Thales Communications & Security, CRISTAL, Gennevilliers (92)

Propositions de Stage 2017

1 Méthode GLV en dimension 4 sur les $\mathbb{Q}$-courbes

Type de stage : Recherche & Développement

Contacts : olivier.bernard2@thalesgroup.com, renaud.dubois@thalesgroup.com
et olivier.orciere@thalesgroup.com

Contexte

La cryptographie à base de courbes elliptiques demeure actuellement un outil incontournable permettant d'apporter efficacement de hauts niveaux de sécurité aux applications civiles et militaires. Les courbes standardisées par le NIST dans la norme FIPS 186-2 ont maintenant plus de 15 années, et récemment les révélations d'Edward Snowden ont levé des doutes quant au fait que ces courbes puissent cacher des vulnérabilités.

Dans ce contexte, le besoin d'une nouvelle génération de courbes elliptiques, telle qu'initiée par le NIST en 2015 (*Workshop on Elliptic Curve Cryptography Standards*), sert deux motivations : la première est de retrouver la confiance du public, la seconde est de bénéficier des multiples avancées algorithmiques de la dernière décennie.

Ces avancées permettent, notamment *via* le choix de nouveaux modèles de courbes et de lois d'addition complètes, d'obtenir de meilleures performances hardware et software, des implémentations plus simples et plus sûres, des propriétés de résistance aux *timing attacks* ou aux *side-channel attacks*.

La courbe Four$\mathbb{Q}$ proposée par Microsoft Research [7, 8, 9] semble adresser à la fois les problématiques de performances, de simplicité et de sécurité. Elle concurrence directement la courbe `Curve25519` de Bernstein. Basée sur les familles de $\mathbb{Q}$-courbes de Smith [5], elle combine l'utilisation des endomorphismes de Frobenius et de la multiplication complexe, la loi d'addition fortement unifiée des modèles d'Edwards tordus, le tout modulo un nombre premier de la forme $2^n - \epsilon$.

Le but de ce stage est de reproduire les gains de performances obtenus par Costello et Longa [7], ainsi que, si le temps le permet, de proposer des améliorations et des extensions à des niveaux de sécurité plus élevés.

Description du stage

Dans un premier temps, le stagiaire se familiarisera avec la méthode GLV [2] et son extension sur les courbes GLS [3]. L'attention sera surtout portée sur les familles de $\mathbb{Q}$-courbes [5] ainsi que sur les méthodes de type GLV multi-dimensionnelles comme [6]. L'objectif de cette phase de bibliographie est de comprendre les mécanismes utilisés pour l'arithmétique des $\mathbb{Q}$-courbes [5, 6, 4] et de la courbe Four$\mathbb{Q}$ notamment [7].

Dans un deuxième temps, le stagiaire réalisera une implémentation haute performance et en temps constant de la multiplication scalaire sur ces courbes [7, 8, 9].

En particulier, le stagiaire aura à implémenter une arithmétique efficace sur $\mathbb{F}_{p^2}$, où p est un nombre premier creux de la forme $2^n - \epsilon$. Il implémentera également la multiplication scalaire en coordonnées étendues sur les courbes d'Edwards tordues. Un soin particulier sera apporté à la recherche d'une décomposition optimale du scalaire sur la base des valeurs propres des endomorphismes retenus [4, 7].

Une étude des propriétés intrinsèques de résistance aux attaques par canaux auxiliaires (SPA, DPA, *timing attacks*) [9, 10] sera faite ainsi que l'intégration de contremesures propriétaires spécifiées par le laboratoire [1].

Le code produit devra être raisonnablement générique et s'intégrer à la librairie cryptographique modulaire du Laboratoire Chiffre.

Pour terminer, le stagiaire sera amené à proposer des solutions originales tant au niveau de l'algorithmique que de l'implémentation, qui pourront le cas échéant faire l'objet d'une publication.

De solides compétences mathématiques sur les courbes elliptiques sont nécessaires, ainsi qu'une bonne connaissance d'algorithmie arithmétique. Une certaine aisance en programmation, notamment dans le langage C, sera très appréciée.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[1] O. Bernard, R. Dubois : Contremesures face aux SPA à très faible bruit sur la multiplication scalaire de points, In *Rapport interne, TCS, 2016*.

[2] R.P. Gallant, R.J. Lambert, S.A. Vanstone : Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms, In *Advances in Cryptology – CRYPTO 2001*, pp. 190-200, Lecture Notes in Computer Science vol. 2139, Springer Berlin Heidelberg.

[3] S.D. Galbraith, X. Lin, M. Scott : Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves, In *Advances in Cryptology – EUROCRYPT 2009*, pp. 518-535, Lecture Notes in Computer Science vol. 5479, Springer Berlin Heidelberg.

[4] P. Longa, F. Sica : Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication, In *Journal of Cryptology* vol. 27 **(2)**, April 2014, pp. 248-283, Springer US.

[5] B. Smith : Families of Fast Elliptic Curves from $\mathbb{Q}$-curves, In *Advances in Cryptology – ASIACRYPT 2013*, pp. 61-78, Lecture Notes in Computer Science vol. 8269, Springer Berlin Heidelberg.

[6] A. Guillevic, S. Ionica : Four-Dimensional GLV via the Weil Restriction, In *Advances in Cryptology – ASIACRYPT 2013*, pp. 79-96, Lecture Notes in Computer Science vol. 8269, Springer Berlin Heidelberg.

[7] C. Costello, P. Longa : Four$\mathbb{Q}$: Four-Dimensional Decompositions on a $\mathbb{Q}$-curve over the Mersenne Prime, In *Advances in Cryptology – ASIACRYPT 2015*, pp. 214-235, Lecture Notes in Computer Science vol. 9452, Springer Berlin Heidelberg.

[8] P. Longa : Software Implementation of Public-Key Cryptography, In *SAC Summer School 2016 (S3)*, slides.

[9] K. Järvinen, A. Miele, R. Azarderakhsh, P. Longa : Four$\mathbb{Q}$ on FPGA : New Hardware Speed Records for Elliptic Curve Cryptography over Large Prime Characteristic Fields, In *Cryptographic Hardware and Embedded Systems – CHES 2016*, pp. 517-537, Lecture Notes in Computer Science vol. 9813, Springer Berlin Heidelberg.

[10] E. Nascimento, L. Chmielewski, D. Oswald, P. Schwabe Attacking embedded ECC Implementations through cmov side channels, In `eprint.iacr.org/2016/923`.

2 Attaques par canaux auxiliaires sur les schémas post-quantiques

Type de stage : Recherche & Développement

Contacts : ange.martinelli@thalesgroup.com et thomas.prest@thalesgroup.com

Contexte

Les récents progrès vers la construction d'ordinateurs quantiques remettent en cause la sécurité des protocoles cryptographiques classiques. En effet, ceux-ci sont basés sur les problèmes de la factorisation et du logarithme discret, que de tels ordinateurs pourraient aisément résoudre. La cryptographie post-quantique utilise d'autres objets mathématiques sur lesquels ils existe des problèmes supposés difficiles pour les ordinateurs quantiques : les réseaux euclidiens [1, 2], les codes correcteurs [3], les fonctions de hachage [4], les polynômes multivariés, etc.

D'autre part, les attaques par canaux auxiliaires permettent d'exploiter des données physiques (temps d'exécution, consommation électrique, etc.) mesurables durant l'exécution d'un algorithme pour en extraire les éléments secrets. Ces attaques ont donné les meilleurs résultats pratiques connus et sont un domaine extrêmement actif de la recherche appliquée.

L'organisme de standardisation NIST a lancé un appel à candidatures pour standardiser des schémas post-quantiques. Dans ce contexte, la résistance aux attaques par canaux auxiliaires sera un critère discriminant. L'arrivée récente d'implémentations pratiques de schémas post-quantiques [3, 5] a permis l'étude et la réalisation d'attaques par canaux auxiliaires qui donnent déjà d'excellents résultats [6].

Description du stage

L'objectif de ce stage est d'étudier la vulnérabilité aux attaques par canaux auxiliaires de schémas post-quantiques. Dans un premier temps, un état de l'art des schémas résistant aux attaques quantiques sera effectué. Puis le stagiaire étudiera la vulnérabilité aux attaques par canaux auxiliaires d'un schéma préalablement choisi. Enfin, il pourra proposer des contre-mesures aux attaques mises en valeur. Les résultats obtenus pourront faire l'objet d'une publication académique.

La répartition des travaux sera la suivante :

1. **État de l'art :** étude des schémas post-quantiques, de leurs implémentations et des attaques par canaux auxiliaires sur celles-ci. (1 mois)
2. **Attaque sur un schéma post-quantique :** un schéma sera choisi comme cible pour une attaque par canaux auxiliaires. Après une étude théorique, le stagiaire pourra être amené à évaluer celle-ci sur une implémentation pratique. (3 mois)
3. **Contre-mesures :** le stagiaire soumettra des contre-mesures aux attaques existantes, aussi bien celles qu'il aura trouvées que celles publiées. (1 mois)
4. **Rédaction :** écriture du rapport et préparation à la soutenance de stage. (1 mois)

Un solide bagage mathématique sera indispensable. Des bases en programmation, notamment en language C, seront appréciées, ainsi que des connaissances sur les attaques par canaux auxiliaires. Le stagiaire devra disposer d'un goût pour la recherche et faire preuve d'esprit d'initiative.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[1] L. Ducas, A. Durmus, T. Lepoint, V. Lyubashevsky, Lattice Signatures and Bimodal Gaussians, In *Advances in Cryptology – CRYPTO 2013*, pp. 40-56.

[2] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe Post-quantum key exchange - A new hope, In *25th USENIX Security Symposium, USENIX Security 2016*, pp. 327-343.

[3] D.J. Bernstein, T. Chou, P. Schwabe, McBits : Fast Constant-Time Code-Based Cryptography, In *Cryptographic Hardware and Embedded Systems – CHES 2013*, pp. 250-272.

