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.