Foundations and Applications of Lattice-based Cryptography
Lightning Talks – Session One (Monday)

Katharina Boudgoust (Aarhus University, Denmark)
How to make crypto events safe and more inclusive?
The IACR has initiated in 2018 a Code of Conduct and refers to the Ethics Committee and a Code of Conduct Liaison person in order to report any incidents that violate this code. However, only very few incidents have been reported since then and we are wondering how to improve the current situation. Because we all know, no reporting does by no means mean no incidents.How do we create inclusive and safe environments at crypto events? In the five minutes, I would mainly try to make people aware of the problem and encourage people to think about it and help us find ideas.

Sergi Rovira (Universitat Pompeu Fabra, Spain)
An overview of current key-switching techniques in Multikey and Multiparty FHE
This short talk is focused on the current key-switching (also known as relinearization) methodology used in the multikey/multiparty fully homomorphic encryption setting. We will explain how this technique works and discuss some open problems and applications.

Hans Heum (Simula UiB, Norway)
A better model of imperfect correctness
Lattice-based schemes often suffer a small likelihood of decryptions failing. Thins is usually modelled as epsilon-correctness, a relaxation of perfect correctness in which correctness is only required to hold up to high probability. Here, the probability is taken over both key generation and the randomness used in encryption. By splitting rather splitting up this probability into one for key generation and one for encryption, each with an associated parameter, we get a more fine-grained model of imperfect correctness, allowing for further trade-offs when deriving system parameters.

Ethan Lee (University of New South Wales Canberra, Australia)
Safe primes and primes represented by polynomials

Sieve methods enable us to deduce information about the number of primes represented by polynomials, hence about primes which are safe to use in cryptosystems. I will talk about the information we can presently deduce about primes represented by an irreducible polynomial using sieve methods, and what results could be possible in the future.

Fuchun Lin (Imperial College London, UK) - ZOOM
Geometrical View on Algebraic LLL for Module Lattices
We initiate a geometrical-perspective analysis on algebraic LLL-reduced bases of module lattices and identify a geometric property of the base ring, over which the modules are defined, that governs whether an algebraic LLL-reduced basis admits a provable Hermitian style bound.

Algebraically size-reducing a rank one sub-module using another rank one sub-module is interpreted as size-reducing a basis of an ideal lattice by subtracting a basis of another ideal lattice transformed by an integer matrix. This interpretation reveals a hidden role of the principal angles between two liner spaces spanned by two ideal lattices in evaluating the effectiveness of the algebraic size-reduction.

Lightning Talks – Session Two (Wednesday)

Thinh Pham (University of Bristol, UK)

RISC-V ISEs research framework for cryptography

The talk will briefly present an in-progress research framework for a cryptographic developer to optimise the performance of cryptographic algorithms on the RISC-V architecture. This work is keen on promoting cryptographic implementations for an open instruction set architecture, and the usage of custom instructions that could untie the consideration of cryptographic algorithm design for performance optimisation against a specific instruction set architecture.

Tjerand Silde (NTNU, Norway)

Lattice-based zero-knowledge proofs for post-quantum cryptographic voting

Cryptographic voting protocols have recently seen much interest from practitioners due to their (planned) use in countries such as Estonia, Switzerland and Australia. Many organizations also use Helios for elections. While many efficient protocols exist from discrete log-type assumptions, the situation is less clear for post-quantum alternatives such as lattices. This is because previous voting protocols do not carry over easily due to issues such as noise growth and approximate relations. In particular, this is a problem for tested designs such as verifiable mixing and decryption of ballot ciphertexts.

In this work, we make progress in this direction. We propose a new verifiable secret shuffle for BGV ciphertexts as well as a compatible verifiable distributed decryption protocol. The shuffle is based on an extension of a shuffle of commitments to known values which is combined with an amortized proof of correct re-randomization. The verifiable distributed decryption protocol uses noise drowning for BGV decryption, proving correctness of decryption steps in zero-knowledge.

We give concrete parameters for our system, estimate the size of each component and provide an implementation of all sub-protocols. Together, the shuffle and the decryption protocol are suitable for use in real-world cryptographic voting schemes, which we demonstrate with a prototype voting protocol design.

Akira Takahashi (Aarhus University, Denmark)

MuSig-L: Lattice-Based Multi-Signature With Single-Round Online Phase

Multi-signatures are protocols that allow a group of signers to jointly produce a single signature on the same message. In recent years, a number of practical multi-signature schemes have been proposed in the discrete-log setting, such as MuSig2 (CRYPTO'21) and DWMS (CRYPTO'21).

The main technical challenge in constructing a multi-signature scheme is to achieve a set of several desirable properties, such as (1) security in the plain public-key (PPK) model, (2) concurrent security, (3) low online round complexity, and (4) key aggregation. However, previous lattice-based, post-quantum counterparts to Schnorr multi-signatures fail to satisfy these properties.

In this paper, we introduce MuSigL, a lattice-based multi-signature scheme simultaneously achieving these design goals for the first time. Unlike the recent, round-efficient proposal of Damgård et al. (PKC'21), which had to rely on lattice-based trapdoor commitments, we do not require any additional primitive in the protocol, while being able to prove security from the standard module-SIS and LWE assumptions. The resulting output signature of our scheme therefore looks closer to the usual Fiat--Shamir-with-abort signatures.

Joint work with Cecilia Boschini and Mehdi Tibouchi. To appear in CRYPTO'22.

Christopher Battarbee (University of York)

Cryptographic Implications of the Telescoping Equality

Since 2013 there has been some cryptographic research on the development and cryptanalysis of a group-theoretic generalisation of Diffie-Hellman key exchange known as Semidirect Product Key Exchange. We detail the destructive power and limitations of an equation inherent to this type of scheme, known as the telescoping equality.

Valerio Cini (AIT Austrian Institute of Technology)

The k-R-ISIS assumption

In this talk I will present a new family of lattice-based computational assumptions, denoted k-Ring-Inhomogeneous Short Integer Solution (or k-R-ISIS for short), which naturally generalizes the standard Short Integer Solution (SIS) assumption, and discuss known reductions to other computational problems. This assumption has been introduced in the paper "Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable", which is a joint work with Martin R. Albrecht, Russell W. F. Lai, Giulio Malavolta, and Sri AravindaKrishnan Thyagarajan, where a lattice-based vector commitment scheme supporting openings to constant-degree polynomial maps, and a lattice-based SNARK have been constructed whose security relies on the k-R-ISIS assumption.

Sarra Talbi (University of science and technology Houari Boumediene, Algérie) - ONLINE

The average hull dimension of cyclic codes over finite rings

I will give the characterization of the hull of cyclic codes in term of their generator polynomials over finite rings. I will also establish the average q−dimension of the hull of cyclic codes of length n over R. The formula for the average q−dimension of the hull of cyclic codes of length n over R will be derived.

https://files.smartsurvey.io/2/1/3IMI125U/191292402_16505527_2308773.pdf

---