Jordan University of Science and Technology

Transistor level optimization of sub-pipelined AES design in CMOS 65nm

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

Abstract: Stage optimization of the hardware implementation of the popular encryption algorithms, the Advanced Encryption Standard (AES), is presented. The optimization, for lower power dissipation, is based on implementing the Multi Threshold CMOS (MTCMOS) technique in each of the AES stages. The critical paths are implemented using high performance gates based on high driving current transistors. For the optimized design, the Simulation results show about 10% reduction in power consumption compared to non optimized designs while maintaining the same throughput of 18Gbit/sec.