THALES

Laboratoire Chiffre

Propositions de Stages 2019

Gennevilliers, Île-de-France

Rejoignez Thales, leader mondial des technologies de sûreté et de sécurité pour les marchés de l'Aérospatial, du Transport, de la Défense et de la Sécurité. Fort de 64 000 collaborateurs dans 56 pays, le Groupe bénéficie d'une implantation internationale qui lui permet d'agir au plus près de ses clients, partout dans le monde.

Les 14 000 collaborateurs de l'activité Systèmes d'information et de communication sécurisés développent des systèmes de communications militaires et de numérisation de l'espace de bataille, des systèmes de sécurité urbaine, de protection des États et des infrastructures critiques, ainsi que des solutions de cybersécurité.

Le site de Gennevilliers est le cœur des activités de conception, de développement et de soutien des produits et solutions de radiocommunications des armées, des réseaux d'infrastructures résilients et de communications par satellite, ainsi que des solutions de cybersécurité.

Les stages proposés se dérouleront sur une période de 6 mois terminant avant fin septembre 2019, sur le site de Gennevilliers, au sein du laboratoire chiffre (LCH). La rémunération est, à titre indicatif, de 1 250 euros brut mensuel environ. Toute candidature devra être faite par email en transmettant un CV et une lettre de motivation aux contacts indiqués pour chaque sujet.

1 Cryptographie Lightweight

Type de stage : Recherche & Développement

Contacts : emeline.hufschmitt@thalesgroup.com et ange.martinelli@thalesgroup.com

Contexte

Dans le contexte des systèmes médicaux connectés, les piles des appareils de surveillance ne peuvent être changées qu'au prix d'une intervention chirurgicale. Néanmoins, la confidentialité et surtout l'intégrité des informations transmises relèvent de l'importance vitale pour le patient concerné.

Au sein d'une voiture autonome, les informations acquises par les capteurs vidéo doivent être transmises et traitées dans un temps très contraints afin de limiter les risques d'accidents. Or ces informations ne doivent en aucun cas pouvoir être altérées par un tiers et nécessitent donc l'utilisation d'algorithmes cryptographiques.

Le prix unitaire d'une puce sans contact, telles que celles utilisées dans la grande distribution, est proportionnel à la taille de ses composants électroniques. Néanmoins l'information qu'elle transmet doit pouvoir être authentifiée pour des raisons économiques évidentes.

La cryptographie *lightweight* - ou cryptographie bas-coût - est la réponse que les cryptologues offrent à ce type de challenges. En effet l'algorithme de chiffrement AES, standardisé en 2000 par le l'institut de standardisation américain (NIST) et dont la sécurité n'a pas été significativement altérée depuis, n'est pas assez performant pour des systèmes aussi contraints. La cryptographie lightweight est spécifiquement conçue pour fournir un niveau de sécurité adéquat tout en minimisant une ou plusieurs métrique telles que :

- la vitesse d'exécution,
- la taille de l'implémentation,
- la consommation de courant,
- ...

Elle est, par nature, spécifique à un cas d'usage et relaxe certains paramètres de sécurité acceptables selon le contexte afin d'en optimiser le service.

Par ailleurs, ces algorithmes sont voués à être implémentés dans des systèmes embarqués et la menace d'attaques par canaux auxiliaires doit être prise en compte dès la phase de spécification.

Malgré cette spécificité, l'industrie a besoin de standards éprouvés par la communauté scientifique en lesquels avoir confiance. Afin de fournir des standards de haut niveau dans le domaine de la cryptographie lightweight, le NIST a lancé un nouvel appel à candidature pour février 2019. Les algorithmes candidats devront répondre à des contraintes spécifiques et seront évalués par la communauté scientifique dans le but d'en standardiser les plus prometteurs. Ces contraintes ont fait l'objet d'un travail préliminaire et sont recensées dans un document disponible sur la page web dédiée au concours (`https://csrc.nist.gov/Project/Lightweight-Cryptography`).

