CORR 99-09

Catching Kangaroos in Function Fields

Andreas Stein, Edlyn Teske

Introduction In this paper we generalize the parallelized lambda method for computing invariants in real quadratic function fields.

A basic such invariant is the regulator, which plays an important role in cryptosystems based on real quadratic function fields. For example, in the key-exchange protocol by Scheidler, stein and Williams [SSW96], the regulator provides a measure for the key space; moreover, computation of the regulator is an instance of solving the discrete logarithm problem in real quadratic function fields.

Pollard's lambda method [Pol78], also called the method of catching kangaroos, was originally developed to compute discrete logarithms in $\mathbb{Z}/p\mathbb{Z}$ and has been canonically generalized to solve the discrete logarithm problem in any finite abelian group. The key ingredient for the lambda method is that we know that the discrete logarithm lies in a given interval $[a, b[$; then the expected running time is $O(\sqrt{b-a})$ group operations. Van Oorschot and Wiener [vOW99] have shown that the lambda method can be parallelized with linear speed-up, which makes the method attractive for distributed attacks. It is important to note that the lambda method is very space efficient, which is its basic advantage over square-root attacks based on Shanks' baby step-giant step method.

The objects with which we deal in real quadratic function fields are reduced principal ideals, which do *not* constitute a group. However, the baby step-giant step method could be efficiently adapted to this setting by defining analogues of baby steps and giant steps that make use of the ideal arithmetic (see [SZ91]). the disadvantage of this method is that the space restrictions of the machines constitute a bound on how large regulators can be computed. Currently, this bound is at about 25 digits ([SW98]). It is therefore natural to ask whether such a space efficient method as the lambda method can be

employed to real quadratic function fields. In this paper we show that this indeed can be done. This allows us to push the range for regulator computation much further. In fact, we estimate that with the parallelized Pollard lambda attack on a network of 40 fast machines, a 31-digit regulator can be computed within a week.

In the following, we first give an overview of the lambda method and its parallelization, where we deal with both the variant of van Oorschot and Wiener [vOW99] and Pollard [Pol]. We keep this exposition as general as possible. Since no experimental results with the parallelized lambda method (not to mix with the parallelized rho method!) have been published so far, we also include some statistics about experiments with elliptic curve groups showing that the practical performance essentially matches the theoretical predictions. Then, in Section 3, we give the basic definitions and facts needed about real quadratic function fields. In Section 4 we specialize the lambda method for the problem of regulator and class number computation in function fields and give experimental results. For the full version of this paper, we refer to [ST].