PhD Thesis Offer - Offre de thèse

English version - PhD Thesis Proposal (CIFRE)

Industrial Supervisor :
— Pierre-Yvan Liardet (pylou@eshard.com)
Academic Supervisors :
— Christophe Negre (christophe.negre@univ-perp.fr)
— Vincent Zucca (vincent.zucca@univ-perp.fr)

Main Site : eShard PESSAC, France.

Subject : ***Study of new counter-mesures for improved security of post-quantum cryptosystems facing side channel analysis.***

The world of public key cryptography is operating its revolution. Threaten by the raise of quantum computer and associated algorithms, that will break the old age public key primitives ; the cryptographic community is coming with proposals for a Post Quantum Cryptography (PQC) world where new algorithms will be out of reach from the Quantum Computer Power. But, like existing implementation of any cryptographic algorithm, the new algorithms are under the fire of hardware attacks i.e : side-channel and faults attacks, c.f. for instance [1].

The community is actively producing implementation integrating mitigation against these attacks on post quantum algorithms. Nevertheless, to validate the resistance of such implementations and avoid bad surprises when pushed inside products, there is an increasing need of, on one hand, a good understanding of the deployed countermeasure and, on the other hand, an effective verification. Indeed, it should be clarified to what extent the protections are effective against the vast arsenal of attack methods developed during the three last decades.

The objective of this PhD thesis is manifold, a first direction is to follow the new initiative of PQC algorithms and participate in the study of the new proposals from the hardware attack standpoint. Indeed, even if the NIST (National Institute of Standards and Technology) has initiated a standardization phase for a selected Key Exchange Mechanism (KEM) and three PQC Signature algorithms, the call for new algorithms is continuing to have alternatives on signature side. Indeed, the NIST officially launched a new Call for Proposals. For all these algorithms, implementation well protected against hardware attacks is a must have, especially for application with a high tradition in security, like banking, passport, ... or where the fast growing deployment is demanding in terms of security, like automotive and IoT in general. To address this strong demand, the PhD student will address the practical validation counter-measures against side-channel attacks for the coming standard, and will also propose implementation alternatives.

Version Française - Proposition de Thèse (CIFRE)

Encadrant industriel :
— Pierre-Yvan Liardet (pylou@eshard.com)
Encadrants académiques :
— Christophe Negre (chistophe.negre@univ-perp.fr)
— Vincent Zucca (vincent.zucca@univ-perp.fr)

Site Principal : eShard PESSAC Gironde

Titre : ***Études de contre-mesures pour protéger les cryptosystèmes post-quantiques contre les attaques par canaux cachés.***

Le monde de la cryptographie à clé publique fait sa révolution... Menacé par la montée en puissance de l'ordinateur quantique et des algorithmes associés qui promettent la fin des schémas basés sur la factorisation ou du logarithme discret. Depuis quelques années déjà, la communauté cryptographique propose des solutions avec des algorithmes dit post quantiques dont la difficulté du problème sous-jacent et la dimension des paramètres associés mettraient une sécurité théorique de l'encapsulation de clé (KEM) et de la signature numérique hors de portée d'ordinateur quantique. Cependant, comme pour toutes les implémentations d'algorithmes cryptographiques, les attaques hardwares telles que les attaques par canaux auxiliaires ou les attaques par faute constituent une menace importante, c.f. l'analyse sur les principaux algorithmes sélectionnés par le NIST [1].

La communauté est très active depuis plusieurs années afin de produire des implémentations intégrant des contre-mesures pour ces algorithmes post quantiques. Cependant, la validation de la résistance de ces implémentations, pour notamment anticiper de mauvaises surprises avant le déploiement, nécessite une bonne compréhension des contre-mesures déployées, ainsi que des moyens efficaces pour valider leur résistance. En effet, il est important de clarifier dans quelle mesure les protections proposées sont efficaces face à l'arsenal des attaques side-channel développées ces trente dernières années.

Les objectifs de cette thèse sont multiples, tout d'abord suivre les nouvelles initiatives et participer à l'effort collectif d'évaluation des nouvelles propositions. En effet, même si le NIST (National Institute of Standards and Technology), a déjà initié la phase d'écriture des standards pour un mécanisme d'échange de clé (KEM) et de trois schémas de signatures, l'organisme américain a lancé de nouveaux appels à candidature pour définir des alternatives aux algorithmes de signature numérique.

Tous ces algorithmes doivent, non seulement offrir une résistance convaincante à la cryptanalyse traditionnelle, y compris celle assistée de l'ordinateur quantique, mais également proposer des implémentations dûment protégées contre les attaques physiques comme le nécessitent traditionnellement certaines applications, comme la carte bancaire, le passeport,... mais aussi pour les applications en plein essor comme le domaine automobile ou plus généralement l'IoT.

Afin d'adresser cette forte demande, le travail de thèse traitera de la validation pratique des contre-mesures proposées dans les implémentations des standards à venir et proposera des implementations alternatives.

Références

[1] P. Ravi, A. Chattopadhyay, J. P. D'Anvers, and A. Baksi. Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium) : Survey and new results. *ACM Transactions on Embedded Computing System*, june 2023.