Propositions de Stage 2024-2025

Gennevilliers (Île-de-France), Cholet (Pays de la Loire), France

Thales propose des systèmes d'information et de communication sécurisés et interopérables pour les forces armées, les forces de sécurité et les opérateurs d'importance vitale. Ces activités, qui regroupent radiocommunications, réseaux, systèmes de protection, systèmes d'information critiques et cybersécurité, répondent aux besoins de marchés où l'utilisation des nouvelles technologies numériques est déterminante. Thales intervient tout au long de la chaîne de valeur, des équipements aux systèmes en passant par le soutien logistique et les services associés.

Les sites de Gennevilliers et Cholet sont au cœur des activités de conception, et de développement et de soutien des produits et solutions de radiocommunications des Armées, des systèmes de réseaux d'infrastructures résilients et de communications par satellite, et ainsi que des solutions de cybersécurité.

Les stages proposés se dérouleront sur une période de 6 mois terminant avant fin septembre, sur le site de Gennevilliers ou de Cholet, au sein du service de cryptologie. La rémunération est, à titre indicatif, de 1 500 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.

Sujets de stage

1 Attaques par canaux auxilliaires en crypto fondée sur les réseaux

Type de stage : Recherche
Lieu du stage : Gennevilliers
Contacts : `pierre.louis.cayrel@univ-st-etienne.fr`, `vincent.grosso@cnrs.fr`, `thomas.legavre@thalesgroup.com`, `angelique.lopez@thalesgroup.com`, `thomas.ricosset@thalesgroup.com`

Contexte

L'émergence de l'informatique quantique menace la sécurité de nombreux protocoles cryptographiques largement utilisés, en particulier ceux fondés sur la factorisation et le logarithme discret. La cryptographie fondée sur les réseaux euclidiens (*lattices*) est une alternative prometteuse en raison de sa résistance supposée aux attaques quantiques et de son efficacité. La transformation Fiat-Shamir avec rejets est largement adoptée pour construire des schémas de signature fondés sur les réseaux. C'est en particulier le cas du nouveau standard `ML-DSA/Dilithium` et du candidat `Haetae`.

Cependant, les attaques par canaux auxiliaires, qui exploitent des vulnérabilités spécifiques aux implémentations (telles que la consommation d'énergie, le temps d'exécution ou les émissions électromagnétiques), font peser une importante menace même sur les primitives théoriquement sûres. Des recherches récentes ont montré que les schémas de signature fondés sur les réseaux sont particulièrement vulnérables à de telles attaques, soulevant de sérieuses inquiétudes quant à la sécurité de leurs implémentations.

Ce stage se concentrera sur l'identification, l'analyse et l'atténuation des vulnérabilités liées aux attaques par canaux auxiliaires sur les schémas de signatures de type Fiat-Shamir fondés sur les réseaux euclidiens.

Objectifs

L'objectif principal de ce stage est d'étudier les attaques par canaux auxiliaires visant les schémas `ML-DSA/Dilithium` [Dilithium] et `Haetae` [Haetae]. Les tâches principales incluent :

- **Étude de schémas de signature Fiat-Shamir** : Comprendre les principes fondamentaux de la transformation Fiat-Shamir et comment elle est appliquée aux schémas `ML-DSA/Dilithium` et `Haetae`.
- **État de l'art des attaques par canaux auxiliaires** : Explorer la littérature existante sur les attaques par canaux auxiliaires contre `ML-DSA/Dilithium` [RCDB24, BAERS24, BCMV23].
- **Évaluation des vulnérabilités** : Identifier les vulnérabilités potentielles dans une implémentation choisie d'un de ces deux schémas, en se concentrant sur l'analyse de la consommation d'énergie.
- **Démonstration expérimentale d'attaques** : Mettre en place un environnement pour mener des attaques par canaux auxiliaires sur cette implémentation. Cela peut inclure la collecte de la consommation électrique, grâce à un ChipWhisperer et l'application de techniques statistiques et calculatoires pour extraire des informations secrètes.
- **Contre-mesures** : Selon opportunité, rechercher et proposer des contre-mesures pour atténuer les vulnérabilités liées aux fuites identifiées et évaluer l'efficacité de ces contre-mesures.