[4] D.J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn, SPHINCS : Practical Stateless Hash-Based Signatures, In *Advances in Cryptology – EUROCRYPT 2015*, pp. 368-397.

[5] PQCrypto Usage & Deployment - `https://ianix.com/pqcrypto/pqcrypto-deployment.html`

[6] L.G. Bruinderink, A. Hülsing, T. Lange, Y. Yarom, Flush, Gauss, and Reload - A Cache Attack on the BLISS Lattice-Based Signature Scheme, In *Cryptographic Hardware and Embedded Systems – CHES 2016*, pp. 323-345.

3 Sécurisation du Cloud – Schémas de recherche sur données chiffrées avancés

Type de stage : Recherche & Développement

Contact : alexandre.anzalayamajako@thalesgroup.com, emeline.hufschmitt@thalesgroup.com

Contexte

La constante augmentation des débits de connexion et l'apparition sur le marché d'appareils mobiles aux ressources plus limitées que celles d'un ordinateur personnel, engendrent de nouveaux besoins. Après la démocratisation des services de messagerie électronique, l'avènement du *cloud computing* offre de nouvelles perspectives aux utilisateurs comme le partage de médias (documents, musique, vidéos, livres) et d'applications (tableurs, traitement de texte, affichage de documents, requêtes à des bases de données).

La récente impulsion du projet Cloudwatt visant à doter la France d'une infrastructure de *cloud* souveraine s'explique notamment par les problématiques de sécurité liées à l'hébergement de données sur un serveur distant qui n'est pas nécessairement de confiance. Cependant, la recherche d'un niveau de service plus élevé via l'adaptation de résultats académiques sur la recherche sur données chiffrées à un contexte opérationnel reste aujourd'hui peu répandue.

Les schémas de chiffrement *totalement homomorphiques* initialement proposés par Gentry [1], c'est-à-dire les schémas dont la fonction de chiffrement conserve la structure d'anneau, apportent une réponse théorique à la problématique générale de manipulation aveugle de données chiffrées mais imposent encore aujourd'hui des contraintes qui empêchent leur adoption au sein de systèmes opérationnels. En se concentrant sur la problématique plus restreinte de recherche sur les données chiffrées, on se donne alors la possibilité d'obtenir des schémas présentant des garanties de sécurité sans sacrifier l'aspect pratique.

Dans ces schémas un client stocke ses données sur un serveur en dehors de son périmètre de confiance tout en conservant la possibilité d'effectuer des recherches sur ces données. La propriété de sécurité que l'on cherche à atteindre est que le serveur distant opère sans découvrir ni les requêtes ni leurs réponses. Des publications récentes ainsi que des travaux internes ont conduit à valider la possibilité de schémas pratiques de recherche sur données chiffrées. L'objectif est aujourd'hui de consolider et d'apporter des fonctionnalités supplémentaires aux travaux existants.

Description du stage

En s'appuyant sur des travaux internes [5], [6], [7], [8], le (la) stagiaire sera amené(e) à réaliser une étude bibliographique des schémas de recherche sur données chiffrées symétriques en portant une attention particulière au schéma de D. Cash *et al.* introduit à CRYPTO 2013 ainsi que des extensions génériques liées [2], [4], [3]. Sur la base de ces résultats, on évaluera le compromis entre sécurité et fonctionnalités selon trois axes :

- l'ajout du **dynamisme** (ajout, suppression de fichier) ;
- l'adaptation pour des requêtes **évoluées** (booléennes, sur des intervalles, sur des sous-chaînes) ;
- l'intégration de capacité de **délégation et de révocation de droits de recherche à des tiers**.

De solides compétences en cryptographie sont nécessaires, ainsi qu'une bonne maîtrise de l'algorithmie. Une certaine aisance en programmation, notamment dans le langage C, sera très appréciée.

Durée des travaux

La durée prévue pour ce stage est de 6 mois.

Références

[1] C. Gentry Fully homomorphic encryption using ideal lattices In *STOC 20009*, pp.169-178

[2] D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, M. Steiner Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries In *Advances in Cryptology – CRYPTO (1) 2013*, pp.353-373

[3] S. Jarecki, C. S. Jutla, H. Krawczyk, M. Rosu, M. Steiner Outsources symmetric private information retrieval In *Computer & Communication Security 2013*, pp.875-888

[4] S. Faber, S. Jarecki, H. Krawczyk, H. Nguyen, M. Rosu, M. Steiner Rich quesries on encrypted data : Beyond exact matches In *ESORICS 2015*, pp.123-145

[5] B. Dravie Techniques de Recherche sur les Données Chiffrées In Document interne Thales/ Université Paris 13, 2013

[6] T. Ricosset, M. Latimier Recherche sur les Données Chiffrées Évoluée et Efficace In Document interne Thales/ Université Paris 13, 2014

[7] T. Rouxel Recherche sur les Données Chiffrées Dynamique In Document interne Thales/ Université Versailles Saint-Quentin-En-Yvelines, 2015

[8] M. Giraud Cryptanalyse de schémas de recherches sur données chiffrées In Document interne Thales/ Université de Bordeaux, 2016