MAX PLANCK INSTITUTE
FOR MATHEMATICS

Conference on ”The Mathematics of Post-Quantum Cryptography”

Program

Wed, 04 Dec 2024

12:00 - 13:00	**Registration**
13:00 - 13:20	MPIM Lecture Hall **Welcome and Introduction**
13:20 - 14:20	MPIM Lecture Hall Wouter Castryck (KU Leuven) **Interpolating isogenies between elliptic curves: destructive and constructive applications**
14:25 - 15:10	MPIM Lecture Hall Peter Stevenhagen (Leiden University) **Lattices in Number Theory**
15:15 - 16:00	MPIM Lecture Hall Leo Ducas (Centrum Wiskunde and Informatica, and Leiden University) **Principles of Lattice Cryptography, and cryptanalysis by lattice reduction**
16:00 - 16:30	MPIM Tea Room **Tea and Coffee Break**
16:40 - 17:25	MPIM Lecture Hall Monika Trimoska (Eindhoven University of Technology) **Algebraic cryptanalysis applied to equivalence problems**
17:30 - 18:30	MPIM Lecture Hall **Problem Session**
19:00 - 21:00	**Conference Dinner with subsequent discussion round**

Thu, 05 Dec 2024

09:00 - 09:45	MPIM Lecture Hall Hugues Randriam (ANSSI) **The syzygy distinguisher**
09:45 - 10:30	MPIM Lecture Hall Sabrina Kunzweiler (Inria Bordeaux and Université de Bordeaux) **Isogeny-based group actions in cryptography**
10:30 - 11:00	MPIM Tea Room **Tea and Coffee Break**
11:00 - 11:40	MPIM Lecture Hall Aurel Page (Inria Bordeaux and Université de Bordeaux) **Hardness of isogeny problems and equidistribution**
11:40 - 14:05	**Lunch Break**
14:05 - 14:50	MPIM Lecture Hall Severin Barmeier (University of Cologne) **Utility and usability of projective resolutions**
15:00 - 16:00	MPIM Lecture Hall Wessel van Woerden (Oberseminar) (University of Bordeaux) **Dense and smooth lattices in any genus**
16:00 - 16:30	MPIM Tea Room **Tea and Coffee Break**

Abstracts

Wouter Castryck

Interpolating isogenies between elliptic curves: destructive and constructive applications

A degree-d isogeny $\Phi : E \longrightarrow E'$ between elliptic curves is always uniquely determined by the images of any $4d + 1$ points $P \in E$. In a series of recent(ish) works, this statement was made algorithmically effective: given any point $Q \in E$, we now understand how to efficiently compute its image $\Phi(Q)$ from such interpolation data (over finite fields, and assuming that the interpolation points generate a group of smooth order). We will explain this method, in which higher-dimensional abelian varieties play a surprising role. We will then discuss SIKE, a candidate for post-quantum key exchange that had advanced to round 4 of a standardization effort run by NIST, and show why it is naturally broken by isogeny interpolation. Finally, as time permits, we will discuss various constructive applications.

Peter Stevenhagen

Lattices in Number Theory

I will define lattices and discuss some of their basic properties, including Minkowski's theorem on lattice points in convex bodies. In the setting of algebraic number theory, I will explain how number rings and their ideals come with a natural embedding as lattices in Euclidean spaces.

Leo Ducas

Principles of Lattice Cryptography, and cryptanalysis by lattice reduction

In this presentation, I will present lattice-based cryptography as stemming from tessellating a Euclidean vector space according using a lattice basis. This directly points at lattice reduction algorithm for cryptanalysis, and I will cover the famous LLL algorithm, and discuss stronger but slower algorithm. If times allow, I will also discuss the special case of ideal lattices of a number field, how the reduction theory differs, and how it can be exploited for attacks and hardness proof.

