Curves over Finite Fields and Cryptography

Gerhard Frey, University of Duisburg-Essen

In this lecture we shall explain in more detail the topics mentioned in the colloquium talk, in particular we shall discuss how curves over finite fields can be applied to public key cryptography.

After recalling the principles of a Diffie-Hellman key exchange scheme we shall discuss algorithms for addition in divisor class groups $\mathrm{Pic}^0(\mathcal{C})$, where $\mathcal{C}$ is a projective curve over a finite field $\mathbb{F}_q$. Of special interest are elliptic and hyperelliptic curves, and as consequence of the results one can try to use their Picard groups for cryptographic schemes based on discrete logarithms. For this, we have to test the hardness of the computation of the discrete logarithm, and it turns out that a very efficient attack based on index-calculus eliminates all curves of genus ≤ 4 and non-hyperelliptic curves of genus 3. Going further and using an explicit isogeny of Jacobians of hyperelliptic curves of genus 3 we have to exclude "many" hyperelliptic curves of genus 3.

The good news is that the remaining curves (including nearly all curves of genus 1 and 2) are till today "exponentially secure" against all known attacks based on conventional computer algorithms, and since one can solve the point counting task for these curves in cryptographically relevant ranges 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 since the discrete logarithm will have only polynomial complexity (key word "Shor's algorithm").

This opens a new and very interesting area of research. Amongst other proposals the idea of using isogeny graphs of elliptic curves and the hardness to compute explicitly isogenies between elliptic curves (known to be isogenous) leads to key exchange schemes away from discrete logarithms.

We shall present such schemes using ordinary elliptic curves (Couveignes-Stolbunov et.al) (rather slow) and supersingular elliptic curves over prime fields $\mathbb{F}_p$ (W. Castryck et. al) (very fast), which are both of subexponential security. Going to supersingular curves over $\mathbb{F}_{p^2}$ we explain the scheme of De Feo, Jao et.al which is not so fast as Castryck's scheme but has, at our present knowledge, exponential security.