The new variable-length key symmetric cryptosystem

ABSTRACT

Problem statement: In this study, we proposed a new 64-bit block cipher that accepted a variable-length key up to 512 bits, which was suitable for implementation in a variety of environments. Approach: The cipher algorithm was a 16-round Feistel network with a bijective function f and was made up of two key-dependent 16×16 S-boxes, bitwise rotations, and a carefully designed key schedule. Results: The block cipher, what we called NBC08, was designed to perform under the powerful operations supported in today’s computers, resulting in an improved security/performance tradeoff over existing block ciphers. Conclusion: The study concluded the differential, linear and algebraic cryptanalysis on the NBC08 and showed that the cipher cannot be analyzed by any cryptanalytic attack. The statistical test results for NBC08 did not indicate a deviation from random behavior.

Keyword: Block ciphers; Feistel structure; Key dependent s-box; Attacks