UNIVERSITÉ DE TOULON

Contrat doctoral Etablissement 2022/2025
Formulaire de candidature

Titre de la thèse	Arithmétique modulaire pour la cryptographie à clé publique

Ecole Doctorale	ED548
Laboratoire	IMath
Discipline	Informatique
Directeur(s) de Thèse & Encadrant(s)	Directeur de thèse : Pascal Véron Co-encadrant : Nicolas Méloni

Description du sujet de recherche

(3 pages maximum - contexte scientifique, objectifs, mots clé, références)

Contexte, originalité et pertinence par rapport à l'état de l'art :

La sécurité des communications est devenue un enjeu essentiel des sociétés modernes. Qu'il s'agisse d'enjeux économiques (paiement par internet, sans contact, par téléphone), de vie privée (communication par téléphone, messagerie instantanée, e-mail) ou de sécurité des données (accès et chiffrement des bases de données) la croissance exponentielle des moyens de communication (internet très haut débit, réseau 5G, internet des objet) entraîne un développement du même ordre des besoins d'expertise dans le domaine de la cryptographie. Plus particulièrement, la **cryptographie à clé publique** est l'outil fondamental qui permet de mettre en place un canal de communication sécurisé entre deux entités. Introduit dans les années 1970, il s'agit d'un domaine de recherche extrêmement actif duquel ont émergé les deux standards actuels que sont les protocoles RSA (Rivest-Shamir-Adleman) et ECC (Elliptic Curve Cryptography). Bien que ces deux protocoles soient considérés comme sûrs d'un point de vue théorique, il a été montré à maintes reprises que l'implantation même des différents algorithmes sous-jacents peut être vulnérable à des attaques particulièrement efficaces appelées attaques par canaux auxiliaires (ACA). L'implantation de ces protocoles sur différentes plateformes (ordinateur, smartphone, carte à puce) est ainsi devenu un domaine de recherche à part entière dans lequel l'efficacité et la sécurité des implantations sont toujours mises en balance. À cela est venu s'ajouter les avancées rapides dans le domaine des ordinateurs quantiques qui menacent de mettre à mal la sécurité théorique des protocoles actuels. C'est pour cela que le NIST (National Institute of Standard and Technology) à lancer un appel international pour la mise au point de nouveaux standards cryptographiques dits

post-quantiques censés résister à un ordinateur quantique. Quand bien même, l'implantation de ces nouveaux protocoles sera malgré tout toujours vulnérable aux attaques par canaux auxiliaires.

L'arithmétique modulaire, et en particulier l'arithmétique des corps finis, est la brique essentielle à partir de laquelle sont construits plusieurs protocoles, notamment RSA, ECC et également le protocole post-quantique SIKE. On trouve dans la littérature deux grandes approches concernant l'implantation de cette arithmétique. La première basée sur la représentation des nombres en multi-précision et la seconde consistant à définir un système de représentation non-conventionnel des entiers. Parmi les systèmes possibles, le système de représentation PMNS (Polynomial Modular Number System) proposé en 2005 n'a pas retenu l'attention de la communauté cryptographique malgré ses propriétés originales. Un premier travail débuté en 2016, au sein du laboratoire IMath, a remis au goût du jour ce système en démontrant son efficacité dans le domaine de la cryptographie sur les courbes elliptiques. L'originalité de cette thèse sera d'étudier l'apport d'un tel système pour la cryptographie à clé publique en général où les entiers manipulés sont de taille parfois supérieure à 1000 bits contrairement à ce qui se passe dans le cadre des courbes elliptiques. On s'intéressera de plus à l'apport de ce système pour l'optimisation et la sécurisation des protocoles post-quantiques.

Objectifs :

L'objectif de cette thèse est d'étudier en profondeur un système ayant connu un regain d'intérêt récemment appellé Polynomial Modular Number System (PMNS). De nombreuses questions restent en suspens concernant ce système aussi bien d'un point de vue théorique (concernant l'existence de paramètres optimaux pour un protocole donné) que pratique (concernant l'efficacité et la sécurisation des implantations). Ce travail doit de plus permettre de rendre le système suffisamment versatile pour qu'il puisse s'adapter à la variété des systèmes sur lesquels il pourra être implanté. On s'intéressera en priorité à optimiser le système pour les jeux d'instructions des processeurs de dernières génération permettant un certain parallélisme ainsi qu'aux possibilités offertes par les circuits reprogrammables utilisés dans le domaine de l'informatique embarquée.

