Cryptology ePrint Archive: Report 2011/366

Highly Nonlinear Boolean Functions with Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks

Deng Tang and Claude Carlet and Xiaohu Tang

Abstract: In this paper, we present a new combinatorial conjecture about binary strings. Based on the new conjecture, two classes of Boolean functions of $2k$ variables with optimal algebraic immunity are proposed, where $k\ge 2$. The first class contains unbalanced functions having high algebraic degree and nonlinearity. The functions in the second one are balanced and have maximal algebraic degree and high nonlinearity. It is checked that, at least for small numbers of variables, both classes of functions have a good behavior against fast algebraic attacks. Compared with the known Boolean functions resisting algebraic attacks and fast algebraic attacks, the two classes of functions possess the highest lower bounds on nonlinearity. These bounds are however not enough for ensuring a sufficient nonlinearity for allowing resistance to the fast correlation attack. Nevertheless, as for previously found functions with the same features, there is a gap between the bound that we can prove and the actual values computed for small numbers of variables. Moreover, these values are very good and much better than for the previously found functions having all the necessary features for being used in the filter model of pseudo-random generators.

Category / Keywords: secret-key cryptography / Boolean functions, balancedness, algebraic immunity, fast algebraic attack, algebraic degree, nonlinearity.

Date: received 6 Jul 2011

Contact author: dengtanghome at qq com