Construction of n-variable balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{n/2}$

Deng Tang

In this talk we consider the maximum absolute value in the autocorrelation spectrum (not considering the zero point) of cryptographic Boolean functions. In even number of variables n, bent functions possess the highest nonlinearity with absolute value equals 0. The long standing open question (for two decades) in this area is to obtain a theoretical construction of balanced functions with absolute value strictly lesser than $2^{n/2}$. So far there are only a few examples of such functions for $n = 10, 14$, but no general construction technique is known. In this talk, we mathematically construct an infinite class of balanced Boolean functions on n variables having absolute indicator strictly lesser than $2^{n/2}$ and almost optimal nonlinearity, which can also be viewed as an infinite class of counterexamples against Zhang-Zheng conjecture proposed in 1995.