Problématique : Un PMNS (Polynomial Modular Number System) est un ensemble $\mathbb{B}$ *C* Z[X] défini par 5 paramètres (p,n,γ,r,E):

- p signifie que l'on souhaite représenter les entiers de Z/pZ.
- n signifie que chaque entier sera représenté par un polynôme $A(X)$ tel que $deg\ (A(X)) < n$.
- γ *signifie que* tout entier a de Z/pZ, est représenté par un polynôme $A(X)$ tel que $A(\gamma) = a \bmod p$.
- r signifie que pour tout $A(X)$, les coefficients de $A(X)$ sont bornés strictement par l'entier r.
- Enfin E est un polynôme de degré n. Toute opération entre les polynômes représentant des entiers sera effectué modulo E(X).

Plus précisément l'ensemble $\mathbb{B}$ est muni de deux lois de composition interne **+** et **x** tel que :

- $A(X) + B(X)$ correspond à l'addition modulo $E(X)$ des polynômes $A(X)$ et $B(X)$.
- $A(X) \times B(X)$ correspond à la multiplication modulo $E(X)$ des polynômes $A(X)$ et $B(X)$.

Ces deux opérations sont suivies d'une étape de **réduction interne** afin d'obtenir à nouveau un résultat dans l'ensemble $\mathbb{B}$. Un élément a de Z/pZ est donc représenté par un polynôme $A(X)$, de degré au plus $n-1$, tel que $A(\gamma) = a \bmod p$, pour un certain couple de paramètres n et γ fixés lors de l'élaboration du système. Ainsi a est représenté par au plus n coefficients. L'arithmétique modulo p est remplacée par une arithmétique dans Z[X]. Afin que le nombre de coefficients n'augmente pas au cours des opérations effectuées, chaque calcul est réalisé modulo un polynôme $E(X)$ de degré n (étape de **réduction externe**). De plus afin de maîtriser la taille des coefficients des polynômes, chaque étape de calcul produisant un polynôme $R(X)$ est suivie d'une réduction interne qui consiste à trouver un polynôme $S(X)$ tel que $S(\gamma)=R(\gamma) \bmod p$ et dont les coefficients sont tous bornés

(en valeur absolue) par le paramètre *r* défini au moment de la construction du système de représentation. Cette étape de réduction interne conditionne fortement les performances du système de représentation. Il existe actuellement deux méthodes permettant de réaliser cette opération : la méthode Montgomery-like et la méthode de Babai. L'efficacité du système PMNS a été démontrée (dans la thèse de Yssouf Dosso du laboratoire Imath) sur une architecture 64 bits pour les entiers utilisés classiquement dans le domaine de la cryptographie basée sur les courbes elliptiques (entiers de taille 256 à 512 bits). Au-delà, au fur et à mesure que le rapport entre la taille de *p* et la taille des mots machine augmente, il est de plus en plus difficile de trouver un jeu de paramètres permettant d'obtenir une implémentation logicielle efficace. Ceci explique aussi pourquoi dans le cadre de systèmes embarqués (architecture 8, 16 voire 32 bits) les PMNS sont peu adaptés. Un premier axe de recherche de cette thèse sera de comprendre d'où provient cette limitation et de chercher à la contourner en adoptant une approche hybride combinant la représentation multi-précision des entiers et les PMNS. Plus précisément, on étudiera une arithmétique efficace et sécurisée sur des mots de 128 bits afin de pouvoir diminuer le rapport entre la taille de *p* et la taille des mots manipulés. Suite à cette première exploration, de nombreuses pistes sont envisageables en prenant en compte les spécificités des jeux d'instructions AVX2 et AVX512, ce dernier permettant par exemple d'effectuer en parallèle 4 multiplications d'entiers de 52 bits ce qui correspond à une arithmétique sur 104 bits au lieu de 128.