Description du stage

L'objectif de ce stage est d'étudier l'état de l'art en matière de cryptographie lightweight via une étude poussée des candidats au concours du NIST. En particulier le stagiaire classifiera les algorithmes proposés en fonction des différentes contraintes imposées par le NIST pour déterminer les designs les plus pertinents

en fonction des métriques choisies. Un état de l'art des méthodes de cryptanalyse menées sur ce type d'algorithme sera effectué en parallèle afin de d'éliminer les caractéristiques les plus risquées. Un regard sur les attaques par canaux auxiliaires et la facilité d'implémentation des contremesures à celles-ci sera apprécié. Enfin le stagiaire sera amené à choisir une primitive et à l'implémenter de manière efficace.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[1] D. Dinu, A. Biryukov, J. Großschädl, D. Khovratovich, Y. Le Corre, L. Perrin, FELICS – Fair Evaluation of Lightweight Cryptographic Systems, July 2015, `https://www.cryptolux.org/index.php/FELICS`.

[2] M. Sönmez Turan NIST's Lightweight Crypto Standardization, March 2018, `https://csrc.nist.gov/Presentations/2018/NIST-s-Lightweight-Crypto-Standardization`.

2 Chiffrement homomorphe pour un anonymat post-quantique

Type de stage : Recherche & Développement

Contacts : {aurelien.dupin, melissa.rossi, thomas.ricosset}@thalesgroup.com

Contexte

La sécurité de la cryptographie usuelle repose sur des problèmes mathématiques réputés difficiles à résoudre : trouver un logarithme discret (DLOG), ou décomposer de grands nombres en facteurs premiers (FACT). Toutefois, cette cryptographie est menacée par une percée technologique : l'ordinateur quantique. En effet, les opérations élémentaires des ordinateurs classique et quantique étant de natures différentes, elles rendent ce dernier capable de résoudre efficacement les problèmes DLOG et FACT. Cette menace a fait s'intéresser les chercheurs à des alternatives pouvant lui résister.

L'une de ces alternatives, parmi les plus prometteuses de cette décennie, repose sur des problèmes géométriques d'un objet mathématique connu sous le nom de réseau euclidien. Outre sa potentielle résistance à l'ordinateur quantique, la cryptographie basée sur les réseaux euclidiens ouvre également de nouvelles perspectives en permettant d'effectuer des opérations sur les données chiffrées. Étant donné le chiffré d'une donnée μ, on peut calculer le chiffré de $f(\mu)$ pour toute fonction f, sans avoir à déchiffrer la donnée ou connaitre la clé de déchiffrement. Un schéma de chiffrement ayant cette propriété est appelé complètement homomorphe.

En parallèle de cette menace, les exigences gouvernementales concernant la vie privée et l'anonymat sont de plus en plus fortes en France (CNIL) et en Europe (RGPD/GDPR). Les garantir via la cryptographie nécessite des primitives avancées et peu ou pas de solutions post-quantiques n'existent. Afin de répondre à cette problématique, Thales participe au projet européen PROMETHEUS qui a pour objectif la protection de la vie privée dans un monde post-quantique en fournissant une boîte-à-outils complète de techniques cryptographiques innovantes, résistantes à l'ordinateur quantique et adaptées aux technologies nouvelles.

Objectifs du stage

Lors de ce stage au sein du Laboratoire CHiffre (LCH), le stagiaire sera amené à réaliser une étude bibliographique des schémas de chiffrement homomorphe basés sur les réseaux euclidiens en portant une attention particulière aux schémas de Z. Brakerski, C. Gentry et V. Vainkuntanathan [BGV] introduit à ITCS 2012 et de C. Gentry, A. Sahai et B. Waters [GSW] introduit à CRYPTO 2013 ainsi que leurs évolutions (p. ex. [FV, TFHE]) et à leurs utilisations au sein de protocoles anonymes (p. ex. vote électronique [eVoting]).