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 ;
- Recherche de contributions scientifiques et 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.

References

[Dilithium] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehlé: CRYSTALS-Dilithium – Algorithm Specifications and Supporting Documentation (Version 3.1). Specification document. 2021-02-08.
`https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf`

[Haetae] Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, MinJune Yi: HAETAE – Specifications (Version 3.0). Specification document. 2024-07-04.
`https://drive.usercontent.google.com/u/0/uc?id=11FONomxp4XwETrLfQIHrka-jy0DP29Iv&export=download`

[RCDB24] Prasanna Ravi, Anupam Chattopadhyay, Jan Pieter D'Anvers, Anubhab Baksi: Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results. ACM Trans. Embed. Comput. Syst. 2024.
`https://eprint.iacr.org/2022/737.pdf`

[BAERS24] Olivier Bronchain, Melissa Azouaoui, Mohamed ElGhamrawy, Joost Renes, Tobias Schneider: Exploiting Small-Norm Polynomial Multiplication with Physical Attacks: Application to CRYSTALS-Dilithium. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2024.
`https://eprint.iacr.org/2023/1545.pdf`

[BCMV23] Alexandre Berzati, Andersson Calle Viera, Maya Chartouny, Steven Madec, Damien Vergnaud, David Vigilant: Exploiting Intermediate Value Leakage in Dilithium: A Template-Based Approach. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023.
`https://eprint.iacr.org/2023/050.pdf`

2 Méthode d'extraction de clé à partir de distingueurs

Type de stage : Recherche
Lieu du stage : Gennevilliers
Contacts : nicolas-i.david@thalesgroup.com thomas.rabaud@thalesgroup.com

Contexte

La cryptologie possède une histoire riche et ancienne qui remonte à des milliers d'années. Au fil du temps, les conceptions cryptologiques ont évolué parallèlement aux techniques utilisées pour les attaquer. Alors que les cryptographes inventaient de nouvelles façons de sécuriser les informations, leurs adversaires répliquaient avec des approches innovantes pour extraire des données à partir de messages cryptés. Cette dynamique a conduit au développement de méthodes de plus en plus sophistiquées et à l'émergence de la cryptographie moderne.

Les primitives cryptographiques actuelles peuvent être séparées en deux famille : *cryptographie symétrique* et *cryptographie asymétrique*. La cryptographie symétrique, également connue sous le nom de cryptographie à clé secrète, implique l'utilisation d'une seule clé secrète partagée pour le chiffrement et le déchiffrement. Ce type de cryptographie est efficace et rapide, ce qui le rend adapté à la transmission et au stockage sécurisés de données à travers l'utilisation de primitives comme les chiffrements par blocs.

La cryptanalyse des chiffrements par blocs fait parfois appel à des distingueurs (par ex la cryptanalyse différentielle [BS91]) pour monter une attaque permettant d'extraire la clé à partir de couples de messages clairs-chiffrés (key recovery attack). Si la technique du early abort semblait être la technique à adopter lors de l'extraction de clé, des travaux récents semblent indiquer que d'autres opérateurs d'extraction de clés peuvent exister [Bour+23, Ah+24, Song+24].

Ce stage a pour but d'identifier et d'appliquer les opérateurs de key recovery à différents types de distingueurs. Par exemple, nous pourrions explorer les attaques rotationnelles avec un opérateur de key recovery de type Meet-in-the-Middle.

