Propositions de Stage 2025-2026

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 1 250 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.

Table des matières

1 Chiffrement avancé fondé sur les problèmes LWE

Type de stage : M2 (6 mois) – Recherche – Lattice-based cryptography

Lieu du stage : Gennevilliers (RER C, Metro 13)

Contacts : `gregoire.anquetin@thalesgroup.com`, `ky.nguyen@lip6.fr` [1], `thomas.ricosset@thalesgroup.com`, `eric.sageloli@thalesgroup.com`

Résumé : Ce stage vise à analyser et concevoir des schémas de chiffrement fondé sur l'identité (IBE) et sur les attributs (ABE), en exploitant les trappes MP12 [MP12] et des hypothèses de sécurité modernes comme *Succinct-LWE* [Wee24]. Les applications ciblent la *data-centric security*, où le chiffrement doit intégrer directement la politique d'accès. La poursuite de ces travaux de stage en thèse Cifre est prévue et souhaitée.

Motivation : L'essor des architectures centrées sur les données appelle des primitives de chiffrement avancé : IBE et ABE permettent de se passer d'une PKI lourde et d'intégrer les politiques de contrôle directement au sein des données. Côté post-quantique, les hypothèses lattices/réseaux ((M)SIS, (M)LWE, etc.) fournissent de bonnes garanties de sécurité ainsi que la flexibilité nécessaire à la conception des telles primitives. L'objectif est d'obtenir des constructions d'IBE puis d'ABE compactes satisfaisant un fort niveau de sécurité dans le modèle standard (en opposition au modèle de l'oracle aléatoire). Concernant l'ABE, afin de rendre les contructions plus efficaces, de *petites* politiques d'accès seront considérées, dans les régimes *key-policy* (KP) et *ciphertext-policy* (CP).

Trappes MP12 : Introduites par Micciancio–Peikert (2012) [MP12], elles reposent sur une matrice dite « gadget » et permettent d'échantillonner un petit vecteur gaussien entier $\mathbf{z}$ satisfaisant $\mathbf{Az} = \mathbf{0} \bmod q$ pour une matrice $\mathbf{A}$ pseudo-aléatoire. Elles permettent en particulier de délivrer des clés privées à partir d'identités ou d'attributs dans certains IBEs et ABEs. Des techniques plus récentes de trappes (p. ex. [LLW21]) ont amélioré les trappes MP12 dans le même contexte.

Succinct-LWE : Variante récente de LWE permettant des constructions plus générales (ABE pour circuits) grâce à des structures additionnelles, tout en cherchant à maintenir une sécurité satisfaisante [Wee24]. Cette hypothèse ouvre des perspectives de recherche intéressantes.

Objectifs du stage :

1. Étude de l'état de l'art des IBEs modèle standard, de [ABB10] à des travaux plus recents (p. ex. [Yam17]).
2. Étude de l'état de l'art des ABEs fondés sur Succinct-LWE (p. ex. [Wee25]).
3. Recherche de nouvelles techniques pour la conception d'un IBE.
4. Extension vers l'ABE et étude du cas des politiques d'accès bornées.

Ces objectifs sont ambitieux et visent à orienter le déroulement du stage tout en clarifiant les attentes. Ils pourront être ajustés en fonction des progrès réalisés et des idées échangées au fil du stage.

Prérequis : Bien que la connaissance des constructions cryptographiques dont la sécurité repose sur les réseaux euclidiens (problèmes LWE, SIS, ...) soit un atout, elle n'est pas indispensable. Nous conseillons donc aux personnes intéressées de déposer une candidature même si elles n'ont pas encore étudié les thèmes abordés.

1. Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

Références

[ABB10] Shweta Agrawal, Dan Boneh, Xavier Boyen : Efficient Lattice (H)IBE in the Standard Model. EUROCRYPT 2010. https://www.iacr.org/archive/eurocrypt2010/66320276/66320276.pdf

[MP12] Daniele Micciancio, Chris Peikert : Trapdoors for Lattices : Simpler, Tighter, Faster, Smaller. EUROCRYPT 2012. https://eprint.iacr.org/2011/501.pdf

[Yam17] Shota Yamada : Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques. CRYPTO 2017. https://eprint.iacr.org/2017/096.pdf

