On Galois Representations in Theory and Praxis

Gerhard Frey, University of Duisburg-Essen

One of the most astonishing success stories in recent mathematics is arithmetic geometry, which unifies methods from classical number theory with algebraic geometry ("schemes"). In this context an extremely important role is played by the Galois groups of base schemes like 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, and their representations induced by the action on divisor class groups of varieties over these domains yield 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 becomes 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 (fixed) and $\log(q)$ (g fixed). So one could hope to use such groups for public key cryptography, e.g. for key exchange, as established by Diffie-Hellman for the multiplicative group of finite fields.
But the obtained insights play not only a constructive role but also a destructive role for the security of such systems. Algorithms for fast scalar multiplication and point counting (e.g. the algorithm of Schoof-Atkin-Elkies) make it possible to find divisor class groups in cryptographically relevant ranges but, at the same time, 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.

In the lectures we shall give an overview on the methods and results for the rather satisfying situation of elliptic and hyperelliptic cryptography–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.
Therefore we formulate a rather abstract setting for Diffie-Hellman key exchange schemes using (closely related) categories for the exchange partners, for which push-outs exist and are computable. The DL-systems with cyclic groups are the easiest realizations (and by Shor's algorithm cracked in polynomial time), the next level are G-sets (G a semi group) with a commutativity condition. If G is abelian (e.g. equal to $\mathbb{N}$) then an algorithm of Kuperberg for the hidden shift problem with subexponential complexity can be applied, for general groups no such algorithm is known (but the commutation condition is difficult to realize).
Using fundamental results of M. Deuring about isogenies of elliptic curves we describe the system of Couveignes-Stolbunov for key exchange using the isogeny graph of ordinary elliptic curves with endomorphism ring O, which is a G-set with $G = \mathrm{Pic}(O)$ and so only of subexponential security under quantum computing, and the system of De Feo using supersingular elliptic curves (and nicely fitting into our categorical frame) for which no non-exponential quantum computer attack is known till now.