Geometric Galois Representations in Theory and Praxis

Gerhard Frey, University of Duisburg-Essen

1 Diffie-Hellman Key Exchange

One of the important problems of public key cryptography is the key exchange in open channels.
We describe how schemes of Diffie-Hellman type can be used to solve this task.
We begin with the most abstract setting based on categories in which the push out is computable. This will be helpful to understand possible schemes that could be resistant against attacks by quantum computers and which will be discussed in the fourth lecture.
Then we specialize to key exchange schemes using group sets (e.g. $\mathbb{Z}$-sets) and, again as special case, to "classical" key exchange using discrete logarithms in cyclic groups of prime order. This setting is most important for presently used public key systems. It leads to a precise and hard challenge concerning the construction of families of groups providing secure and fast crypto systems.

2 Arithmetic of Galois Representations

In this lecture we shall give a short exposition of the theory and important consequences lying behind the cryptographical applications we have in mind. The central topics are Galois representations and their arithmetic over interesting fields like number fields or finite fields. We explain how Picard groups of curves are used to construct such representations. In particular elliptic curves, their isogenies and attached modular curves and functions become crucial for the study of two-dimensional ℓ-adic Galois representations.
A high point of modern arithmetic geometry is the proof of Serre's conjecture by Khare, Wintenberger, Kisin and many others concerning odd two-dimensional representations, and we shall explain how this implies a five-line proof of FLT.

3 Discrete Logarithms Attached to Picard Groups

Using the results of Lecture 2 we concentrate now on the arithmetic of Picard groups (i.e. divisor class groups) of curves over finite fields. In addition to the theoretical results we can rely on the big advances in the algorithmic theory of such curves, for instance the outstanding result 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 key exchange. 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 public key 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").

4 Isogeny Graphs of Elliptic Curves and Post Quantum Crypto

We come back to the general setting for Diffie-Hellman key exchange schemes explained in the first lecture. For this 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. The "weakness" of subexponential security under quantum operations comes from the fact that we use the structure of a G-set with G commutative (class group of a number field).

This can be avoided if we switch to supersingular elliptic curves whose ring of endomorphisms over $\overline{\mathbb{F}_q}$ is a quaternion algebra, and so, surprisingly, it seems to be possible to get better cryptographical results than by using ordinary elliptic curves. We shall 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. designed a scheme for key exchange which is very fast.