ON CRYPTOGRAPHIC PROPERTIES OF A CLASS OF POWER PERMUTATIONS IN ODD CHARACTERISTIC

MOHIT PAL
(UNIVERSITY OF BERGEN NORWAY)

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where p is an odd prime and n is a positive integer. We denote by $\mathbb{F}_q^*$ the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$ and by $\mathbb{F}_q[X]$ the ring of polynomials in indeterminate X and coefficients in $\mathbb{F}_q$. It is well-known, due to Lagranges' interpolation formula, that any function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be uniquely expressed by a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $\leq q-1$. A polynomial $f(X) \in \mathbb{F}_q[X]$ is called a permutation polynomial if the induced mapping $c \mapsto f(c)$ permutes the elements of $\mathbb{F}_q$. Recently, interest in permutation polynomials over finite fields of odd characteristic with good cryptographic properties increased as many cryptographic primitives have been proposed in the literature which operate on prime field $\mathbb{F}_p$ for some large prime p. Here, we consider the boomerang uniformity and algebraic degree of a class of differentially 4-uniform power permutations over finite fields of odd characteristic. We also determine the compositional inverse of this class of power permutations and compute the algebraic degree of its compositional inverse.