Calcolo di multipli di peso basso di polinomi binari attraverso il logaritmo discreto

Claudia Tinnirello

Abstract

Calcolare in modo efficiente multipli di peso basso di polinomi binari è spesso l'elemento chiave degli attacchi di correlazione a Stream Ciphers realizzati mediante Linear Feedback Shift Register (LFSR).
Nel talk verrà presentato un approccio alternativo a quello basato sul problema del compleanno generalizzato sviluppato da David Wagner, che utilizza il logaritmo discreto in un campo finito. Tale approccio produce un algoritmo con una memory complexity più bassa ed una time complexity comparabile all'algoritmo basato sul problema del compleanno generalizzato.