Some statistical simulation results over the 128-bit block cipher CLEFIA

ABSTRACT

CLEFIA , a 128-bit block cipher designed using Diffusion Switching Mechanism (DSM) , was proposed by Sony Corporation in 2007. The attainment of some properties such as completeness, strict avalanche criterion and randomness cause the invigoration of confusion and diffusion properties in block ciphers. In this paper, we evaluate CLEFIA by considering these three important properties. For the case of 128-bit key, it supplies the first two criteria with at least assurance factor 97%.This paper shows also some statistical simulation results of block cipher CLEFIA.

Keyword: Block Cipher; CLEFIA; Security evaluation; Completeness; Avalanche; Randomnes