Second International Conference "Mathematics Days in Sofia"
July 10–14, 2017, Sofia, Bulgaria

Fast Implementation of the ANF Transform

Valentin Bakoev

University of V. Tarnovo "St. Cyril and St. Methodius", Bulgaria
v.bakoev@uni-vt.bg

The algebraic normal forms (ANFs) of Boolean functions are used in computing the algebraic degree of S-boxes, which is one of the most important cryptographic criteria. It should be computed by fast algorithms so that more S-boxes are generated and the best of them are selected. Here we continue our previous work for fast computing the ANFs of Boolean functions. We represent and investigate the full version of bitwise implementation of the ANF Transform. The obtained algorithm has a time-complexity $\Theta((9n-2).2^{n-7})$ and $\Theta(2^{n-6})$ space complexity. The experimental results show that it is more than 20 times faster in comparison to the well-known byte-wise ANF Transform.