Suite à cette étude bibliographique, les travaux porterons, en fonction du profil du stagiaire, sur au moins un des objectifs suivants :

- Analyse de sécurité du protocole retenu en présence d'attaquants malveillants ;
- Implémentation en langage C du schéma homomorphe et/ou du protocole retenus ;
- Optimisations algorithmiques propres au schéma homomorphe et/ou au protocole retenus ;
- Conception d'un nouveau schéma homomorphe mieux adapté au protocole retenu.

Une collaboration du type définition d'un sujet de TER/PFE, suivi du stage, est possible.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Description des travaux

Les tâches à traiter pendant le stage et leurs durées estimées sont les suivantes :
- Lecture et restitution du contenu d'articles scientifiques : 2 mois ;
- Implémentation et/ou recherche de contributions scientifiques : 3 mois ;
- Rédaction du rapport et préparation de la soutenance : 1 mois.

Ce découpage est donné à titre indicatif et sera modifié en fonction de l'avancement des travaux.

Références

[BGV] Z. Brakerski, C. Gentry, V. Vaikuntanathan
(Leveled) Fully Homomorphic Encryption without Bootstrapping
Innovations in Theoretical Computer Science, pages 309-325, 2012

[GSW] C. Gentry, A. Sahai, B. Waters
Homomorphic Encryption from Learning with Errors : Conceptually-Simpler, Asymptotically-Faster, Attribute-Based
Advances in Cryptology – CRYPTO, pages 75-92, 2013

[FV] J. Fan, F. Vercauteren
Somewhat Practical Fully Homomorphic Encryption
Cryptology ePrint Archive, Report 2012/144, 2012

[TFHE] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène
Faster Fully Homomorphic Encryption : Bootstrapping in less than 0.1 Seconds
Advances in Cryptology – ASIACRYPT, partie I, pages 3-33, 2016

[eVoting] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène
A Homomorphic LWE Based E-voting Scheme
Post-Quantum Cryptography, pages 245-265, 2016

3 Développement d'une Blockchain THALES

Type de stage : Développement expérimental

Contacts : renaud.dubois@thalesgroup.com et mickaël.geffrault@thalesgroup.com

Contexte

La blockchain est un mécanisme cryptographique de calcul d'intégrité distribué et décentralisé. Cette technologie permet de développer des usages dans des systèmes dans lequel on souhaite opérer sans autorité de confiance. Elle permet également à un système d'obtenir des ressources (puissance de stockage, de calcul) en échange de récompense (incentive) à des unités (mineurs) qui permettent le fonctionnement du système.

Ce type de mécanisme permet notamment la réalisation de systèmes de monnaie électronique sans autorité centrale, la délégation de bases de donnée, etc. Des applications autres que financières dans le monde défense sont envisagées. Par exemple la DARPA explore la possibilité d'exporter une base de donnée chiffrée dans la blockchain pour sa résistance intrinsèque aux attaques.

Objectifs du stage

- Dans une première partie du stage, le stagiaire se familiarisera avec les mécanismes sous-jacents à la blockchain : preuve de travail et d'enjeux (Pow et PoS) [Na09], consensus, récompenses(incentive) et smartcontracts. Les cas d'usages seront examinés de manière critique [WG17] afin de distinguer les usages qui survivront à l'emballement actuel de ceux qui relèvent de l'opportunisme.
- Dans la seconde partie, des mécanismes propriétaires imaginés par THALES sur les PoS et mécanismes cryptographiques d'un framework existant (ethereum) seront développées par le stagiaire en langage python.

Le profil recherché est celui d'un bon algorithmicien avec des compétences en programmation. Une expérience (stage/TER) de manipulation d'un framework existant (émulation d'une blockchain privée, travail sur les sources) serait fortement appréciée. Une collaboration du type définition d'un sujet de TER/projet fin d'étude suivi du stage est possible.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[Eth] Ethereum
Blockchain app platform
www.ethereum.org

[Na09] S. Nakamoto
A peer-to-peer electronic cash system. 2009

[WG17] K. Wüst and A. Gervais
Do you really need blockchain ?
eprint 2017. report 375