**OPTIMIZED ARCHITECTURE FOR AES**

**Abstract:**

This paper presents a highly optimized architecture for Advanced Encryption Standard (AES) by dividing and merging (combining) different sub operations in AES algorithm. The proposed architecture uses ten levels of pipelining to achieve higher throughput and uses Block-RAM utility to reduce slice utilization which subsequently increases the efficiency. It achieves the data stream of 57 Gbps at 451 MHz working frequency and obtains 36% improvement in efficiency to the best known similar design throughput per area (Throughput/Area) and 35% smaller in slice area. This architecture can easily be embedded with other modules because of significantly reduced slice utilization.

**Index Terms**—Advanced Encryption Standard (AES), Composite Field Arithmetic, Field Programmable Gate Array (FPGA)

**TOOLS:**

1. **XilinxISE 14.7**

**LANGUAGE:**

1. **VerilogHDL**