Cryptology ePrint Archive: Report 2013/148

AES-like ciphers: are special S-boxes better then random ones? (Virtual isomorphisms again)

Alexander Rostovtsev

Abstract: In [eprint.iacr.org/2012/663] method of virtual isomorphisms of ciphers was applied for differential/linear cryptanalysis of AES. It was shown that AES seems to be weak against those attacks. That result can be generalized to AES-like ciphers, which diffusion map is a block matrix, and its block size is the same as the S-box size. S-box is possibly weak if it is affine equivalent to a substitution that has the same cycling type as an affine substitution. Class of possibly weak S-boxes is very large; we do not know is there an S-box that is not possibly weak. Strength of AES-like cipher is defined by virtual isomorphism and not by differential/linear properties of the S-box. So we can assume that special S-boxes have little or no advantage comparatively to random nonlinear S-boxes. The conjecture is verified by experiments. If the conjecture is true, then search of the best S-boxes that maximizes the cipher strength against differential and linear attacks joined with virtual isomorphisms has no sense.

Category / Keywords: secret-key cryptography / AES, block ciphers, cryptanalysis, linear cryptanalysis

Publication Info: alexander.rostovtsev@ibks.ftk.spbstu.ru

Date: received 12 Mar 2013

Contact author: alexander rostovtsev at ibks ftk spbstu ru