Arithmetic Geometry: Deep Theory, Efficient Algorithms and Surprising Applications

Gerhard Frey, University of Duisburg-Essen

The aim of the talk is to give an overview over a fascinating area of mathematical research, which we shall describe below.

One of the most astonishing success stories in recent mathematics is arithmetic geometry, which unifies methods from classical number theory with algebraic geometry. In particular, an the extremely important role is played by the Galois groups of base schemes like the spectra of rings of integers of number fields or rings of holomorphic functions of curves over finite fields. These groups are the algebraic analogues of topological fundamental groups. Their representations induced by the action on divisor class groups of varieties over these domains yielded spectacular results like Serre's Conjecture for two-dimensional representations of the Galois group of $\mathbb{Q}$, which implies for example the modularity of elliptic curves over $\mathbb{Q}$ and so Fermat's Last Theorem (and much more).
At the same time the algorithmic aspect of arithmetical objects like lattices and ideal class groups of global fields became more and more important and accessible, stimulated by and stimulating the advances in theory. An outstanding result is the theorem of F. Heß and C.Diem yielding that the addition in divisor class groups of curves of genus g over finite fields $\mathbb{F}_q$ is (probabilistically) of polynomial complexity in g (g fixed) and $\log(q)$ (g fixed).

This opens the way to use the discrete logarithm in divisor class groups of curves over finite fields for public key cryptography, e.g. for key exchange, as established by Diffie-Hellman for the multiplicative group of finite fields.
Indeed, one finds fast algorithms for scalar multiplication and point counting (e.g. the algorithm of Schoof-Atkin-Elkies). But, at the same time, these insights yield algorithms for the computation of discrete logarithms that are in many cases "too fast" for security. The good news is that there is a narrow but not empty range of candidates usable for public key cryptography and secure against all known attacks based on conventional computer algorithms: carefully chosen curves of genus 1 (elliptic curves) and hyperelliptic curves of genus ≤ 3 over prime fields.
As result we have a rather satisfying situation of cryptography based on elliptic and hyperelliptic curves–as long as we restrict the algorithms to classical bit-operations. But the possibility of the existence of quantum computers in a not too far future forces to look for alternatives (key word "Shor's algorithm").

Therefore we formulate a rather abstract setting for Diffie-Hellman key exchange schemes, e.g. by using categories for the exchange partners, for which push-outs exist and are computable. To get examples we use results on isogenies of elliptic curves. The theoretical background relies on fundamental results of M. Deuring, the algorithmic aspects are till today in the center of intensive research activities circling around the computation of isogenies. For instance, the security of the schemes we discuss next depends on the difficulty to find explicitly an isogeny between two isogenous elliptic curves.

As first example of a key exchange scheme, which has good chances to have a subexponential complexity under quantum computer attacks is the system of Couveignes-Stolbunov using the isogeny graph of ordinary elliptic curves with fixed endomorphism ring. Its disadvantage is that it is, even in refined versions, slow.

Surprisingly, it seems to be possible to get better results by using supersingular elliptic curves. We present a system due to De Feo and Jao nicely fitting into our categorical frame for which no non-exponential quantum computer attack is known till now and which is pretty efficient. Weakening the security condition "exponential" to "subexponential" and using supersingular elliptic curves defined over prime fields, W. Castryck et. al. design a scheme for key exchange which is very fast and needs only a small key size.