# Jordan University of Science and Technology

## Area efficient-high throughput sub-pipelined design of the AES in CMOS 180nm

**Authors:** A. Alma'aitah and Z. E. Abid,

**Abstract:** In this paper, efficient hardware of one of the most popular encryption algorithms, the Advanced Encryption Standard (AES), is presented. A modified sub-pipelined structure is proposed targeting high speed and low power-delay product of the compact AES design with on-the-fly key expansion unit. By adding 25.8% in hardware complexity to the existing ASIC designs, the throughput is increased more than 158% with better overall power-delay product. Compared to other compact AES implementation the proposed structure can go up to 6Gbit/sec with about 13k gate count.