Monika Trimoska

Algebraic cryptanalysis applied to equivalence problems

In this talk, we first give an introduction to algebraic cryptanalysis, before looking into concrete applications to solving hard problems relevant for cryptography. The examples chosen for this talk are equivalence problems. Broadly, an equivalence problem considers two instances of the same mathematical object and asks if there exists a map between them that preserves some defined property. Two such problems will be looked at in detail. The matrix code equivalence problem takes as input two error-correcting codes in the rank metric and the map we are tasked to find is an isometry that preserves the rank of codewords. The second problem we are interested in is the alternating trilinear form equivalence, where we are given two alternating trilinear forms and the goal is to find an isomorphism between them. We first show how these two problems are similar, namely that an alternating trilinear form can be viewed as a matrix code with special properties, or that a matrix code can be viewed as a trilinear form without the alternating property. We then present some of our results on attacking these problems using tools from algebraic cryptanalysis. The rising interest in equivalence problems is due to their aptness for building a zero-knowledge-based identification scheme which, using the Fiat-Shamir transform, can be turned into digital signature schemes.

Hugues Randriam

The syzygy distinguisher

We present a new distinguisher for alternant and Goppa codes, whose complexity is subexponential in the error-correcting capability, hence better than that of generic decoding algorithms. Moreover it does not suffer from the strong regime limitations of the previous distinguishers or structure recovery algorithms: in particular, it applies to the codes used in the Classic McEliece candidate for postquantum cryptography standardization. The invariants that allow us to distinguish are graded Betti numbers of the homogeneous coordinate ring of a shortening of the dual code. Since its introduction in 1978, this is the first time an analysis of the McEliece cryptosystem breaks the exponential barrier.

Sabrina Kunzweiler

Isogeny-based group actions in cryptography

The hardness of computing discrete logarithms in a prime order group builds the basis of many constructions in cryptography. While there exist efficient quantum algorithms for solving this problem, the situation is different when we consider group actions: Given two elements x, y in a set X, and a group G acting on X, the ”group-action DLOG problem” asks to find a group element $g \in G$ so that $y = gx$ (if it exists). In this talk, the focus will be on group actions that are used in isogeny-based cryptography. In particular, we will discuss different properties that are specific to the group action used in the Commutative Supersingular Isogeny Diffie-Hellman protocol (CSIDH).

Aurel Page

Hardness of isogeny problems and equidistribution

When studying proposed isogeny-based cryptosystems, several computational problems naturally appear: some are upper bounds for the security of the system (if one can solve the problem, then one can break the cryptosystem), some are lower bounds (if one can break the cryptosystem, then one can solve the problem). We would therefore like to understand the relative difficulty of these problems, ideally showing that they are all equivalent. I will explain the proof of one such equivalence, between the supersingular Endomorphism Ring problem (given a supersingular elliptic curve, find all its endomorphisms) and the supersingular One Endomorphism problem (given a supersingular elliptic curve, find one non-scalar endomorphism). The proof uses properties of fast equidistribution in isogeny graphs of supersingular elliptic curves equipped with extra structure, which we prove by going via quaternion algebras and modular forms. This is joint work with Benjamin Wesolowski.

Severin Barmeier

Utility and usability of projective resolutions

Projective resolutions are a standard tool of homological algebra that allow to compute cohomology and associated invariants such as Betti numbers which are used in both abstract contexts and concrete applications. From a theoretical perspective, all projective resolutions are (homotopy) equivalent. Projective resolutions can appear in a wide range of flavours, some more apt for abstract arguments, others more apt for concrete calculations. It is often a change of perspective on the object one is trying to resolve that can make an untractable problem suddenly tractable which I will illustrate in several examples.

Wessel van Woerden (Oberseminar)

Dense and smooth lattices in any genus

The Lattice Isomorphism Problem (LIP) was recently introduced as a new hardness assumption for post-quantum cryptography. The strongest known efficiently computable invariant for LIP is the genus of a lattice. To instantiate LIP-based schemes one often requires the existence of a lattice that (1) lies in some fixed genus, and (2) has some good geometric properties such as a high packing density or a small smoothness parameter. In this talk I will show that such lattices exist. In particular, building upon classical results by Siegel (1935), we will see that essentially any genus contains a lattice with a close to optimal packing density, smoothing parameter and covering radius.