Abstract

Name: ***Adnan Abdul-Aziz M. S. Gutub***

Title: *A Hardware Model of an Expandable RSA Cryptographic System*

Major Field: *Computer Engineering*

Date of Degree: *December 1998*

Data security is an important aspect of information transmission and storage in an electronic form. Cryptographic systems are used to encrypt such information to guarantee its security. To retrieve such information, the encrypted form must be first decrypted. One of the most popular cryptographic systems is the RSA system. The security of the RSA-encrypted information largely depends on the size of the used encryption key. The larger the key size is the longer the encryption/decryption time will be. To cope with the continuous demand for larger key sizes, faster hardware implementations of the RSA algorithm has become an active area of research. One disadvantage of hardware implementations is their fixed key sizes. If the key size is to be increased, the hardware design should be fully replaced.

The work reported here proposes an RSA hardware implementation that can be expanded as the key size gets larger. This implementation is modeled using VHDL in a parametrizable manner. Two other parameterized RSA hardware designs have also been VHDL modeled for comparison. The three models are compared for a 1024-bit key size and the results are analyzed. The complexity of the designs are compared and conclusions regarding optimal delay and area parameters are made.

Master of Science Degree

King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia
December 1998

بسم الله الرحمن الرحيم

خلاصة الرسالة

الاســـم : عدنان بن عبدالعزيز بن محمد صديق قطب

عنوان الرسالة : تصميم دائرة إلكترونية دقيقة قابلة للتطوير حسب الحاجة لعملية التشفير بنظام RSA

التخصـص : هندسة الحاسب الآلي

تاريخ الشهادة : شعبان 1419هـ

التشفير(Cryptography) هو الأسلوب الأمثل لحماية المعلومات والحفاظ على سريتها. وأحد أنجـح طـرق التشفير المستخدمة يعرف بـ (RSA) ، وهي الطريقة التي تعتمد على حجم مفتاح الشفرة لتعقيد استنباط الرسالة الأساسية في وقت قصير ، وتعاني طريقة (RSA) من سلبية في تصميمها بالدوائر الإلكترونية الدقيقة ، وهـي أن الدوائر مصممة للتشفير بمفتاح ذو حجم معين ثابت ، لو تغير لأحتاج تغيير التصميم الإلكتروني بالكلية.

وقد تم في هذا البحث تصميم طريقة جديدة مبنية على فكرة تطوير الدائرة الإلكترونيـة الدقيقـة حـسب الحاجة، بحيث تم تمثيل هذا التصميم باستعمال نموذج محاكاة التصميم الإلكتروني باسـتخدام لغـة (VHDL) ، وقورن هذا النموذج بالتفصيل مع تصميمين آخرين أيضاً باستخدام (VHDL) ، وأثبت التصميم المقترح تفوقاً في السرعة بالرغم من أنه يعتبر الأكبر مساحة.

وقد تم إجراء مقارنة بين التصاميم الثلاثة من حيث كفاءة الأداء والسرعة و التكلفة (التكلفة = المساحة × السرعة^2)، وأظهر التصميم المقترح نتائج مقاربة لأفضل تصميم. واعتبرت زيادة التكلفة نوع من الثمن مقابل للمرونة المتوفرة في هذا التصميم والتي تجعله قابل للتطـوير حسب حاجة المستخدم.

درجة الماجستير في العلوم

جامعة الملك فهد للبترول والمعادن

الظهران - المملكة العربية السعودية

شعبان 1419هـ