

# Attaques par recouvrement et décomposition du logarithme discret sur courbes elliptiques

Vanessa Vitse (Versailles-St Quentin)

Résumé :

Le problème du logarithme discret sur courbes elliptiques (définies sur corps finis) est à la base de nombreux protocoles cryptographiques, considérés comme sûrs dans la mesure où on ne connaît en général pas d'algorithmes permettant de les attaquer efficacement. Dans le cas où la courbe est définie sur des extensions de corps finis, il existe néanmoins des menaces théoriques basées sur la restriction de Weil et le calcul d'indices. On présente dans cet exposé un algorithme combinant transfert par recouvrement et méthodes de décompositions, qui permet d'attaquer le problème du logarithme discret sur courbes elliptiques définies sur des extensions de degré composé. En particulier, on donnera un exemple concret d'application à un sous-groupe de taille 150 bits d'une courbe définie sur  $\mathbb{F}_{p^6}$ , a priori résistant à toute autre attaque connue.