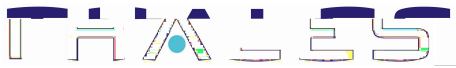

Thales Communications & Security, CRISTAL, Gennevilliers (92)

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 reference* dans le sujet de stage. Il devra être capable de répondre aux questions de compréhension posées sur le sujet du stage.

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