Cryptology ePrint Archive: Report 2011/489

Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis

A. N. Alekseychuk and L. V. Kovalchuk

Abstract: In this paper, we present new general techniques for practical security evaluation against differential and linear cryptanalysis for an extensive class of block ciphers similar to the cipher GOST. We obtain upper bounds of the average differential and linear characteristic probabilities for an arbitrary GOST-like cipher. The obtained bounds have similar form to the upper bounds of the average differential and linear characteristic probabilities known for some Markov Feistel ciphers. But, the expressions of our bounds contain new parameters (different from the classical differential and linear probabilities) of the cipher's s-boxes. These parameters are very natural for GOST-like ciphers, since they inherit the type of operation (key addition modulo 2^m) used in these ciphers. The methods our proofs are based on are of independent interest and can be used for investigation both of a wider class of block ciphers and of a wider class of attacks.

Application of our results to GOST shows that maximum values of the average differential and linear characteristic probabilities of this cipher (with 32 rounds and some s-boxes) are bounded by $2^{-59.57}$ and 2^{-42}, respectively. The last two estimates of practical security of GOST against the differential and linear cryptanalysis are not quite impressive. But, as far as we know, they are the best of such estimates obtained by an accurate mathematical proof.

Category / Keywords: secret-key cryptography /

Publication Info: A part of results from this paper was published in 2006 - 2007

Date: received 9 Sep 2011

Contact author: lv_kov_crypto at mail ru