CORR 2001-57

Boolean Functions with Large Distance to all Bijective Monomials: N odd case

Amr Youssef & Guang Gong*

Abstract Cryptographic Boolean functions should have large distance to functions with simple algebraic description to avoid cryptanalytic attacks based on successive approximation of the round function such as the interpolation attack. Hyper-bent functions achieve the maximal minimum distance to all the coordinate functions of all bijective monomials. However, this class of functions exists only for functions with even number of inputs. In this paper we provide some constructions for Boolean functions with odd number of inputs that achieve large distance to all the coordinate functions of all bijective monomials.

Keywords Boolean functions, hyper-bent functions, extended Hadamard transform, Legendre sequences, nonlinearity.