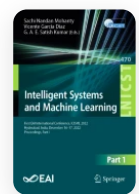


[Home](#) > [Intelligent Systems and Machine Learning](#) > Conference paper

Comparison of Advanced Encryption Standard Variants Targeted at FPGA Architectures

Conference paper | First Online: 10 July 2023

pp 346–355 | [Cite this conference paper](#)




Intelligent Systems and Machine

Learning

(ICISML 2022)

[Nithin Shyam Soundararajan](#)  & [K. Paldurai](#)

 Part of the book series: [Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering](#) ((LNICST, volume 470))

 Included in the following conference series:
[International Conference on Intelligent Systems and Machine Learning](#)

 282 Accesses

Abstract

Digital communication of any form must provide data confidentiality as the threats are increasing in today's rapid world. Data privacy and security are crucial factors as data is considered gold in the modern era. The 128-bit Advanced Encryption Standard algorithm, commonly known as AES, has been implemented in several designs, focusing on specific purposes and is used widely. The 256-bit variant uses the same fundamental cipher blocks as the 128-bit version but differs in key size, the key expansion function and the number of cipher rounds. This paper investigates the 256-bit AES algorithm targeted at FPGA-Field Programmable Gate Arrays architectures and compares it with the 128-bit implementation, reporting performance and resource utilization. Also, the security offered is discussed. The security is determined by the complexity of recovering the key using cryptanalytic attacks. Both encryption and