Number Field Sieve over GF(p) of Low Hamming Weight Characteristic

Abstract

The security of the digital signature algorithm (DSA) and Diffie-Hellman key exchange is based on the difficulty of the discrete logarithm problems (DLP) over prime field GF(p), and thus it is important to evaluate the difficulty of DLP over GF(p) for discussing the security of these protocols. The number field sieve (NFS) is asymptotically the fastest algorithm to solve DLP over GF(p). NFS was first proposed by Gordon and then it was improved by Schirokauer and Joux-Lercier. On the other hand, Schirokauer presented a new variant of NFS, which is particularly efficient for the characteristic p with low weight (p has a signed binary representation of low Hamming weight). In this talk, we compare the running time of the NFS using the polynomials by Joux-Lercier (JL03) and Schirokauer (Sch06) with respect to low weight primes of 194-bit, and up to 259-bit. Sch06 is about 4, 8, or 18 times faster than JL03 for 146-bit, 192-bit, or 259-bit, respectively. Our experiment was carried out on two Xeon E5440 CPU using gcc, pthread and GMP.