جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الإلكترونيات والاتصالات

تقييم فعالية تنفيذ معيار التشفير المتقدم باستخدام شريحة صفيفة بوابات قابلة للبرمجة حقلياً

Evaluation of the Performance of Implementing Advanced Encryption Standard (AES) using Field Programmable Gate Array (FPGA) Chip

إعداد م. ميرفت الشريف

إشراف د.م. عادل خضور علي

الملخص

التطور السريع في تقانات المعلومات جعل البيانات عرضة للهجمات، مما دفع الباحثين لتطوير آليات مختلفة لحمايتها إحداها خوارزمية التشفير المتقدمAES ،حيث تعددت الدراسات السابقة لتقييم فعالية تطبيق هذه الخوارزمية باستخدام شرائح FPGAs، تم في هذه الدراسة مقارنة أداء ثمانية عائلات من شرائح مختلفة منFPGAs وذلك بتنفيذ خوارزميةAES على تلك الشرائح واختيار الشريحةKintex-7 ذات الفعالية الأعلى التي بلغت 4.06Mbps/slice .

القسم النظري

أهمية البحث:

حماية بيانات المستخدمين وذلك عند انتقالها من خلال تقنيات الاتصال المختلفة لضمان سريتها وتكاملها وعدم التلاعب بها وضمان وصولها للمستخدم المناسب ،وذلك في مجالات مختلفة مثل المجال العسكري أو المجال الاقتصادي عن طريق خوارزميات التشفير المختلفة وتنفيذها باستخدام شرائح الكترونية منهاFPGA.

مسوغات البحث:

برزت عدة دراسات لتقييم فعالية خوارزمية التشفير المتقدمAES وكل باحث يحاول تحسين فعالية هذه الخوارزمية بطرق مختلفة.

هدف البحث:

تقييم فعالية تنفيذ خوارزمية معيار التشفير المتقدم AES باستخدام شرائح صفيفة البوابات القابلة للبرمجة حقليا وذلك بتنفيذ الخوارزمية على شرائح مختلفة وتحديد أي شريحة أفضل.

النتائج والمناقشة

جاءت هذه الدراسة لتسلط الضوء على أهمية خوارزميات التشفير في حماية البيانات المختلفة بتنفيذ إحداها وهي خوارزمية معيار التشفير المتقدم AES على شرائح البوابات القابلة للبرمجة حقلياً وتقييم الفعالية فكانت النتائج وفق الآتي

1- لدى مقارنة نتائج فعالية تنفيذ الخوارزمية AES باستخدام ثمانية أنواع من شرائح FPGAs كانت العائلةKintex-7 الأفضل من حيث قيمة الفعالية حيث بلغت 4.06 Mbps/slice.

2-عند مقارنة نتائج فعالية خوارزمية البحث مع دراسات سابقة وجدنا أن هذه الدراسة حققت تحسيناً عن الدراسة[3] بمقدار 172.06 %.

المراجع

[1]Priya,s. KarthigaiKumar,P.Teja,N.(2021,October).FPGA implementation of AES algorithm for high-speed applications. Analog Integrated Circuits and Signal Processing.

[2] Arul Murugan, C. Karthigaikumar,P.,& Priya,S (2020,September).FPGA implementation of hardware architecture with AES encryptor using sub- pipelined S-box techniques for compact applications. Journal for Control, Measurement, Electronics, Computing and Communications,61(4),682-693.

[3] Zodpe,H.Sapkal,A.An efficient AES implementation using FPGA with enhanced security features (2020,July).In Journal of King Saud University-Engineering Sciences ,32,115-122.

[4] Nabil, M., M. Khalaf, A., &M.Hassan,s. Design and implementation of pipelined and parallel AES encryption systems using FPGA. (2020), Indonesian Journal of Electrical Engineering and Computer Science,20(1),287-299.