International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.2, No. V (2009), pp 259-269

# IMPLEMENTATION OF RIJNDAEL ALGORITHM USING VERILOG FOR ENHANCING DATA SECURITY

**MAHESH A. GANGARDE, PRADEEP B. MANE AND SHRIDHAR S. DUDAM**

**Abstract**

The current fast growing use of the Internet for commercial transactions has created large demands for data protection and network security. This in turn has made the cryptography, an important component in the design of modern information systems. Rijndael algorithm is the new Advanced Encryption Standard (AES) adopted by the National Institute of Standards and Technology (NIST) to replace existing Data Encryption Standard (DES). Compared to software implementation, hardware implementation of Rijndael algorithm provides more physical security as well as higher speed. Reprogrammable devices are highly attractive options for hardware implementation of AES (Rijndael) algorithm. This paper presents an implementation of sub bytes, shift rows, Mix columns and Add round key operations in verilog. A look up table called S-Box has been used to obtain the sub byte values instead of applying affine transformation every time to calculate sub byte values. The existing Rijndael algorithm has been modified by including on the fly key generation, which has facilitated simultaneous execution of sub bytes, shift rows, and round key generation to lower execution time. Implementation supports for encryption as well as decryption of 128 bit data using 128-bit key. This can be used as IP (Intellectual Property) core in many applications for data security.

---

**Keywords:** AES, DES, FPGA, Cryptography.