Abstract
The AES encryption/decryption algorithm is widely used in modern consumer electronic products for security. To shorten the encryption/decryption time of plenty of data, it is necessary to adopt the algorithm of hardware implementation; however, it is possible to meet the requirement for low cost by completely using software only. How to reach a balance between the cost and efficiency of software and hardware implementation is a question worth of being discussed. In this paper, we implemented the AES encryption algorithm with hardware in combination with part of software using the custom instruction mechanism provided by the ARM7 with keil platform. we explored various combinations of hardware and software to realize the AES algorithm and discussed possible best solutions of different needs.

Reference

- AN 188: Custom Instructions for the Nios Embedded Processor, Altera Corporation [5]

Index Terms

Computer Science Wireless
Key words

Cryptography
custom instruction

ARM processor

AES