The vulnerability analysis and the security evaluation of block ciphers

ABSTRACT

The first step for evaluation of block ciphers is the confidence on attainment of some properties such as completeness, strict avalanche criterion and static information leakage. The attainment of these properties causes the strength of confusion and diffusion properties in block ciphers. In this paper, we describe the computational efficiency of these properties for doing of security evaluation on the different classes of block ciphers. This paper contains the latest scientific results which are used for evaluation of output sequences of cryptosystems.

Keyword: Block cipher; Security evaluation; Completeness; Avalanche; Static information leakage