The reciprocity laws of algebraic number fields and cryptography

S.V.Vostokov, E.S.Vostokova

Saint-Petersburg state University, faculty of mathematics and mechanics,
Stary Peterhof, University Ave 28, Saint-Petersburg, Russia

sergei.vostokov@gmail.com, lizk.vostokova@gmail.com

We consider local pairings arised in the classical reciprocity laws at the turn of the 20th century and define a new cryptosystem and an electronic signature. Pairings in number fields considered in the present paper first appeared when David Hilbert began to develop Kronecker's idea concerning an analogy between numbers and functions.Hilbert applied this idea to a long-standing problem on the reciprocity law, which consisted in finding an explicit expression for the product of nth power residue symbols in a number field containing all nth roots of 1,

$$f(\alpha,\beta)\in\mathbb{Z} \mod n\mathbb{Z}, \qquad \left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \zeta_n^{f(\alpha,\beta)},$$

In his 9th problem, D. Hilbert suggested to extend the calculations from number fields to the fields of p-adic numbers, i.e. from global fields to local fields. In other words, to make these calculations local, which in essense is an analog of the calculation of the Abelian integral of a differential form on a Riemann surface in terms of residues.

In 1975, a public-key cryptography was invented. As a result, all asymmetric encryption systems appeared later were based on a certain hard-to-calculate problem. Every such a system led to a thorough investigation of the problem providing its security.

The RSA motivated the study of integer factorization, and the Diffie–Hellman protocols and ElGamal cryptosystems drew attention to the discrete logarithm problem. It is not known whether the discrete logarithm or the factorization problem belongs to the class of NP-complete problems, i.e., the problems which are considered to be computationally hard. Moreover, for these problems, there are algorithms running in polynomial time on quantum computers. All this motivates a further search for new computationally hard problems, which could be used for constructing encryption systems.

We propose two new cryptographic system and new electronic signature based on explicit pairing in local fields.