Cryptology ePrint Archive: Report 2011/698

A generalization of the class of hyper-bent Boolean functions in binomial forms

Chunming Tang, Yu Lou, Yanfeng Qi, Baocheng Wang, Yixian Yang

Abstract: Bent functions, which are maximally nonlinear Boolean functions with even numbers of variables and whose Hamming distance to the set of all affine functions equals $2^{n-1}\pm 2^{\frac{n}{2}-1}$, were introduced by Rothaus in 1976 when he considered problems in combinatorics. Bent functions have been extensively studied due to their applications in cryptography, such as S-box, block cipher and stream cipher. Further, they have been applied to coding theory, spread spectrum and combinatorial design. Hyper-bent functions, as a special class of bent functions, were introduced by Youssef and Gong in 2001, which have stronger properties and rarer elements. Many research focus on the construction of bent and hyper-bent functions. In this paper, we consider functions defined over $\mathbb{F}_{2^n}$ by $f^{(r)}_{a,b}:=\mathrm{Tr}_{1}^{n}(ax^{r(2^m-1)}) +\mathrm{Tr}_{1}^{4}(bx^{\frac{2^n-1}{5}})$, where $n=2m$, $m\equiv 2\pmod 4$, $a\in \mathbb{F}_{2^m}$ and $b\in\mathbb{F}_{16}$. When $r\equiv 0\pmod 5$, we characterize the hyper-bentness of $f^{(r)}_{a,b}$. When $r\not \equiv 0\pmod 5$, $a\in mathbb{F}_{2^m}$ and $(b+1)(b^4+b+1)=0$, with the help of Kloosterman sums and the factorization of x^5+x+a^{-1}, we present a characterization of hyper-bentness of $f^{(r)}_{a,b}$. Further, we give all the hyper-bent functions of $f^{(r)}_{a,b}$ in the case $a\in\mathbb{F}_{2^{\frac{m}{2}}}$.

Category / Keywords: Boolean functions, bent functions, hyper-bent functions, Walsh-Hadamard transformation, Kloosterman sums

Date: received 21 Dec 2011, last revised 12 Nov 2012

Contact author: tangchunmingmath at 163 com