Galois Theory and Discrete Logarithms

Gerhard Frey, University of Duisburg-Essen

An important family of crypto primitives is delivered by discrete logarithms (DL-systems) in divisor class groups of curves over finite fields. Both for constructive aspects and for security analysis it is important to understand the background formed by arithmetic geometry. Prominent examples are the results of Diem/Gaudry about efficiency of index-calculus attacks in abelian varieties of low dimension or the existence and use of bilinear structures. This are two examples amongst many others where Galois theory plays a key role, and it is typical that not only the Galois groups of finite fields with the Frobenius automorphism but also those of local fields and even global fields are used both for constructive and destructive aspects of DL-systems. It will be the purpose of the lecture to give a survey of the methods and results in this area.