PETR LISONEK, Simon Fraser University

Non-existence results for vectorial bent functions with Dillon-type exponents

Vectorial bent functions with Dillon-type exponents have attracted attention because they are hyperbent whenever they are bent, and they achieve the highest possible algebraic degree among all bent functions on the same domain. We study monomial functions $f(x) = \mathrm{Tr}_k^{2m}(ax^{2^m-1})$ where $a \in \mathbb{F}_{2^{2m}}^*$ and Tr_k^{2m} denotes the trace from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^k}$. Muratović-Ribić, Pasalic and Bajrić (IEEE Trans. Inform. Theory 2014) proved that f is not bent when $k = m$. Lapierre and Lisoněk (Proceedings ISIT 2016) proved that f is not bent when $k = m/2$, $k \geq 2$. In the current work we further introduce new proof techniques and we prove that f is not bent when $k = m/3$ where k is odd, $k \geq 3$. Our techniques use results that relate the divisibility of the Kloosterman sum $K(a)$ by powers of 2 and the coefficients of the characteristic polynomial of a due to Göloğlu, Lisoněk, McGuire and Moloney (IEEE Trans. Inform. Theory 2012). This is joint work with Luc Lapierre.