Differential Spectra of Power Permutations

Daniel J. Katz (joint work with Kyle Pacheco and Yakov Sapozhnikov)

If F is a finite field and d is a positive integer relatively prime to $|F^\times|$, then the power map $x \mapsto x^d$ is a permutation of F, and so is called a *power permutation of F*. For any function $f\colon F \to F$, and $a, b \in F$, we define the *differential multiplicity of f with respect to a and b*, written $\delta_f(a,b)$, to be the number of pairs $(x,y) \in F^2$ with $x - y = a$ and $f(x) - f(y) = b$. We usually insist that $a \neq 0$, since it is immediate that $\delta_f(0,0) = |F|$ and $\delta_f(0,b) = 0$ for $b \neq 0$. The *differential spectrum* of f, written Δ_f, is defined as $\Delta_f = \{\delta_f(a,b) : a \in F^\times, b \in F\}$. Differential spectra of power permutations are of interest in applications to cryptography and digital communications. We are especially interested in fields F and exponents d such $f(x) = x^d$ is a power permutation over F whose differential spectrum contains at most three values. We present computational experiments that suggest conjectures as to which (F, d) pairs produce such spectra.