

La guerre des records sur les logarithmes discrets

Écrit par Administrator

Lundi, 22 Avril 2013 13:30 - Mis à jour Lundi, 22 Avril 2013 13:46

Après le record annoncé par A. Joux, voici un nouveau record de Faruk Gologlu, Robert Granger, Gary McGuire et Jens Zumbagel :

"We are very pleased to announce a new record for the computation of discrete logarithms in finite fields. In particular, we were able to compute discrete logarithms in the field $GF(2^{6120})$ in only 749.5 core-hours. As far as we are aware, the previous record for discrete logarithms in binary fields was in $GF(2^{4080})$ (ndldr : celui d'Antoine Joux dont on a parlé précédemment).

This computation was performed using a hybrid index calculus algorithm, combining our polynomial time relation generation method for degree 1 elements of the extension $GF(2^{6120}) / GF(2^{24})$, an enhanced variant of our polynomial time degree 2 elimination method from the same paper, an analogue of Joux's elimination method for other small degrees, and a variant of classical descent for all higher degrees."

On peut voir l'annonce [ici](#) .

Ces auteurs avaient établi précédemment un record de 1971 bits (voir l'article [ici](#)).