Polynomial time computation of Galois representations attached to modular forms.

Bas Edixhoven
Universiteit Leiden, Netherlands
edix@math.leidenuniv.nl

Modular forms give rise to number fields with non-solvable Galois groups, acting faithfully on finite subgroups of jacobian varieties of curves. In joint work with Couveignes, de Jong and Merkl, generalised by Bruin, it was shown that these number fields can be computed in polynomial time. The major difficulty is that such computations must be done in time polynomial in the dimension of the jacobian varieties that arise. This difficulty was solved by approximate computations and bounds that allow us to get exact solutions from approximate ones. The bounds will be discussed briefly. We will focus on Couveignes's algorithms for the approximate computations. Finally, real computations by Bosman, Mascot, Zeng, Derickx, van Hoeij and Peng will be presented.

Joint work with Jean-Marc Couveignes (Université Bordeaux 1), Robin de Jong (Universiteit Leiden), Franz Merkl (Universität München) and Peter Bruin (Universiteit Leiden).