Laboratoire Chiffre (LCH)

Propositions de Stage 2020

Ce document comporte 4 sujets de stage

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.

Les sites de Cholet et Gennevilliers sont au 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 2020, sur le site de Gennevilliers ou Cholet, 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 Développement d'implémentation *threshold* sur un banc DPA

Type de stage : Développement expérimental

Lieu : Gennevilliers, Île-de-France, France

Contacts : {renaud.dubois, valentin.mascre}@thalesgroup.com

Contexte

Les attaques DPA sont une classe d'attaques physiques qui utilisent un canal auxiliaire (consommation de courant, rayonnement électromagnétique) et des outils statistiques pour extraire le secret d'un composant de sécurité. Le service des composants cryptographiques de THALES (SCC), développe des composants qui intègrent des contre-mesures qui préviennent ces attaques. Les implémentations par seuil (*Threshold*) sont une technique de masquage de premier ordre dans laquelle une fonction combinatoire masquée est exprimée de telle sorte que chaque part de la sortie soit indépendante d'au moins une part de l'entrée. La décomposition doit aussi présenter des propriétés d'uniformité [2]. Dans une récente amélioration [3], les auteurs présentent une technique dite *without fresh randomness* qui ne requiert aucun aléa supplémentaire au masquage initial. Cette technique est donc très prometteuse car la génération d'aléa est une contrainte très forte dans le développement de protection anti-DPA.

Objectifs du stage

Le travail réalisé dans le stage sera le suivant :

— dans un premier temps, le stagiaire étudiera les deux articles cités, et réalisera une évaluation de la complexité de leur implémentation,

— dans un second temps, une réalisation d'une version protégée de l'AES conforme à [3] sera réalisée en langage VHDL,

— enfin une évaluation de la résistance de l'implémentation sur le banc de mesure DPA du laboratoire sera faite afin de quantifier le niveau de résistance obtenu. Ce banc requiert de développer des scripts d'attaque en python.

Profil recherché

Le profil recherché est celui d'un étudiant avec une double compétence électroniques/mathématiques : électronicien en dernière année d'école d'ingénieur avec de fortes compétences en mathématiques (discrètes, statistiques), ou étudiant en Master Crypto avec des connaissances en électronique. Une accentuation sur l'un des aspects du stage est possible selon le profil du candidat. La définition d'un projet de fin d'étude type TER préalablement au stage est possible.

Références

[1] P. Kocher, J.Jaffe et B. Jun. Differential Power Analysis. (CRYPTO 1999)

[2] Joan Daemen. Changing of the Guards : A simple and efficient Method for achieving Uniformity in Threshold Sharing. (CHES 2017)

[3] Felix Wegener et AMir Moradi A First-Order SCA Resistant AES without Fresh Randomness. (COSADE 2018)

2 Cryptanalyse quantique d'algorithmes symétriques

Type de stage : État de l'art/Développement expérimental

Lieu : Gennevilliers, Île-de-France, France

Contacts : {zoe.amblard, aurelien.dupin, ange.martinelli}@thalesgroup.com

Contexte

Avec l'arrivée attendue de l'ordinateur quantique, la menace de l'algorithme de Shor impose à la communauté cryptographique de trouver des alternatives à la factorisation ou au logarithme discret. Pour la majorité de la communauté, l'ordinateur quantique se résume à l'algorithme de Shor ou à celui de Grover. Pourtant un ordinateur quantique a de nombreuses capacités encore inexploitées dans le cadre de la cryptanalyse.

Ce sont ces capacités qu'explorent Maria Maya-Placensia *et al.* [KLLNP16, BNP18, BNPS19] dans le cadre de la cryptographie symétrique. Pour cela, ils définissent de nouveaux modèles d'attaquants en fonction de l'accès à un ordinateur quantique, voire à un oracle quantique et montrent que de nombreux modes opératoires sont menacés dans ces modèles.