Un deuxième axe de recherche concerne spécifiquement l'algorithme de Babai. Jusqu'à présent la réduction interne via la méthode Montgomery-like était considérée comme étant la plus performante. Un travail récent effectué par Nicolas Méloni montre que la méthode de Babai permet elle aussi d'obtenir une réduction interne efficace. Dans un premier temps, on étudiera comment l'arithmétique développée dans l'axe précédent peut être intégrée au sein de la méthode de Babai. Par la suite, on s'intéressera à la sécurisation de cet algorithme en introduisant de l'aléa au fur et à mesure des calculs effectués. En effet, afin de résister aux attaques par canaux auxiliaires, il est important de pouvoir introduire de l'aléa au sein de chaque étape d'un algorithme afin que la répétition de ce dernier avec un jeu de données identique ne produise pas les mêmes valeurs intermédiaires.

Finalement, on étudiera la faisabilité de l'implémentation des solutions proposées dans les 2 axes ci-dessus dans le contexte des FPGA. Plus précisément, l'objectif sera d'identifier pour des tailles cryptographiques standards, quelle est l'arithmétique la plus appropriée (en terme de taille de mots) pour obtenir une représentation efficace des entiers.

Méthodes :

L'étudiant commencera par effectuer une bibliographie précise du peu de résultats existants dans le domaine récent de la représentation PMNS. Des réunions hebdomadaires avec ce dernier permettront de suivre l'évolution de la thèse et de faire évoluer les perspectives de recherche. Un entrepôt github sera mis en place afin de suivre l'évolution de la thèse et pouvoir effectuer régulièrement des revues de code.

Retombées attendues :

Publications dans des revues internationales de rang A. Renforcement d'une collaboration avec la société Thalès qui mène aussi des recherches dans le domaine de l'arithmétique modulaire efficace. Mise en ligne d'une bibliothèque de calcul multi-précision adaptée à la cryptographie à clé publique.

Mots clés :

Cybersécurité, Cryptographie post-quantique, IoT, arithmétique des ordinateurs.

Références :

On Polynomial Modular Number Systems over Z/pZ

Jean-Claude Bajard, Jérémy Marrez, Thomas Plantard, Pascal Véron
Advances in Mathematics of Communications, AIMS, In press, ⟨10.3934/amc.2022018⟩
DOI : 10.3934/amc.2022018

Compact variable-base ECC scalar multiplication using Euclidean addition chains
Fabien Herbaut, Nicolas Méloni, Pascal Véron
18th International Conference on Security and Cryptography (SECRYPT 2021), Jul 2021, Online Event, Italy. pp.531-539, ⟨10.5220/0010551705310539⟩
DOI : 10.5220/0010551705310539

Efficient modular operations using the adapted modular number system
Laurent-Stéphane Didier, Fangan-Yssouf Dosso, Pascal Véron
Journal of Cryptographic Engineering, Springer, 2020, ⟨10.1007/s13389-019-00221-7⟩
DOI : 10.1007/s13389-019-00221-7

Randomization of Arithmetic over Polynomial Modular Number System
Laurent-Stéphane Didier, Fangan-Yssouf Dosso, Nadia El Mrabet, Jérémy Marrez, Pascal Véron
26th IEEE International Symposium on Computer Arithmetic, Jun 2019, Kyoto, Japan. pp.199-206, ⟨10.1109/ARITH.2019.00048⟩
DOI : 10.1109/ARITH.2019.00048

Euclidean addition chains scalar multiplication on curves with efficient endomorphism
Fangan-Yssouf Dosso, Fabien Herbaut, Nicolas Méloni, Pascal Véron
Journal of Cryptographic Engineering, Springer, In press, ⟨10.1007/s13389-018-0190-0⟩
DOI : 10.1007/s13389-018-0190-0

Encadrement et conditions matérielles pour le doctorant

L'étudiant sera encadré par Nicolas Méloni et Pascal Véron du laboratoire Imath. Il disposera d'un bureau au bâtiment M et le laboratoire se chargera de financer un équipement adéquat nécessaire au bon déroulement de sa thèse.

Compétences attendues et personnes à contacter

Compétences attendues :

Le candidat devra avoir des bases solides dans le développement informatique ainsi que des notions en mathématiques discrètes (arithmétique dans Z/nZ, théorie des corps finis) et en cryptographie.

Personne(s) à contacter :

Pascal Véron (veron@univ-tln.fr) ou Nicolas Méloni (meloni@univ-tln.fr)