World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:01, 2018

NUX: A Lightweight Block Cipher for Security at Wireless Sensor Node Level

Authors : Gaurav Bansod, Swapnil Sutar, Abhijit Patil, Jagdish Patil

Abstract : This paper proposes an ultra-lightweight cipher NUX. NUX is a generalized Feistel network. It supports 128/80 bit key length and block length of 64 bit. For 128 bit key length, NUX needs only 1022 GEs which is less as compared to all existing cipher design. NUX design results into less footprint area and minimal memory size. This paper presents security analysis of NUX cipher design which shows cipher's resistance against basic attacks like Linear and Differential Cryptanalysis. Advanced attacks like Biclique attack is also mounted on NUX cipher design. Two different F function in NUX cipher design results in high diffusion mechanism which generates large number of active S-boxes in minimum number of rounds. NUX cipher has total 31 rounds. NUX design will be best-suited design for critical application like smart grid, IoT, wireless sensor network, where memory size, footprint area and the power dissipation are the major constraints.

Keywords : lightweight cryptography, Feistel cipher, block cipher, IoT, encryption, embedded security, ubiquitous computing
Conference Title : ICSC 2018 : International Conference on Security and Cryptography
Conference Location : Sydney, Australia
Conference Dates : January 29-30, 2018