

Cryptology ePrint Archive: Report 2011/515

A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity

Qingfang Jin and Zhuojun Liu and Baofeng Wu and Xiaoming Zhang

Abstract: In this paper, we propose two classes of $2k$ -variable Boolean functions, which have optimal algebraic immunity under the assumption that a general combinatorial conjecture is correct. These functions also have high algebraic degree and high nonlinearity. One class contain more bent functions, and the other class are balanced.

Category / Keywords: Boolean function, Algebraic immunity, Bent function, Balancedness, Nonlinearity, Algebraic degree

Date: received 18 Sep 2011

Contact author: qfjin at amss ac cn

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20110922:024517 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]