

Nouveau record DLP sur une courbe elliptique

Écrit par Administrator

Mercredi, 30 Septembre 2009 16:20 - Mis à jour Samedi, 02 Janvier 2010 16:25

Une équipe de chercheurs vient de calculer un logarithme discret sur une courbe elliptique sur un corps fini premier F_p où le nombre premier p a 112 bits. On pourra trouver les détails sur [le site des chercheurs](#)

. Le calcul a été effectué au "laboratory for cryptologic algorithms" de l'Ecole Polytechnique Fédérale de Lausane (EPFL).