Abstract

This paper proposes the Application Specific Integrated Circuit (ASIC) implementation of Advanced Encryption Standard (AES) cryptographic algorithm with reconfigurable 128-bit, 192-bit, 256-bit keys. The proposed implementation has compact 32-bit I/O for both data and key transfer. By using on the fly key generation for encryption process along with efficient implementation of MixColumn and InverseMixColumn operations using finite field GF(22) for our 32-bit AES crypto system gives a maximum of 80.1% improvement in operating frequency when compared to the recent implementations. The maximum operating frequency of our proposed pipelined implementation is 333 MHz with high throughput of around 10.656 Gbps in 180 nm standard cell CMOS technology.

Index Terms

Computer Science

Security
Key words

Keywords - AES

Cryptography

Galois Field GF(28)

On the fly key generation

Throughput