[LLW21] Qiqi Lai, Feng-Hao Liu, Zhedong Wang : New Lattice Two-Stage Sampling Technique and Its Applications to Functional Encryption - Stronger Security and Smaller Ciphertexts. EUROCRYPT 2021. https://eprint.iacr.org/2022/779.pdf

[Wee24] Hoeteck Wee : Circuit ABE with poly(depth,λ)-Sized Ciphertexts and Keys from Lattices. CRYPTO 2024. https://eprint.iacr.org/2024/1416.pdf

[Wee25] Hoeteck Wee : Almost Optimal KP and CP-ABE for Circuits from Succinct LWE. EUROCRYPT 2025. https://eprint.iacr.org/2025/509.pdf

2 Cryptanalyse symétrique aidée par MILP

Type de stage : M2 (6 mois) – Recherche – Cryptanalyse symétrique

Lieu du stage : Gennevilliers (RER C, Metro 13)

Contacts : `nicolas-i.david@thalesgroup.com`, `aurelien.dupin@thalesgroup.com`, `thomas.rabaud@thalesgroup.com`

Résumé : Ce stage a pour objectif l'étude des applications de l'outil MILP (*Mixed Integer Linear Programming*) en cryptanalyse symétrique.

Motivation : L'analyse de la sécurité des primitives symétriques repose souvent sur des procédés algorithmiques complexes, susceptibles d'entraîner des erreurs. L'automatisation par ordinateur de ces études permet non seulement d'optimiser les performances des attaques, mais aussi de limiter les risques d'erreur. Depuis le début des années 2010, les techniques MILP [MWGP11] se sont imposées comme un outil puissant pour modéliser et renforcer les méthodes de cryptanalyse symétrique. Tandis que les travaux initiaux ciblaient principalement les attaques différentielles et linéaires [MWGP11], de nombreuses recherches ultérieures ont démontré que l'usage de cette approche permet également d'optimiser tout ou partie d'attaques fondées sur des paradigmes plus avancés [DDV20, BDG25, Qin+21, Qingju+18].

MILP : Le *Mixed Integer Linear Programming* (MILP) est une méthode d'optimisation mathématique qui vise à maximiser ou minimiser une fonction linéaire sous des contraintes linéaires, tout en imposant que certaines variables doivent prendre des valeurs entières.

Objectifs du stage :

1. Étude de l'état de l'art des modélisations des techniques aidées par MILP en commençant par [MWGP11].
2. Mise en évidence du dimensionnement associé aux applications.
3. Implémentation des techniques décrites dans la littérature.
4. Modélisation et implémentation de techniques plus avancée aboutissant à des attaques concrètes.

Ces objectifs sont ambicieux et visent à orienter le déroulement du stage tout en clarifiant les attentes. Ils pourront être ajustés en fonction des progrès réalisés et des idées échangées au fil du stage.

Références

[MWGP11] Mouha, Nicky and Wang, Qingju and Gu, Dawu and Preneel, Bart : Differential and linear cryptanalysis using mixed-integer linear programming
International Conference on Information Security and Cryptology 2011 `https://lirias.kuleuven.be/retrieve/333686`

[DDV20] Stéphanie Delaune, Patrick Derbez and Mathieu Vavrille : Catching the Fastest BoomerangsApplication to SKINNY
IACR Transactions on Symmetric Cryptology, 2020 `https://tosc.iacr.org/index.php/ToSC/article/view/8750`

[BDG25] Christina Boura, Patrick Derbez and Baptiste Germon : Extending the Quasidifferential Framework : FromFixed-Key to Expected Differential Probability
IACR Transactions on Symmetric Cryptology, 2025 `https://doi.org/10.46586/tosc.v2025.i1.515-541`

[Qin+21] Qin, Lingyue and Dong, Xiaoyang and Wang, Xiaoyun and Jia, Keting and Liu, Yunwen : Automated search oriented to key recovery on ciphers with linear key schedule : applications to boomerangs in SKINNY and ForkSkinny
IACR Transactions on Symmetric Cryptology, 2021 https://tosc.iacr.org/index.php/ToSC/article/view/8911/8487

[Qingju+18] Qingju Wang and Yonglin Hao and Yosuke Todo and Chaoyun Li and Takanori Isobe and Willi Meier Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly
Crypto, 2018 https://eprint.iacr.org/2017/1063