M2 Internship : Hardware security
Simplification-based physical attacks on lattice-based cryptosystems

Brice Colombier (https://bcolombier.fr) Pierre-Louis Cayrel (https://cayrel.net/)
Laboratoire Hubert Curien, Université Jean Monnet & CNRS, Saint-Étienne

Start date: February 2025

Context

The **post-quantum cryptography** standardization process, initiated by NIST [1] in 2016, aims to define new standards for key exchange and digital signature whose security is not threatened by the existence of a quantum computer of sufficient capacity. This resulted in the standardization of several algorithms in July 2024. An additional process is underway for digital signatures. Most of the selected algorithms base their security on hard problems from lattice theory. Numerous research works have investigated the hardness of these problems, and we now have a large taxonomy of problems of varying degrees of hardness.
Nevertheless, most of these studies do not take into account the additional information that could be obtained by carrying out **physical attacks** on implementations of these cryptosystems in electronic devices. Indeed, many studies have shown that physical attacks, by observing side-channels or injecting faults, provide more information than the knowledge of the cryptosystem's input and output values.
We therefore want to investigate the possibility of exploiting this additional information, obtained through physical attacks, to reduce the security of the cryptosystem by moving from the initial hard problem to a simpler instance or related problem.

Objectives

The objectives of this internship are :
- to rank known lattice problems and their various instances by hardness,
- to study the possibilities of moving down this hierarchy by exploiting additional information obtained through physical attacks,
- to carry out physical attacks to validate their practical feasibility.

These objectives will be discussed and may evolve according to the profile and preferences of the chosen student.

Requirements

We are looking for a student with a background in cryptography and an interest in hardware security. A Ph.D. may be considered at the end of the internship.

Practical aspects

Location Laboratoire Hubert Curien, Saint-Étienne (partial remote work is possible)

Compensation Internship allowance of around 600€/month, 50% of transportation costs covered for public transport (tram, bus, train, etc).

Expected start date February 2025

Duration Up to 6 months

How to apply ?

To apply for this internship, send your CV to {b.colombier; pierre.louis.cayrel}@univ-st-etienne.fr

1. National Institute of Standards and Technology

Stage M2 : Sécurité matérielle

Étude d'attaques physiques par simplification sur des cryptosystèmes basés sur les réseaux

Brice Colombier (https://bcolombier.fr) Pierre-Louis Cayrel (https://cayrel.net/)

Laboratoire Hubert Curien, Université Jean Monnet & CNRS, Saint-Étienne

Date de début : Février 2025

Contexte

Le processus de standardisation de la **cryptographie post-quantique**, initié par le NIST [1] en 2016, a pour objectif de définir de nouveaux standards pour l'échange de clés et la signature numérique dont la sécurité n'est pas menacée par l'existence d'un ordinateur quantique de capacité suffisante. Cela a abouti à la standardisation de plusieurs algorithmes en juillet 2024. Un processus additionnel est en cours pour les signatures numériques. La majorité des algorithmes sélectionnés fonde sa sécurité sur des problèmes difficiles en théorie des réseaux euclidiens, ou *lattices*. De nombreux travaux de recherche ont étudié la difficulté de ces problèmes, et l'on dispose à présent d'un inventaire important de problèmes réputés plus ou moins difficiles.
Néanmoins, la plupart de ces études ne prennent pas en compte l'information supplémentaire qui pourrait être obtenue par la réalisation d'**attaques physiques** sur des implémentations de ces cryptosystèmes dans des circuits électroniques. En effet, de nombreux travaux ont montré que des attaques physiques, par observation des canaux auxiliaires ou par injection de fautes, permettent d'obtenir davantage d'information que la connaissance des valeurs d'entrée et de sortie du cryptosystème.
Nous voulons donc étudier la possibilité d'exploiter ces informations supplémentaires, obtenues par des attaques physiques, en vue de réduire la sécurité du cryptosystème en passant du problème difficile initial à une instance ou à un problème connexe plus simple.

Objectifs

Les objectifs de ce stage sont :

- de hiérarchiser par difficulté les problèmes connus sur les réseaux euclidiens et leurs différentes instances,
- d'étudier les possibilités de descendre dans cette hiérarchie en exploitant des informations supplémentaires obtenues par des attaques physiques,
- de réaliser des attaques physiques pour valider leur faisabilité en pratique.

Ces objectifs seront discutés et pourront évoluer selon le profil et les préférences de l'étudiant·e retenu·e.

Profil recherché

Nous recherchons un·e étudiant·e disposant de connaissances en cryptographie et présentant un intérêt pour le domaine de la sécurité matérielle. Une poursuite en doctorat à l'issue du stage pourra être envisagée.

Informations pratiques

Lieu Laboratoire Hubert Curien, Saint-Étienne (télé-travail partiel envisageable)

Rémunération Indemnité de stage d'environ 600€/mois, prise en charge de 50% des frais de transport pour les trajets en transports en commun (tram, bus, train, etc).

Date de début souhaitée Février 2025

Durée Jusqu'à 6 mois

Candidature

Pour déposer votre candidature à ce stage, envoyez un CV à {b.colombier; pierre.louis.cayrel}@univ-st-etienne.fr

1. National Institute of Standards and Technology