عنوان مقاله:

a testable pipelined hardware implementation of the advance encryption standard

محل انتشار:

دهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1383)

تعداد صفحات اصل مقاله: 6

نویسندگان:

mahdi nazm bojnordi - *department of electrica&computerl engineering university of tehran*

mehdi semsarzadeh

خلاصه مقاله:

incontrast with software implementioan hardware implementaion provides a higher level of security and cryptography speed here some of so far AES implementations are scrutinized and an unrolled fully pipelined implementation for the AES is presented this implementation is equipped with BIST architecture for self testing in this design both encryption and decryption are considered also the design is potimized to achieve higher speed and less occupied area. the .rijndael algorithm is selected for AES to implement using a 0.35 mm ASIClibrary

کلمات کلیدی:

AES,testable AES,BIST,rijndel ,nurolled,pipeline implementation

لینک ثابت مقاله در پایگاه سیویلیکا: