Service Crypto (SCR)

Propositions de Stage 2023

Ce document comporte 3 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 81 000 collaborateurs dans 68 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 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 2023, sur le site de Gennevilliers, au sein du service crypto (SCR). 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 Algorithme d'Euclide en temps constant pour la cryptographie

Type de stage : Recherche & Développement

Lieu : Gennevilliers (92)

Durée : 6 mois

Contacts : {simon.abelard, valentin.vasseur} @thalesgroup.com

Contexte

L'algorithme d'Euclide permet de calculer efficacement des pgcd dans des anneaux euclidiens. Les algorithmes les plus récents bénéficient d'améliorations permettant d'effectuer cette tâche en temps quasi-optimal (i.e. avec une complexité quasi-linéaire en la taille de l'entrée à comparer à une complexité quasi-quadratique pour l'algorithme d'Euclide naïf) et on dispose par ailleurs d'implémentations publiques très efficaces. En cryptologie, l'algorithme d'Euclide revêt une importance particulière pour effectuer des inversions modulaires, une tâche générale qui se retrouve aussi bien dans la cryptographie elliptique traditionnelle (par exemple dans ECDSA) que dans la cryptographie post-quantique (par exemple pour générer des clés dans le schéma BIKE).

Les applications cryptographiques ne peuvent malheureusement pas se satisfaire des implémentations actuelles de l'algorithme d'Euclide car malgré une efficacité certaine, il n'est pas conçu pour que son exécution prenne un temps constant. Cela signifie que l'on s'expose à des *timing attacks*, c'est-à-dire que les variations de temps de calcul peuvent permettre à un attaquant d'en déduire des informations secrètes. Pallier ce défaut est donc un pré-requis incontournable avant d'envisager une utilisation de l'algorithme d'Euclide au sein de primitives cryptographiques.

Récemment, Bernstein et Yang [1] ont proposé une variante de l'algorithme d'Euclide dont l'éxécution est plus finement maîtrisée afin non seulement de gagner en performances mais aussi de résister aux timings attacks. Pour justifier la pertinence de leurs travaux et leur applicabilité en cryptographie, ils ont principalement montré que l'emploi de leur algorithme dans le cadre d'ECDSA et du KEM NTRU permettait un gain de temps par rapport aux solutions usuelles. Dans ces applications, le problème sous-jacent est respectivement l'inversion modulo $p = 2^{255} - 19$ et modulo $P(X) = (X^{701} - 1)/(X - 1)$.

Ce stage se propose d'évaluer la pertinence de cet algorithme dans le cadre de la cryptographie post-quantique et plus spécifiquement du schéma BIKE qui a été sélectionné au Round 4 de la compétition du NIST. Dans ce cas particulier, cela revient à étudier l'inversion dans $\mathbb{F}_2[X]/(X^r - 1)$ avec r de l'ordre de 10000 (de 12323 à 40973 selon le niveau de sécurité). Suivant les résultats obtenus et les intérêts du ou de la stagiaire, il pourra être envisagé d'explorer le cas du schéma CSIDH basé sur les isogénies dans lequel il est nécessaire de calculer des inverses modulo un nombre premier p de la forme $4 \prod p_i - 1$, où les p_i sont tous les nombres premiers inférieurs à une limite (de l'ordre de 600 actuellement).

Enfin, au-delà des problématiques de temps constant, le standard en termes de résistance aux attaques par canaux auxiliaires est de disposer d'une implémentation dite masquée, c'est-à-dire conçue de telle sorte qu'un attaquant ne disposant que d'une seule sonde ne pourra pas obtenir d'information lui permettant de récupérer des éléments secrets. Le masquage n'est pas toujours simple à mettre en œuvre et représente un coût parfois important en termes de performances, a fortiori quand on doit l'appliquer sur des algorithmes qui ne s'y prêtent pas. Il serait donc également très intéressant d'évaluer à quel point ce nouvel algorithme d'inversion modulaire se prête au masquage. Le cas échéant, cela constituerait un argument fort en faveur de son utilisation et pourrait stimuler davantage de recherche et de développements dans cette direction.

Objectifs du stage

Il s'agit dans un premier temps de se familiariser avec les algorithmes standard (notamment à base de demi-pgcd) pour calculer des pgcd en temps quasi-optimal, puis avec l'algorithme de Bernstein et Yang en lui-même. Le ou la stagiaire effectuera des travaux d'implémentation qui lui permettront d'atteindre une plus grande maîtrise de cet algorithme. Cette implémentation (le langage est à déterminer suivant les préférences du ou de la stagiaire) sera la base de travail pour répondre à une ou plusieurs des questions suivantes :

- l'algorithme de Bernstein et Yang est-il aussi performant dans $\mathbb{F}_2[X]/(X^r - 1)$?
- permet-il un gain d'efficacité dans la génération de clés pour BIKE ?
- peut-on lui apporter des améliorations spécifiques aux anneaux de la forme $\mathbb{F}_2[X]/(X^r - 1)$?
- peut-on lui apporter des améliorations spécifiques aux entiers de la forme $p = 4\prod p_i - 1$?
- peut-on envisager une implémentation masquée de cet algorithme ?

Compétences requises

De bons pré-requis en mathématiques et en calcul formel, un goût pour l'algorithmique et la cryptographie. De bonnes capacités d'apprentissage pour développer une maîtrise de concepts parfois abstraits. La maîtrise d'un langage de calcul formel ou de programmation, une appétence pour le développement logiciel. De l'autonomie, la capacité à travailler en équipe et à expliquer ses travaux à un public hétérogène (spécialistes et non-spécialistes).

Références

[1] Bernstein, D. J., Yang, B. Y. Fast constant-time gcd computation and modular inversion. In *IACR transactions on cryptographic hardware and embedded systems*, 340-398, 2019.

2 Signatures post-quantiques fondées sur le MPC-in-the-Head

Type de stage : Recherche & Développement
Lieu : Gennevilliers (92)
Durée : 6 mois
Contacts : {zoe.amblard, aurelien.dupin, thomas.ricosset}@thalesgroup.com

Contexte

La cryptographie post-quantique, qui s'intéresse à des problèmes mathématiques différents du calcul du logarithme discret et de la factorisation de grands nombres, propose de nouveaux algorithmes cryptographiques conçus pour être résistants face à un attaquant disposant d'un ordinateur quantique. Ce domaine de recherche a connu un essort important dans les dernières années, en particulier lors de l'appel à propositions du NIST qui a évalué nombre de ces algorithmes et en a sélectionné certains pour devenir de futurs standards qui seront massivement utilisés dans l'industrie.

L'un des candidats évalués par le NIST, le schéma de signature PICNIC, est basé sur la combinaison d'une preuve à divulgation nulle de connaissance, d'un schéma de chiffrement symétrique et d'une technique de calcul multipartite appelée "MPC-in-the-Head" [IKOS07]. Cette technique a l'originalité de réaliser le calcul d'un circuit (la primitive symétrique) entre plusieurs participants fictifs qui ne vivent que "dans la tête" du prouveur et qui se partagent des parts du secret. Le prouveur parvient à démontrer qu'il connaît ce secret en dévoilant les informations de tous ses participants imaginaires sauf un, et le vérifieur peut s'assurer que cette preuve est valide mais ne peut pas retrouver le secret sans l'information du participant manquant.

Bien qu'extrêmement intéressant et offrant des perspectives de sécurité très robustes, le schéma de signature PICNIC n'a pas été retenu comme standard principalement car il utilisait le schéma de chiffrement symétrique LowMC non standardisé et moins bien étudié qu'un standard comme AES, et à cause de ses performances moins compétitives que d'autres candidats. Cependant, les schémas de signature basés sur le MPC-in-the-Head sont en plein essor avec de nombreuses nouvelles propositions qui utilisent AES et qui améliorant considérablement les performances et tailles de signature. Le NIST ayant décidé d'ouvrir un nouvel appel à propositions pour les signatures post-quantiques en juin 2023, nous pouvons nous attendre à ce que ce domaine de recherche perdure en dynamisme et en popularité avec de nouvelles propositions pour des futurs standards.

Objectifs du stage

Lors de ce stage au sein du Service Crypto (SCR), le ou la stagiaire sera amené.e à étudier de manière approfondie le schéma de signature post-quantique Helium-AES [KZ22], dernier-né dans la lignée des signatures basées sur le MPC-in-the-Head. Ce schéma de signature est construit en combinant le système de preuve Helium, qui a hérité de nombreuses caractéristiques du système de preuve de PICNIC, et la primitive de chiffrement standardisée AES. Le stage sera en particulier axé sur une compréhension fine de la manière dont la primitive AES s'articule avec Helium pour obtenir des signatures courtes et performantes.

Suite à cette étude bibliographique, les travaux porteront sur au moins un des objectifs suivants :

— Analyse des performances en temps, mémoire et taille de signature de l'implémentation d'Helium-AES existante ;
— Identification de différentes pistes d'optimisation de ces performances, par exemple le possible remplacement de la fonction de hachage utilisée SHAKE par une alternative plus adaptée aux caractéristiques d'Helium-AES ;
— Implémentation et évaluation des optimisations retenues.

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

[IKOS07] Yuval Ishai and Eyal Kushilevitz and Rafail Ostrovsky and Amit Sahai
Zero-knowledge from secure multiparty computation
Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007

[KZ22] D. Kales, G. Zaverucha
Efficient Lifting for Shorter Zero-Knowledge Proofs and Post-Quantum Signatures
Cryptology ePrint Archive, Paper 2022/588, 2022

3 Analyse d'une hypothèse de sécurité fondée sur les réseaux euclidiens et ses applications pour la sécurité des schémas cryptographiques post-quantiques

Type de stage : Recherche & Développement

Lieu : Gennevilliers (92) & Paris (75)

Durée : 6 mois

Contacts : {hugo.beguinet, olivier.bernard2, morgane.guerreau}@thalesgroup.com, melissa.rossi@ssi.gouv.fr

Contexte

Les réseaux euclidiens sont une structure mathématique prometteuse pour l'élaboration de schémas cryptographiques asymétriques conjecturés post-quantiques. Les problèmes difficiles sous-jacents conduisent à des fortes garanties en matière de sécurité et leur structure permet aussi de compétitives performances. Plusieurs algorithmes de chiffrement et de signature sont en cours de standardisation par le NIST dont l'algorithme de signature Falcon [PFH+20].

L'analyse et la conception de ces nouveaux schémas restent un domaine relativement récent et de nombreuses améliorations sont régulièrement publiées.

Objectifs du stage

L'objet de ce stage est d'étudier une hypothèse de sécurité fondée sur les réseaux euclidiens : l'isomorphisme de réseaux euclidiens ou LIP (pour « Lattice Isomorphism Problem »). Cette hypothèse avait déjà été introduite dans la littérature (par exemple [HR13]) mais il a été récemment prouvé qu'elle permet d'améliorer grandement le schéma de signature Falcon [DW21, DPPW22]. L'hypothèse LIP n'étant pas valide dans le cas des réseaux idéaux, il semble nécessaire de reposer sur des structures plus complexes.

Suite à l'étude bibliographique des deux dernières références citées, les travaux chercheront à répondre en partie ou totalité aux différentes questions suivantes :

- À quel point cette nouvelle hypothèse s'éloigne-t-elle d'une hypothèse plus standard de réseaux euclidiens ?
- Y a-t-il des cas particuliers de paramètres qui rendent cette hypothèse plus difficile ?
- Quels sont les modèles cryptanalytiques en jeu dans l'analyse de sécurité de la nouvelle signature ?
- Cette nouvelle hypothèse introduit-elle de nouveaux points d'entrée pour des attaques physiques (canaux auxiliaires) sur l'implémentation de la signature ?

Organisation du stage

Ce stage sera d'une durée d'environ 6 mois à cheval sur l'été 2022. Il comprendra une partie de revue de littérature assistée par les encadrant·e·s d'environ un ou deux mois. La suite du stage consistera à étudier les différents aspects évoqués. Ce stage pourra comporter des parties d'implémentation et se concentrer sur les aspects plus pratiques ou théoriques selon les goûts du candidat ou de la candidate. Il pourra aussi donner lieu à une publication scientifique si les résultats s'y prêtent.

Le ou la stagiaire sera amené·e à faire des allers-retours entre le laboratoire de cryptographie de Thales et le laboratoire de cryptographie de l'ANSSI de manière à collaborer avec les encadrant·e·s. La répartition du temps de présence initialement prévue est de 80% dans les locaux de Thales et de 20% dans les locaux de l'ANSSI. Elle pourra faire l'objet d'adaptations mineures au cours du stage.

Références

[PFH+20] T. Prest, P. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang
FALCON
Technical report, National Institute of Standards and Technology, 2020

[HR13] I. Haviv, O. Regev
On the Lattice Isomorphism Problem
arXiv :1311.0366

[DW21] L. Ducas, W. v. Woerden
On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography
Cryptology ePrint Archive, Paper 2021/1332, 2021

[DPPW22] L. Ducas, E. W. Postlethwaite, L. N. Pulles, W. v. Woerden
Hawk : Module LIP makes Lattice Signatures Fast, Compact and Simple
Cryptology ePrint Archive, Paper 2022/1155, 2022