Par ailleurs, ils s'intéressent aussi à la cryptanalyse d'algorithmes classiques exploitant les particularités d'un ordinateur quantique. Pour mener ces attaques, ils ont acquis une connaissance poussée de l'architecture et des capacités des ordinateurs quantiques qui est unique dans la communauté cryptographique.

Objectifs du stage

L'objectif de ce stage et d'étudier les capacités d'un ordinateur quantique et ses utilisations possibles dans le cadre de cryptanalyse symétrique.

La première partie de ce stage sera donc une étude du fonctionnement d'un ordinateur quantique et ses possibilités [Nan18]. Ensuite une étude bibliographique des attaques quantiques sur des algorithmes symétriques sera effectuée. Enfin une attaque sera choisie et implémentée sur un exemple jouet à l'aide du framework Qiskit [Qis] permettant de manipuler des états quantiques.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[KLLNP16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier et Maria Naya-Placensia. *BreakingSymmetric Cryptosystems using Quantum Period Finding*. CRYPTO 2016

[BNP18] Xavier Bonnetain et Maria Naya-Placensia. *Hidden Shift Quantum Cryptanalysis and Implications*. ASIACRYPT 2018

[BNPS19] Xavier Bonnetain, Maria Naya-Placensia et André Schrottenloher. *Quantum Security Analysis of AES*. TSC 2019

[Nan18] Giacomo Nannicini. *An Introduction to Quantum Computing, Without the Physics*. IBM 2018

[Qis] IBM *Qiskit – An Open-Source Quantum Computing Software Development Framework*, https://qiskit.org.

Schémas de chiffrement complètement homomorphe hybride pour une délégation de calculs efficace

Type de stage : Recherche & Développement

Lieu : Gennevilliers, Île-de-France, France

Contacts : {olivier.bernard2, thomas.ricosset}@thalesgroup.com

Contexte

De nos jours, le nombre d'objets connectés explose, de plus en plus d'objets intelligents avec des capacités de stockage et de calculs limitées apparaissent, externalisant massivement les données collectées à des compagnies monnayant d'importantes ressources de stockage et de calcul, ce qui engendre de nouvelles problématiques quant à la délégation de données sécurisée. L'interêt croissant pour la protection de la vie privée attesté par la CNIL en France et le récent RGPD européen, ainsi que la profusion de données numériques invitent à considérer de nouveaux chiffrements permetant de déléguer des calculs tout en conservant la confidentialité des données.

Le chiffrement complètement homomorphe, rendu possible en 2009 par Gentry [Gen09] donne une réponse théorique au problème. Ce type de chiffrement permet d'effectuer des opérations sur des chiffrés qui correspondent à l'addition et à la multiplication des données correspondantes. Combiner ces deux opérations rend possible de calcul de n'importe quel traitement de données à partir de chiffrés, sans que cela ne révèle la valeurs des données elles-mêmes ni même des résultats au serveur. De nombreux travaux ont permis d'améliorer cette primitive (*e.g.* [BV11, BGV12, GSW13, DM15, CGGI16]), néanmoins l'utilisation seule du chiffrement complètement homomorphe ne permet pas la délégation de calculs efficace à partir d'objets aux ressources limitées [LNV11]. L'utilisation combinée avec un chiffrement symétrique donne un protocole hybride qui peut être mis en oeuvre sur les objets connectés. Différents chiffrements symétriques ont été créés pour ce protocole hybride, tels LowMC [ARSTZ16], Kreyvium [CCFLNP16], FLIP [MJSC16] et Rasta [DEGLLLMR18], avec des démonstrations de faisabilité dans la librairie homomorphe HElib [HS14]. L'objectif est aujourd'hui de comparer ces différents chiffrements symétriques dans le cadre du protocole hybride dans d'autres libraires, avec des schémas de chiffrement complètement homomorphes plus récents, et de considérer l'efficacité dans le cadre d'applications réelles.

