AN EFFECTIVE AND SECURE CIPHER BASED ON SDDO

Đỗ Thị Bắc, Nguyễn Hiếu Minh, Hồ Ngọc Duy

TÓM TẮT:

To improve the efficiency of security of the information secure mechanism, an algorithm BMD-128 is proposed. This algorithm is built on the SDDO. Using this operator decreases significanthy the cost of hardware implementation. Besides, it also ensures both the high applicability in the transaction needing the change of session keys with high frequency and the ability against slide attack. Concurrently, this algorithm also eliminates the weak keys without the complex round key proceduce. The algorithm is evaluated regards to the standard NESSIE and the ability against the differential cryptanalysis. Concurrently, it is also compared the performance with the other famous ciphers when implementing on hardware FPGA.