Construcción de Trinomios de Permutación sobre Cuerpos Finitos.

Christian A. Rodríguez
Alex D. Santos
Universidad de Puerto Rico
Recinto de Río
Departamento de Ciencia de Cómputos

21 de marzo de 2014

Resumen

Dado un trinomio de la forma $f_{a,b}(X) = X^r(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$ sobre un cuerpo finito $\mathbb{F}_q$ con tamaño de value set s, construímos $d = lcm(d_1, d_2)$ otros trinomios en $\mathbb{F}_q$ con el mismo tamaño de value set. En particular, dado un polinomio de permutación de la forma $f_{a,b}$, construímos $d = lcm(d_1, d_2)$ otros polinomios de permutación en $\mathbb{F}_q$. También construímos secuencias $P_{q^{m_1}}, P_{q^{m_2}}, \cdots$, donde $P_{q^{m_i}}$ es un polinomio de permutación en $\mathbb{F}_{q^{m_i}}$.