**Nyberg, Kaisa**

**Perfect nonlinear S-boxes.** (English) Zbl 0766.94012

Advances in Cryptology, Proc. Workshop, EUROCRYPT '91, Brighton/UK 1991, Lect. Notes Comput. Sci. 547, 378-386 (1991).

Summary: A perfect nonlinear S-box is a substitution transformation with evenly distributed directional derivatives. Since the method of differential cryptoanalysis presented by E. Biham and A. Shamir makes use of nonbalanced directional derivatives, the perfect nonlinear S-boxes are immune to this attack. The main result is that for a perfect nonlinear S-box the number of input variables is at least twice the number of output variables. Also two different construction methods are given. The first one is based on the Maiorana-McFarland construction of bent functions and is easy and efficient to implement. The second method generalizes Dillon's construction of difference sets.

[For the entire collection see Zbl 0756.00008.]

**MSC:**

94A60 Cryptography
05B10 Combinatorial aspects of difference sets (number-theoretic, group-theoretic, etc.)



**Keywords:**

perfect nonlinear S-box; differential cryptoanalysis; nonbalanced directional derivatives; Maiorana-McFarland construction of bent functions; Dillon's construction of difference sets

**Full Text:** DOI