NEW SDDO-BASED BLOCK CIPHER FOR WIRELESS SENSOR NETWORK SECURITY

Đỗ Thị Bắc, Hồ Ngọc Duy, Nguyễn Hiếu Minh

TÓM TẮT:

Wireless sensor networks (WSNs) are exposed to a variety of attacks. The quality and complexity of attacks are rising day by day. Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. This paper concerns the problem of using of the switchable data-dependent operations (SDDOs) oriented to the design of fast cipher suitable to applications in constrained environments. The new SDDO-based block cipher using this approach presented and estimated. The security estimations show that cipher MD-64 is less likely to suffer intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on. Moreover, FPGA synthesis result for hardware implementation (FPGA) proves that new cipher MD-64 is very efficient, especially for WSN.