CORR 99-53

Cryptography in quadratic Function Fields

R. Scheidler*

Abstract We describe several cryptographic schemes in quadratic function fields of odd characteristic. In both the real and the imaginary representation of such a field, we present a Diffie-Hellman-like key exchange protocol as well as a public-key cryptosystem and a signature scheme of ElGamal type. Several of these schemes are improvements of systems previously found in the literature, while others are new. All systems are based on an appropriate discrete logarithm problem. In the imaginary setting, this is the discrete logarithm problem in the ideal class group of the field, or equivalently, in the Jacobian of the curve defining the function field. In the real case, the problem in question is the task of computing distances in the set of reduced principal ideals, which is a monoid under a suitable operation. Currently, the best general algorithms for solving both discrete logarithm problems are exponential (subexponential only in fields of high genus), resulting in a possibly higher level of security than that of conventional discrete logarithm based schemes.