The Number Field Sieve : Tower, Factory and automorphisms

Cécile Pierrot

The security of currently deployed public key protocols relies on the presumed hardness of problems often coming from number theory, such as factoring a large integer or solving the discrete logarithm problem in some group. While cryptographers are working hard to build post-quantum protocols, these cryptosystems coming from the 70's are still in widespread use.
We focus on discrete logarithms in finite fields and particularly on the Number Field Sieve (NFS), THE algorithm to solve the related problem. This talk deals with two variants of NFS, the Tower variant, that permitted to reach the last discrete logarithm record in a finite field GF(p^6), and the Factory variant, that is designed to accelerate the computation when several key targets are living in several different finite fields of the same order of magnitude. We also discuss the practical interest of using automorphisms in the underlying finite fields of the diagram.

This presentation is the result of several articles carried out in collaboration with Haetham Al Aswad, Gabrielle De Micheli, Pierrick Gaudry and Emmanuel Thomé.