

Nouveau record de calcul du logarithme discret dans les corps finis

Écrit par Administrator
Vendredi, 22 Mars 2013 18:40 -

Antoine Joux annonce un nouveau record de calcul du logarithme discret sur un corps fini:

"We are pleased to announce a new record for the computation of discrete logarithms in finite fields. We were able to compute discrete logarithms in $GF(2^{4080})$ using about 14100 CPU.hours. This computation was performed using the same index calculus algorithm as in our recent computation [Jo13]. A draft describing the algorithm is available as [Jo13a]."

[Jo13a] A new index calculus algorithm with complexity $L(1/4+o(1))$ in very small characteristic. Eprint Archive. <http://eprint.iacr.org/2013/095>