Objectifs

L'objectif principal de ce stage est d'étudier les techniques dévelopées dans les travaux de [Bour+23, Ah+24, Song+24] et de proposer une extension de ce type de cryptanalyse à d'autres types de distingueurs. Les tâches principales incluent :

- **État de l'art des techniques de key recovery** : Explorer et comprendre les travaux de [Bour+23, Ah+24, Song+24] dans le cas particulier des distingueurs différentiels.
- **État de l'art des distingueurs** : Explorer la litérature à la recherche de chiffrements et de distingueurs pour lesquels des nouveaux opérateurs de key recovery seraient efficace.
- **Application à la cryptanalyse d'un chiffrement par bloc** : Application de la théorie développée précédemment pour améliorer proposer une nouvelle attaque.

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 ;
- Recherche de contributions scientifiques et 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.

References

[BS91] Eli Biham and Adi Shamir Differential Cryptanalysis of Feal and N-Hash Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings

[Ah+24] Zahra Ahmadian and Akram Khalesi and Dounia M'foukh and Hossein Moghimi and María Naya-Plasencia Improved Differential Meet-in-the-Middle Cryptanalysis Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part I, Lecture Notes in Computer Science `https://eprint.iacr.org/2024/351`

[Bour+23] Christina Boura and Nicolas David and Patrick Derbez and Gregor Leander and María Naya-Plasencia Differential Meet-In-The-Middle Cryptanalysis Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III `https://eprint.iacr.org/2022/1640`

[Song+24] Ling Song and Huimin Liu and Qianqian Yang and Yincen Chen and Lei Hu and Jian Weng Generic Differential Key Recovery Attacks and Beyond Cryptology ePrint Archive, Paper 2024/1447 `https://eprint.iacr.org/2024/1447`

3 Développement et intégration de primitives cryptographiques dans OpenSSL

Type de stage : Développement
Lieu du stage : Cholet
Contact : `sylvain.lachartre@thalesgroup.com, louis.beclair@thalesgroup.com`

Contexte

L'implémentation sûre et maîtrisée de primitives cryptographiques est un domaine prépondérant de la sécurité informatique. En effet, au-delà du bon choix des algorithmes, les attaques mises en œuvre ces dernières années sur les librairies les plus répandues, illustrent le fait qu'une bonne implémentation nécessite énergie et savoir-faire.

Au sein du domaine Sécurité des Technologies de l'Information, vous serez en charge de l'intégration de primitives cryptographiques dans la librairie OpenSSL [OpenSSL]. Après avoir pris connaissance de l'architecture de la librairie, vous serez amené·e à intégrer, un panel de primitives cryptographiques symétriques et asymtériques déjà exsitantes, développées en langage C. Enfin, un effort particulier sera porté sur l'élaboration et la mise en œuvre d'un plan de tests permettant de valider la solution sur un démonstrateur.

La connaissance de la librairie OpenSSL et des compétences en développement logiciel (langage C, assembleur, makefile) ne sont pas pré-requises mais seront valorisées.

Objectifs

L'objectif principal de ce stage est d'intégrer du code maîtrisé dans la librairie cryptographique OpenSSL [OpenSSL]. Les tâches principales incluent :

- **Étude de l'architecture de OpenSSL**: comprendre l'architecture et le fonctionnement de la librairie,
- **Sélection des primitives cryptographiques**: réaliser une sélection de primitives cryptographiques symétriques et asymétriques dans des codes déjà existants,
- **Intégration de ces primitives dans OpenSSL**: intégrer les primitives sélectionnées dans OpenSSL, mettre à jour les procédures de compilation et d'installation de la librairie,
- **Test de la solution**: mettre en place un plan de tests permettant de valider la solution développée, et éventuellement un démonstrateur mettant en œuvre une surcouche protocolaire.

Note: en fonction de l'avancement des travaux, des primitives cryptographiques *supplémentaires* pourront également être développées, puis intégrées à la solution (version optimisées, autres primitives, etc.).

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 :

- Étude de la librairie OpenSSL: 1 mois,
- Intégration des primitives dans OpenSSL: 3 mois,
- Tests et mise en place du démonstrateur: 1 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.

References

[OpenSSL] OpenSSL Software Foundation Inc, OpenSSL Library (v3.3.2, 2024/09/03), `https://www.openssl.org`