Description du stage

Lors de ce stage au sein du Laboratoire CHiffre (LCH) les travaux porteront, en fonction du profil de la ou du stagiaire, sur au moins un des objectifs suivants :

- Implémenter et comparer différents chiffrements symétriques dans une librairie de chiffrement complètement homomorphe implémentant le schéma de [CGGI16].
- Améliorer un schéma de chiffrement symétrique dans le cadre du protocole hybride.
- Evaluer l'efficacité du protocle hybride dans le cadre d'une application réelle, et implémenter dans ce sens.

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

[Gen09] Craig Gentry.
≪Fully homomorphic encryption using ideal lattices.≫
ACM STOC 2009
2009

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan.
≪(Leveled) fully homomorphic encryption without bootstrapping.≫
ITCS 2012
2012

[ARSTZ16] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. ≪Ciphers for MPC and FHE.≫
EUROCRYPT 2015
2015

[BV11] Zvika Brakerski and Vinod Vaikuntanathan.
≪Efficient fully homomorphic encryption from (standard) LWE.≫
FOCS 2011
2011

[CCFLNP16] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey.
≪Stream ciphers : A practical solution for efficient homomorphic-ciphertext compression.≫
FSE 2016
2016

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène.
≪Faster fully homomorphic encryption : Bootstrapping in less than 0.1 seconds.≫
ASIACRYPT 2016
2016

[DEGLLLMR18] Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger.
≪Rasta : A cipher with low anddepth and few ands per bit.≫
CRYPTO 2018
2018

[DM15] Léo Ducas and Daniele Micciancio.
≪FHEW : Bootstrapping homomorphic encryption in less than a second.≫
EUROCRYPT 2016
2015

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters.
≪Homomorphic encryption from learning with errors : Conceptually-simpler, asymptotically-faster,

attribute-based.≫
CRYPTO 2013
2013

[HS14] Shai Halevi and Victor Shoup.
≪Algorithms in HElib.≫
CRYPTO 2014
2014

[MJSC16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet.
≪Towards stream ciphers for efficient FHE with low-noise ciphertexts.≫
EUROCRYPT 2016
2016

[LNV11] Kristin Lauter, Michael Naehrig and Vinod Vaikuntanathan.
≪Can Homomorphic Encryption be Practical ?≫
EPRINT 2011
2011

Implémentation optimisée de schémas de signature post-quantiques

Type de stage : Développement expérimental

Lieu : Cholet, Pays de la Loire, France

Contacts : {sylvain.lachartre, 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 offre de solides garanties de sécurité ainsi que des temps d'exécution compétitifs eu égard aux schémas usuels.

Un chargeur d'amorçage (ou bootloader) intervient au démarrage d'un équipement pour garantir l'intégrité de son système d'exploitation par l'intermédiaire d'une vérification de signature, la signature ayant été générée en amont. La durée de vie d'un tel équipement pouvant être de plusieurs décennies, il est nécessaire de le prémunir contre les attaques futures, en particuliers celles reposant sur la capacité de calcul de l'ordinateur quantique.

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 signature fondés sur les réseaux euclidiens Dilithium [LDKLSSS] et Falcon [PFHKLPRSWZ] en portant une attention particulière à l'implémentation des opérations NTT (pour Number Theoretic Transform) [PG12], une généralisation de la transformée de Fourier discrète permettant de multiplier efficacement des polynômes entre eux, utilisée pour la vérification de signatures.

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

- Implémentation optimisée de la vérification de signatures ;
- Accélération matérielle de la vérification de signatures ;
- Optimisation logicielle de la génération de signatures ;
- Optimisation logicielle de la génération des clés.

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 : 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

[LDKLSSS] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, and D. Stehlé
CRYSTALS-Dilithium
Submission to the NIST Post-Quantum Cryptography Standardization, 2017

[PFHKLPRSWZ] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang
Falcon
Submission to the NIST Post-Quantum Cryptography Standardization, 2017

[PG12] T. Pöppelmann, T. Güneysu
Towards Efficient Arithmetic for Lattice-Based Cryptography on Reconfigurable Hardware
LATINCRYPT 2012