DEMI-JOURNÉE SCIENTIFIQUE

Cryptographie post-quantique

Avancées scientifiques et pratiques

Mercredi
3 avril 2024

14 H - 18 H

Inscriptions

Bâtiment IRIT
Auditorium
Jacques HERBRAND
Université Toulouse III - Paul Sabatier
TOULOUSE

ICO
Institut Cybersécurité Occitanie

cnrs

La Région Occitanie
Pyrénées - Méditerranée

PROGRAMME

14:00 - 14:15 *Accueil - Introduction*

14:15 - 15:00 **KATHARINA BOUDGOUST**
(CNRS, LIRMM)

"A gentle introduction to lattice-based cryptography"

BIO: Katharina Boudgoust is a CNRS researcher affiliated with the ECO team in Montpellier, France. Prior to this, she completed a two-year postdoctoral position at Aarhus University, Denmark, hosted by Peter Scholl. In 2021, Katharina finished her PhD in Rennes, France, under the supervision of Adeline Roux-Langlois and Pierre-Alain Fouque. She is broadly interested in lattice-based cryptography, and more specifically in the computational hardness assumptions underlying lattice-based cryptosystems. In the last few years, she also researched advanced signature and encryption schemes based on lattices. Katharina is involved in several communities to foster inclusion and diversity in our research community, for instance by organizing seminars and virtual coffee break with the Women in Cryptography group.

ABSTRACT: Lattice-based cryptography is a rather recent research area which attracted a lot of interest in the last years. In particular through the encryption scheme Kyber and the two signature schemes Dilithium and Falcon, all three selected by NIST for standardization and all basing their security on lattice problems. But what exactly do we mean by lattice-based cryptography? The goal of today's talk is to give a gentle introduction to this exciting research field. We will see a (small-dimensional) lattice, what the hard problems are in this domain and how we can use them to build encryption schemes. We will conclude with a personal outlook of interesting open research questions.

PROGRAMME

15:00 - 15:45 — **CARLOS AGUILAR MELCHOR** (SANDBOXAQ)

"La transition à la cryptographie post-quantique, fardeau ou aubaine ?"

BIO: Carlos Aguilar Melchor is the Chief Scientist in Cybersecurity at SandboxAQ. During his career, he has been a professor for 15 years and worked for multiple international organizations, contributing to a variety of domains such as cryptography, privacy, cybersecurity and artificial intelligence.

RÉSUMÉ: Face aux avancées techniques en informatique quantique, de nombreux acteurs pensent que la cryptographie actuelle est en danger et doit être remplacée. De nombreuses directives nationales dans le monde demandent la mise en place d'une transition vers une cryptographie résistant aux ordinateurs quantiques communément appelée «Cryptographie Post Quantique». Dans cet exposé nous parlerons de la transition à la cryptographie post-quantique, de la situation actuelle, de ses difficultés et des opportunités qu'elle apporte.

15:45 - 16:00 — *Pause café*

16:00 - 16:45 — **MARC JOYE** (ZAMA)

"Chiffrement complètement homomorphe : Opportunités et défis"

BIO: Marc Joye est cryptographe et directeur scientifique (Chief Scientist) à Zama. Il est actif dans le domaine de la cryptographie depuis plus de 25 ans, depuis les implémentations bas niveau jusqu'à la conception de protocoles cryptographiques haut niveau. Avant de rejoindre Zama en 2020, Marc a travaillé pour plusieurs entreprises de sécurité (Gemplus, Thomson, Technicolor, NXP, OneSpan), en Europe et aux Etats-Unis. Il est détenteur d'un doctorat en cryptographie de l'UC Louvain et est un Fellow de l'IACR.

PROGRAMME

RÉSUMÉ: Le chiffrement complètement homomorphe est une primitive cryptographique permettant de faire des calculs sur des données chiffrées sans avoir à déchiffrer au préalable. Cette propriété remarquable permet le développement d'applications autrement impossibles à réaliser. De nombreuses avancées scientifiques et technologiques ont eu lieu depuis la première percée de Gentry en 2009. Dans cet exposé, nous ferons un tour des opportunités et de certains défis à court terme et à plus long terme liés au déploiement du chiffrement complètement homomorphe.

16:45 - 17:30 **Présentations courtes de travaux récents dans le domaine de la cryptographie post-quantique**

17:30 - 18:00 ***Discussion générale - Conclusions***

LIRMM

IRIT Institut de Recherche en Informatique de Toulouse
CNRS - Toulouse INP - UT3 - UT Capitole - UT2

ICO Institut Cybersécurité Occitanie

LAAS CNRS

cnrs

La Région Occitanie Pyrénées - Méditerranée

CONTACT

bureau@ico-occitanie.fr