Cryptology ePrint Archive: Report 2011/549

1-Resilient Boolean Function with Optimal Algebraic Immunity

Qingfang Jin and Zhuojun Liu and Baofeng Wu

Abstract: In this paper, We propose a class of 2k-variable Boolean functions, which have optimal algebraic degree, high nonlinearity, and are 1-resilient. These functions have optimal algebraic immunity when k > 2 and u = -2^l; 0 =< l < k. Based on a general combinatorial conjecture, algebraic immunity of these functions is optimal when k > 2 and u = 2^l; 0 =< l < k. If the general combinatorial conjecture and a new assumption are both true, algebraic immunity of our functions is also optimal when k > 2, otherwise u.

Category / Keywords: Boolean function Algebraic immunity 1-Resilient Balancedness Nonlinearity Algebraic degree

Date: received 5 Oct 2011

Contact author: qfjin at amss ac cn