Sur les générateurs pseudo aléatoires linéaires

Florette Martinez*[1]

[1]LIP6 – Sorbonne Universite, Centre National de la Recherche Scientifique, Centre National de la Recherche Scientifique : UMR7606 – France

Résumé

Plusieurs générateurs de nombres pseudo aléatoires sont fortement linéaires, ce qui leur donne une très grande rapidité. Certains sont basés sur le generateur congruentiel linéaire, d'autres sur des hypothèses plus solides comme le problème du sac à dos. Dans les deux cas il existe des attaques, en particulier s'aidant de réseaux euclidiens, qui permettent de retrouver la graine de ces générateurs sur de larges plages de paramètres.

*Intervenant