FOUNDATIONS AND APPLICATIONS OF LATTICE-BASED CRYPTOGRAPHY
SPEAKER ABSTRACTS

Damien Stehlé (ENS Lyon)
Introduction to lattice-based cryptography

Lattice-based cryptography is one of the most mature approaches to post-quantum cryptography. It also allows for many advanced constructions, such as fully homomorphic encryption. In this introductory lecture, I will cover the main intractability assumptions underlying lattice-based cryptography, and elementary constructions. In particular, I will present the Short Integer Solution problem (SIS) and the Learning with Errors problem (LWE). I will then describe (i) the public key encryption scheme of Lyubashevsky, Palacio and Segev, whose security relies on the presumed hardness of LWE, and (ii) Lyubashevsky's digital signature scheme, whose security relies on the presumed hardness of SIS. I will cover lattice problems arising from algebraic number theory, which allow for faster and more compact cryptographic constructions.

Alice Pellet-Mary (CNRS and Bordeaux University)
Algebraic lattices for cryptography

In the first talk, we will review some number theoretic results and define algebraic lattices (i.e., ideal and module lattices). We will then discuss about algorithmic problems restricted to these algebraic lattices, and how they can be used for cryptography.

The second talk will be dedicated to attacks that are using the algebraic structure to target specifically algebraic lattices, such as S-unit attacks or subfield attacks.

Martin Albrecht (Royal Holloway, University of London)
Solving the Learning with Errors Problem

In this talk I will discuss algorithms for solving the Learning with Errors problem and their performance.

Ilaria Chillotti (ZAMA)

Introduction to FHE and the TFHE scheme

Fully Homomorphic Encryption (FHE) is a new technology allowing to perform computations over encrypted data. Since the first solution was proposed in 2009, the research has done huge steps forward: operations that were realizable in the order of hours or even days of computation, nowadays can be performed in a matter of milliseconds.

FHE is mainly interesting in this moment because it represent a powerful solution to solve many problems related to the privacy of sensitive data: medical, financial, genomic, and so on.

This data already circulates on the internet, but is only encrypted in transition or when it is stored on a server. However, in order to be manipulated, it needs to be decrypted. With FHE, data could remain encrypted end-to-end, so privacy would be protected and the functionalities offered by service providers still ensured.

Many FHE schemes have been proposed in the literature and are implemented. In particular the ones that are mainly studied and used at the moment are the ones based on the hard lattice problem LWE, which is one of the most promising solution for the post-quantum era.
This talk is going to be split in 2 major parts:

- *In the first part we will introduce FHE in general and we will do an overview of existing schemes and their implementations.*
- *In the second part, we give more details on the scheme BGV and then we will focus on the scheme TFHE, by also showing some applications and experimental results.*

Anamaria Costache (Norwegian University of Science and Technology)
Challenges and open problems in Fully Homomorphic Encryption

In this talk I will start by giving a flavour of how the main FHE schemes work. Then, I will talk about their various trade-offs, the main challenges and open problems in FHE.

Chloe Martindale (University of Bristol)
Isogeny-based cryptography: why, how, and what next?

We will motivate and introduce isogeny-based cryptography, another method of securing communication in a post-quantum world. We will discuss the differences, pros, and cons with respect to lattice-based cryptography from the perspective of real-world applications, give an introduction to the main protocols in isogeny-based cryptography, and finally discuss some important directions for research in the field.

Luca De Feo (IBM Research Europe)
Unexpected discoveries and challenges in isogeny based cryptography

Isogeny based cryptography is a novel branch of post-quantum cryptography that tends to produce bandwidth-efficient-but-computationally-intensive systems for key exchange and signature, and has a certain aura of coolness too. Is there anything else to it?

In this talk, I will review some of the more unusual and less discussed aspects of isogeny based cryptography: from proving isogeny statements in zero-knowledge, to instantiating password-authenticated key exchange, I will highlight some of the unique obstacles that appear when trying to translate pre-quantum protocols to the isogeny setting, and how they may be, sometimes, overcome.

Updated on Tuesday 28th June 2022.