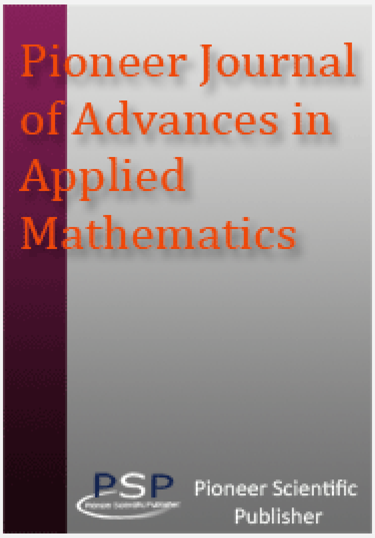
Pioneer Journal of Advances in Applied Mathematics
Volume 2, Issue 1, Pages 21-38 (June 2011)

ISSN: 2231-1858



Pioneer Journal of Advances in Applied Mathematics

PSP Pioneer Scientific Publisher

BIJECTIVE DIFFERENTIALLY 2-UNIFORM FUNCTIONS AND BALANCED INCOMPLETE BLOCK DESIGN: NEW COMBINATORIAL CONSTRUCTION

Cécile Duvigneau and Eric Filiol

Received May 13, 2011

Abstract

As Blondeau et al. reminded us in [Céline Blondeau, Anne Canteaut and Pascale Charpin, Differential properties of power functions, Int. J. Inf. Coding Theory 1(2) (2010), 149-170.], the non-existence of bijective differentially 2-uniform function for an even number of input bits has long been considered as an open conjecture. J. F. Dillon [APN Polynomials: an update, Fq9, International Conference on Finite Field and their Applications, 2009.] recently proved that this conjecture was false by providing a single such function, but failed to produce any general construction method. In this paper, we discuss about the correlation between designs and almost perfect nonlinear permutations in order to build a method to generate optimal bijective differentially 2-uniform functions for an even number of input bits. Our approach is totally different from previous ones which consisted in first, generating the truth table of functions and then checking whether they are optimal or not. Starting from a specific differential matrix, we recursively build the corresponding truth table to generate a family of optimal functions.

These functions are critical primitives in block cipher designs since they determine the security of *S*-boxes against differential cryptanalysis [Eli Biham and Adi. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptology 4(1) (1991), 3-72]. We thus expose an approach for the construction of optimum *S*-boxes, linking differentially 2-uniform permutations and designs.

Keywords and phrases: *S*-box, XOR value, differential matrix, combinatorial designs.