Cryptology ePrint Archive: Report 2011/047

Constructing differential 4-uniform permutations from know ones

Yuyin Yu and Mingsheng Wang and Yongqiang Li

Abstract: It is observed that exchanging two values of a function over ${\mathbb F}_{2^n}$, its differential uniformity and nonlinearity change only a little. Using this idea, we find permutations of differential 4-uniform over ${\mathbb F}_{2^6}$ whose number of the pairs of input and output differences with differential 4-uniform is 54, less than 63, which provides a solution for an open problem proposed by Berger et al. \cite{ber}. Moreover, for the inverse function over $\mathbb{F}_{2^n}$ (n even), various possible differential uniformities are completely determined after its two values are exchanged. As a consequence, we get some highly nonlinear permutations with differential uniformity 4 which are CCZ-inequivalent to the inverse function on $\mathbb{F}_{2^n}$.

Category / Keywords: applications / vectorial boolean function, differential uniformity, nonlinearity, CCZ-equivalence, almost perfect nonlinear (APN)

Date: received 17 Jan 2011, last revised 16 Jun 2011

Contact author: yuyuyin at 163 com