DANIEL KATZ, California State University, Northridge
Almost perfect nonlinear power functions with exponents expressed as fractions

Let F be a finite field, let f be a function from F to F, and let a be a nonzero element of F. The discrete derivative of f in direction a is $\Delta_a f \colon F \to F$ with $(\Delta_a f)(x) = f(x+a) - f(x)$. The differential spectrum of f is the multiset of cardinalities of all the fibers of all the derivatives $\Delta_a f$ as a runs through F^*. The function f is almost perfect nonlinear (APN) if the largest cardinality in the differential spectrum is 2. Almost perfect nonlinear functions are of interest as cryptographic primitives. If d is a positive integer, the power function over F with exponent d is the function $f \colon F \to F$ with $f(x) = x^d$ for every $x \in F$. There is a small number of known infinite families of APN power functions. In this talk, we re-express the exponents for one such family in a more convenient form. This enables us to give the differential spectrum and, even more, to give a very precise determination of individual fibers of the derivatives.