

Thales Communications & Security, CRISTAL, Gennevilliers (92)

Propositions de Stage 2018

Ce document comporte 4 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.

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

Sécurisation du Cloud – Mise en œuvre de schémas de recherche sur données chiffrées

Type de stage : Recherche et développement

Contact : emeline.hufschmitt@thalesgroup.com et thomas.ricosset@thalesgroup.com

Contexte

La constante augmentation des débits de connexion et l'apparition sur le marché d'appareils mobiles aux ressources plus limitées que celles d'un ordinateur personnel, engendrent de nouveaux besoins. Après la démocratisation des services de messagerie électronique, l'avènement du *cloud computing* offre de nouvelles perspectives aux utilisateurs comme le partage de médias (documents, musique, vidéos, livres) et d'applications (tableurs, traitement de texte, affichage de documents, requêtes à des bases de données).

L'impulsion du projet Cloudwatt en 2012 visant à doter la France d'une infrastructure de *cloud* souveraine s'explique notamment par les problématiques de sécurité liées à l'hébergement de données sur un serveur distant qui n'est pas nécessairement de confiance. Cependant, la recherche d'un niveau de service plus élevé via l'adaptation de résultats académiques sur la recherche sur données chiffrées à un contexte opérationnel reste aujourd'hui peu répandue.

Un schéma de recherche sur données chiffrées permet à un client de stocker ses données sur un serveur en dehors de son périmètre de confiance tout en conservant la possibilité d'effectuer des recherches sur ces données. La propriété de sécurité que l'on cherche à atteindre est que le serveur distant opère sans découvrir ni les requêtes ni leurs réponses. Des publications récentes ainsi que des travaux internes ont conduit à valider la possibilité de schémas pratiques de recherche sur données chiffrées. La collaboration avec un service de développement logiciel a permis la mise en place d'un framework permettant d'intégrer ces schémas. L'objectif est aujourd'hui de consolider les travaux existants et d'intégrer les schémas de recherches sur données chiffrées au framework.

Description du stage

Ce stage s'articule autours de deux thématiques :

1. une étude bibliographique,
2. une implémentation de schémas.

En s'appuyant sur des travaux internes [D13, RL14, R15, B17], le (la) stagiaire(e) sera amené(e) à réaliser une étude bibliographique des schémas de recherche sur données chiffrées en portant une attention particulière au schéma $\Sigma o\phi o\varsigma$ de Bost [B16] et ses extensions [BMO17]. Selon opportunité, le stagiaire pourra proposer des améliorations de ces schémas. Sur la base de cette étude, nous sélectionnerons certains schémas afin d'en faire un portfolio synthétique présentant leurs différentes caractéristiques (complexités, communications et fonctionnalités). Ceci permettra de décider les schémas à intégrer au framework.

La deuxième partie du stage sera consacrée à l'intégration de schémas au framework existant. Ce travail s'effectuera en synergie forte avec le laboratoire de développement logiciel. L'objectif est à la fois d'intégrer concrètement un (ou des) schéma(s) mais aussi de travailler sur un interfaçage générique permettant l'intégration de futurs schémas. Le développement se fera en langage C/C++.

Le (La) candidat(e) devra avoir de bonnes compétences en cryptographie et algorithmie cryptographique ainsi qu'une forte maîtrise des langages C et C++. Le candidat devra aussi faire preuve de bonnes capacités de travail en équipe.

Durée des travaux

La durée prévue pour ce stage est 6 mois.

Références

[B16] R. Bost
≪$\Sigma o \phi o \varsigma$- Forward Secure Searchable Encryption≫
CCS 2016
2016

[BMO17] R. Bost and B. Minaud and O. Ohrimenko
≪Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives≫
CCS 2017
2017

[D13] B. Dravie
≪Techniques de recherche sur les données chiffrées ≫
Document interne Thales/ Université Paris 13
2013

[RL14] T. Ricosset et M. Latimier
≪Recherche booléenne sur grand volumes de données chiffrées ≫
Document interne Thales/ Université Paris 8/ Université de Rennes 1
2014

[R15] T. Rouxel
≪Recherche sur les données chiffrées dynamiques≫
Document interne Thales/ Université Versailles Saint-Quentin-en-Yvelines
2015

[B17] J.P. Bultel
≪Sécurisation du cloud et schémas de recherche sur données chiffrées≫
Document interne Thales/ Université de Bordeaux
2017

Private Set Intersection

Type de stage : Recherche & Développement
Contacts : ange.martinelli@thalesgroup.com, aurelien.dupin@thalesgroup.com et emeline.hufschmitt@thalesgroup.com

Contexte

Private Set Intersection (PSI) est un outil permettant à deux parties de connaître l'intersection de leurs bases de données respectives, sans partager plus d'information que cette intersection. En particulier les deux parties ne veulent pas transmettre la taille de leur base de données ni permettre à l'autre partie de récupérer des informations sur le contenu de celles-ci. Avec des applications immédiates dans le cadre des réseaux sociaux ou des systèmes de messageries, les algorithmes de PSI sont amenés à manipuler un grand nombre de données que la plupart ne peuvent supporter.

Pour répondre à cette problématique de nombreuses solutions ont été proposées dans la littérature, en tachant de prendre en compte des contraintes à la fois en terme d'efficacité et de sécurité. Les premières solutions utilisaient des protocoles basés sur des chiffrements homomorphes [FNP04] ou d'autres techniques de chiffrement asymétriques. L'article de Huang, Evans et Katz en 2012 marque un tournant dans la recherche à ce sujet [HEK12]. En effet leur article propose une solution basée sur les *garbled circuits* de Yao. Par la suite, toutes les avancées dans le domaine PSI font appel à des primitives cryptographiques complexes : calcul multi-parties, filtres de Bloom, transfert équivoque,... [PSZ14].

L'objectif de ce stage est de prendre en main les techniques cryptographiques sous-jacentes au problème afin de pouvoir faire une comparaison fiables des différentes propositions de la littérature, puis d'en faire une implémentation opérationnelle. Cette implémentation pourra servir de base pour un démonstrateur logiciel. Dans cette optique le stage s'effectue en collaboration avec l'équipe de développement logiciel de Thales Communication & Security.

Description du stage

Ce stage se déroulera en deux partie :

1. une étude bibliographique à la fois des protocoles de PSI et des primitives cryptographiques nécessaire à la compréhension de ceux-ci.,
2. une implémentation d'un schéma choisis par le stagiaire en accord avec ses encadrants.

L'objectif de ce stage est de faire un état de l'art des méthodes de PSI et une études des algorithmes sous-jacents – calcul multi-partie, transfert inconscient,... – avant d'en choisir un, d'étudier sa sécurité en profondeur et de l'implémenter.

Le (La) candidat(e) devra avoir de bonnes compétences en cryptographie et algorithmie cryptographique ainsi qu'une forte maîtrise des langages C et C++. Le candidat devra aussi faire preuve de bonnes capacités de travail en équipe ainsi que d'un esprit d'initiative et sera force de proposition tout au long du stage.

Durée des travaux

La durée prévue pour ce stage est 6 mois.

Références

[FNP04] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas
≪Efficient Private Matching and Set Intersection≫
Eurocrypt 2004
2004

[HEK12] Yan Huang, David Evans, Jonathan Katz
≪Private Set Intersection : Are Garbled Circuits Better than Custom Protocols ?≫
19th Network and Distributed Security Symposium 2012
2012

[PSZ14] Benny Pinkas, Thomas Schneider and Michael Zohner
≪Faster Private Set Intersection Based on OT Extension ≫
USENIX Security Symposium
2014