

# The Arithmetic of Brauer Groups over Global and Local Fields with Applications to Discrete Logarithms

Gerhard Frey  
Institute for Experimental Mathematics  
University of Duisburg-Essen  
frey@exp-math.uni-essen.de

## Abstract

It is well known that Brauer groups are of great importance for the arithmetic of local and global fields. The key word here is class field theory.

In this lecture we want to make evident that Brauer groups of local and global fields play an important role in public key cryptography, too.

Almost all public key crypto systems used today based on discrete logarithms use the ideal class groups of rings of holomorphic functions of affine curves over finite fields  $\mathbb{F}_q$  to generate the underlying groups. In the first part of the lecture we explain how these groups can be mapped to such Brauer groups via the Tate-Lichtenbaum pairing.

This pairing applied to elements of order  $n$  can be computed with complexity polynomial in  $|\mathbb{F}_q(\mu_n)|$  where  $\mu_n$  is the group of roots of unity of order  $n$ . The image under this map leads to cyclic algebras over local fields with residue field  $\mathbb{F}_q(\mu_n)$ .

One of the main results of local class field theory states that the class of such an algebra is determined by its invariant in  $\mathbb{Z}/n\mathbb{Z}$ . Computing this invariant leads in a natural way to the computation of discrete logarithms in finite fields.

Lifting the local algebras to algebras over global fields and using the Hasse-Brauer-Noether-sequence enables us to apply index-calculus methods described in the third part of the lecture.

As result we get subexponential algorithms for the computation of discrete logarithms in finite fields as well as for the computation of the Euler totient function (so we have an immediate application to the RSA-problem), and, as application to number theory, a computational method to “describe” cyclic extensions of number fields with restricted ramification.