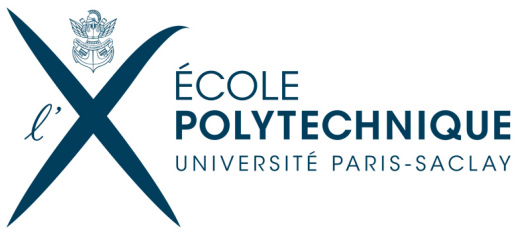
Attaque de Sidelnikov-Shestakov appliquée au cryptosystème de Chor-Rivest

INF 581 - Enseignement d'Approfondissement
D. Augot

Sylvain Colin & Gaspard Férey

Département d'Informatique
Ecole Polytechnique, France

16 Décembre 2013



Cryptosystème de McEliece utilisant les codes de Reed-Solomon

Du texte

- un point

Attaque de Sidelnikov et Shestakov

Le cryptosystème de Chor-Rivest

Attaque de Vaudenay améliorée

Simulations et complexité espérée