Jordan University of Science and Technology

Efficient CMOL Gate Designs for Cryptography Applications

Authors: Z. Abid, A. Alma'aitah, M. Barua, W. Wang

Abstract: This paper introduces new hybrid complementary metal-oxide-semiconductor (CMOS)-nano (CMOL) circuits for efficient implementation of cryptographic algorithms. The novelty of this study is to utilize two types of nanojunction devices with CMOS to build the crypto IC. In particular, efficient XOR gate with resistive junctions and XOR/AND gates with diode-like junctions are develop to be used as building blocks of the corresponding modules of the Advanced Encryption Standard (AES) crypto IC. They allow a reduction of 79%, 43%, and 53% in power dissipation, area, and time delay compared to the existing CMOL implementation of AES system. When compared to field-programmable nanowire interconnect (FPNI) design of AES, a 56% increase in power dissipation was recorded in order to achieve a 92% and 15% reduction in area and time delay. This proposed circuit study also leverages the recent fabrication results, which is a feasible CMOS-nano hybrid solution for future crypto IC development.