

# **FPGA Implementation of Improved S-BOX Architecture for Advanced Encryption Standard**

Prahlad Kumar Khandekar  
[prahladkh@gmail.com](mailto:prahladkh@gmail.com)

*M.Tech. Scholar, ET&T Department*  
Chouksey Engg. College Bilaspur

Sachin Meshram  
[sachinm288@gmail.com](mailto:sachinm288@gmail.com)

*Asst. Professor, ET&T Department*  
Chouksey Engg. College Bilaspur

*Abstract* — Advance Encryption Standard (AES) is one of the most popular cryptographic algorithm now a days providing integrity, authentication and security. The Substitution block, used for security better known as S-BOX is the key element of Advance Encryption Standard algorithm. Different algorithm presented in previous work which are lagging behind in few parameters, which is corrected and implemented in this paper. Proposed architecture is implemented in VHDL Using Xilinx ISE 12.1 on device xc3s1200e-5fg320 of Spartan family.

*Keywords* — S-Box, AES, Galois Field, VHDL, Spartan.