Abstract of Ph. D Thesis Presented to the Graduate School
of the University of Puerto Rico, Río Piedras Campus in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy in Mathematics

Linear recursivity of exponential sums of symmetric functions over Galois Fields

By

Leonid Brehsner Sepúlveda Avendaño

June 2018

In this thesis, we study exponential sums of various functions defined ove any Galois field $\mathbb{F}_q$. Thomas Cusick's proved that exponential sums of rotations symmetric Boolean functions satisfy homogeneous linear recurrences with integer coefficients. A generalized version of Cusick's is proved over any Galois fields in this work. Other functions of cryptographic importance: elementary symmetric polynomial and trapezoid function, with a new techniques of turning ON and OFF some of the variable and recursive generating set are we prove that they satisfies homogeneous linear recurrences with integer coefficients.

Also, we extend the result of Cai, Green and Thierauf (Boolean case), that is, we find closed formulas for exponential sums of symmetric polynomials over any Galois field. The tools Discrete Fourier transform and circulant matrix are connected to obtain these closed formulas. We conclude that one of these closed formulas prove that the sequence of exponential sums of symmetric polynomials satisfies homogeneous linear recurrences with its explicit characteristic polynomial. And another one byproduct of our results, we discover a link between exponential sums of symmetric polynomials over Galois fields and a problem multinomial coefficients which similar to the problem of bisecting binomial coefficients.