Paper ID: 64921
oral
student

49th STUDENT CONFERENCE (E2)
Student Conference - Part 1 (1)

Author: Mr. Carlos Agrinsoni
Puerto Rico

Prof.Dr. Heeralal Janwa
University of Puerto Rico, Puerto Rico
Prof. Moises Delgado
University of Puerto Rico, Puerto Rico

# SOME NEW RESULTS IN THE EXCEPTIONAL APN CONJECTURE EVEN DEGREE CASE AND POTENTIAL LDPC BASED ERROR-CONTROL CODES FOR NEXT GENERATION SPACECRAFT TELECOMMAND

**Abstract**

Permutation functions over finite fields have been used in the construction of low-density parity (LDPC) as proposed error-control codes. Next Generation Space Telecommand as CCSDS standard (see Andrews et al. (JPL group)). Such codes are algebraically structured, hence can be implemented at the physical layer, and have excellent requisite properties. Here we propose almost perfect not-liner functions for such applications to future NASA missions. In additions, research in the theory of finite during the past six decades owes much to NASA missions (much of it developed at JPL and other labs).

Almost Perfect Nonlinear (APN) functions also have many other applications, including in coding theory and cryptography. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called an exceptional APN function if the equation $f(x + a) - f(x) = b$ have at most 2 solutions for every $b, a \in_{2^n}$, with $a \neq 0$. A function is callled an exceptional APN if it is APN on infinitely many extensions of $\mathbb{F}_{2^n}$. This problem was reduced by Janwa and Wilson and then by Rodier to the study analysis of the factorization of the corresponding multivariate function $\phi_f(x, y, z)$. After thirty years of work, it has been conjectured that the only exceptional APN functions up to CCZ equivalence are the Gold and the Kasami-Welch monomial functions. When the polynomial has an odd degree, it has been extensively analyzed, and only a few cases remain. In the even case, there are not many known results. Following the seminal work of Rodier, Caullery characterizes the factorization of the exceptional almost perfect nonlinear polynomials $\phi_f$ when the degree of the polynomial $f$ is $4e$, for $e$ odd. Later, he proved that $f(x)$ is not exceptional APN, when $\deg(f) = 4e$, when is $e$ is odd and is not a Gold or Kasami exponent. In this article we present a characterization of the factorization of $\phi_f$, when $f(x) = x^{4e} + h(x)$, $e$ is Gold or Kasami-Welch exponent and $\deg(h) \equiv 3 \mod 4$. Using this characterization we prove that such $f(x)$ cannot be exceptional APN function.