Abstract

The talk will focus on two problems: The discrete logarithm problem(DLP) and the class group computation problem. Besides the inherent mathematical appeal, both of these problems have strong cryptographical interest.

1. Discrete Logarithm Problem

The computation of discrete logarithms is known to be a hard problem in general. The intractability of the discrete logarithm problem has lead to schemes that revolutionized cryptography. The known algorithms for DLP can be categorised into two major categories, namely, generic algorithms which work in any group and index calculus algorithms which work in a special class of groups.

It is known that Pollard's rho algorithm is the best generic algorithm to compute discrete logarithm. The complete discrete logarithm in a finite field is found by applying Pollard's rho in subproblems that may arise when index calculus algorithms are applied. The tag tracing variant of Pollard's rho is a highly efficient algorithm.

We have intertwined the technique of Montgomery multiplication with tag tracing in fields of prime order. As a result, the expensive modular reductions are completely replaced by divisions by a suitable power of two. The implementation of these divisions is a cakewalk as it is just right shift operations. In doing this, we do not compromise with any advantage that tag tracing offered. The essential difference is instead of doing field multiplication after a certain number of steps we just do a Montgomery multiplication after the same number of steps. The net result of our work is that the speedup is huge without any additional costs of memory or time.

We next focus on general medium prime fields. We perform a record discrete log computation for a field with 22-bit characteristic and 1051-bit size. It successfully combats the challenge to perform a larger discrete logarithm computation for a medium prime case field than what had been reported earlier with- out losing generality. The work also reports progress in discrete logarithm computation for the general medium prime case using the function field sieve algorithm. Fields considered earlier with large sizes en- joyed the advantage offered by the Kummer extension property. This made the factor base size small and 2 ?? 1 descent which is one of the last steps of the index calculus technique easier. In our case, the factor base is larger than what has been considered earlier. The difficulty of 2??1 descent is also clearly visible. An increase in the size of the field makes various steps of the function field sieve more complicated. Our study delves into these difficulties. The linear algebra step along with descent form the main stumbling blocks. Some previously known techniques have been analysed and implemented efficiently. The manner in which the various methods are used in our work is equally applicable for any general medium prime field for performing future record computations, provided suitable computational resources are present.

We next consider the problem of computing discrete logarithms with function field sieve in Fpn for a small characteristic p and composite n. The last phase of the function field sieve, namely the individual logarithm step itself again consist of two sub-steps of initial splitting and descent. The focus in this work is on the initial splitting phase.

We have proposed a new algorithm for initial splitting in small characteristic fields of composite extension degree. It has been shown to be better than the other existing algorithms like Waterloo algorithm and Guillevic's initial splitting algorithm. Implementation of the new algorithm has also been done. Our algorithm reduces the cost of generation of polynomials which are to be tested for smoothness. Additionally, our algorithm is completely parallelizable compared to some sort of semiparallelism possible for Guillevic's algorithm. The usage of this algorithm is appropriate when attempting record discrete logarithm computations over such fields.

2. Class Group Computation

The class group computation problem is quite important and relevant as it provides information about the structure of multiplication in the field. However, computationally it remains a difficult problem to date. Class group computation is one of the four major problems in computational algebraic number theory postulated by Zassenhaus (the others being computation of unit group, ring of integers, Galois group). Class groups are important both mathematically as well as cryptographically.

We have introduced a technique to obtain practical speed-up for relation collection phase when index calculus technique is used to compute class groups. We have done Magma implementations of both the new algorithm as well as the previous one given by Gelin. Timing results confirm that there is indeed a substantial practical speed-up in relation collection by the new algorithm over Gelin's algorithm. In particular, experiments were done for degrees 10; 15; 20; 25 with discriminant size 63; 81; 157; 256 bits re- spectively. It has been seen in all these cases that the time required by Gelin's technique was about 2:86 to 3:39 times more. This suggests that practically our algorithm is about three times faster than Gelin's method in these cases though the asymptotic costs are the same. Our algorithm could also successfully compute a large number of relations for the bigger fields.

The talk will be concluded by pointing some future research directions.