Differential spectrum of non-binary Kasami power function and related topics

Tor Helleseth

Functions with low differential uniformity have been extensively studied in recent years. These functions are of interest in cryptography, coding theory and sequence designs. Finding the complete differential spectra of permutation power functions is in general a much harder problem than just finding their differential uniformity. In this talk the complete differential spectra will be determined for the well known Kasami functions over $GF(p^n)$. These functions are defined by $f(x) = x^d$, $d = p^{2k} - p^k + 1$, where p is an odd prime and k any integer with $gcd(k, n) = 1$. These function are differentially $(p + 1)$-uniform and the case $p = 3$ solves a conjecture by Xu, Cao and Xu. These results are joint work with Yan, Zhou, Weng, Wen and Wang.

The remaining part of the talk will contain an overview of the history of the earlier results of non-binary power functions with low differential uniformity and some related topics.