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

# CONSTRUCTION OF NEW DIFFERENTIALLY $\delta$-UNIFORM FAMILIES

By

Roberto Carlos Reyes Carranza

July 23, 2020

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY
OF PUERTO RICO, RÍO PIEDRAS CAMPUS

Our research work is on the construction of new differentially $\delta$-uniform families of vectorial Boolean functions. Almost all of our families have explicit and compact univariate in a polynomial representations with very few terms whose coefficients are either in $\mathbb{F}_2$ or are in a quadratic or cubic extension. Therefore they can be efficiently implemented in cryptographic applications. In addition, we have sub-families with high nonlinearity better than most of the differentially $\delta$-uniform families recently discovered. Therefore they offer very good resistance to differential cryptanalysis. Given a differentially $\delta$- uniform vectorial Boolean function $\mathbf{F}$, we give a generalization of a well known theorem of Edel and Pott (based on the APN-switching method of Dillon) for APN functions to differential $\delta$-uniform version. We introduce a new switching method for $\delta$-uniform functions, so that from a vectorial Boolean function $\mathbf{F}$, and another univariate Boolean function $f$ and a vector $\mathbf{u}$, we obtain all the switching neighbors of the form $\mathbf{F} + \mathbf{u} \cdot \mathbf{f}$ (generalizing quadratic switching APN functions of Budaghyan, Carlet

and Leander). Our method gives us necessary and sufficient conditions so that these vectorial Boolean functions are differentially $\delta$-uniform. As applications we obtain explicit families of the form stated.

We also discover a new theorem for a dependent variable version of Edel and Dillon on APN function, which provides a different criterion. We algorithmically apply these new theorems to discover new $\delta$-uniform and new APN functions. Also, another new theorem, with $(i, j)$-parameter families of functions, generalizes theorems of Budaghyan and Carlet, when we select $j = i$. This way, we also obtain new cubic APN functions. Different parameters generalize other known results and others yield new families with strong nonlinearity and algebraic degrees. Our functions offer strong resistance to both first and second order Fourier transform analysis (better than well known families, e.g. the Gold families).

The remarkable result that the function $x^3 + tr(x^9)$ is an APN function discovered by Budaghyan, Carlet, and Leander has not yet been generalized since 2008. Bracken, Byrne, Markin, and McGuire computed the Walsh spectrum of such a quadratic function. We give a generalization of that result.

We obtain new families of functions generalizing a result of Budaghyan, by replacing a variable $v$ by a polynomial $u(v)$. We give a variation of the idea of switching neighbor of Pott, and Pott-Budaghyan which yields further generalizations, leading to another new $\delta$-uniform family of functions. We also give a second generalization of these results. Also, we formulate a narrow-sense switching technique along an axis. This technique helps us discover two elegant differentially $\delta$-uniform families for each even $\delta$.

We include tables of the Walsh spectrum and other cryptographic properties of the Gold family over finite fields up to degree 15. These computations demonstrate that some of the not yet studied Gold functions, especially with $\Delta = 8$ and 16 are unusually interesting. We observe that some have of them have remarkable Walsh spectrum of the forms $\{2^{n-3}, 2^{\frac{n}{2}}, 0\}$,

$\{2^{n-4}, 2^{\frac{n}{2}}, 0\}$, $\{2^{\frac{n+3}{2}}, 0\}$ and $\{2^{\frac{n+5}{2}}, 0\}$. We and (we invite others) to investigate such functions with non-traditional Walsh spectrum.

Several authors have shown results on quadratic functions of the type $tr(x^{2^a+1}) + tr(x^{2^b+1})$ (Fitgerald, Lahtonen, McGuire and Ward). We open different directions, and give a lower bound for the nonlinearity of the family of functions $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})$. We develop novel techniques to obtain such new families of functions. We apply our methods to study the Walsh spectrum and the nonlinearity profile of our families that are also applicable to families of functions that contain Boolean terms of the form $tr(bx^{2^k+1})$.

We give new differentially 4-uniform permutations in even degree field extension. Thus, we make a significant contribution to an open problem of Bracken and Leander (only a few results in this direction are known).