A Hardware Model of an Expandable RSA Cryptographic System

by

Adnan Abdul-Aziz M.S. Gutub

A Thesis Presented to the

FACULTY OF THE COLLEGE OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER ENGINEERING

December, 1998

A Hardware Model of an Expandable RSA Cryptographic System

BY

Adnan Abdul-Aziz M.S. Gutub

A Thesis Presented to the

FACULTY OF THE COLLEGE OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

Computer Engineering

December 1998

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS
DHAHRAN 31261, SAUDI ARABIA

COLLEGE OF GRADUATE STUDIES

The Thesis, written by

Adnan Abdul-Aziz M. S. Gutub

under the direction of his Thesis advisor and approved by his Thesis Committee, has been presented to and accepted by the Dean of the College of Graduate Studies, in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER ENGINEERING

Thesis Committee:

27.12.98
Dr. Alaaeldin Amin (Chairman)

27.12.98
Dr. Khalid Elleithy (Member)

28/12/98
Dr. Khalid Al-Tawil (Member)

Abdullah Almejel
Department Chairman

Dean, College of Graduate Studies

30-12-98
Date

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

الاســـــم : عدنان بن عبدالعزيز بن محمد صديق قطب

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

التخصـــص : هندسة الحاسب الآلي

تاريخ الشهادة : شعبان ١٤١٩هـ

التشفير(Cryptography) هو الأسلوب الأمثل لحماية المعلومات والحفاظ على سريتها. وأحد أنجح طـــرق التشفير المستخدمة يعرف بـــ(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 ، وهـــي 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 الإلكترونية الدقيقـــة حســـب الحاجة، بحيث تم تمثيل هذا التصميم باستعمال نموذج محاكاة التصميم الإلكتروني باســـتخدام لغـــة (VHDL) ، وقورن هذا النموذج بالتفصيل مع تصميمين آخرين أيضاً باستخدام (VHDL) ، وأثبت التصميم المقترح تفوقـــاً في السرعة بالرغم من أنه يعتبر الأكبر مساحة.

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

درجة الماجستير في العلوم

جامعة الملك فهد للبترول والمعادن

الظهران – المملكة العربية السعودية

شعبان ١٤١٩هـ

Contents

List of Figures

Vita

❋ ***Adnan Abdul-Aziz M. S. Gutub***

❋ Received Bachelor of Science in Electrical Engineering from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in January 1995.

❋ Working as a Graduate Assistant in Computer Engineering Department at KFUPM since May 1995.

❋ Started Computer Engineering graduate program in January 1996.

❋ Completed the Master of Science in Computer Engineering from KFUPM in December 1998.

نبذة أكاديمية عن الباحث

* عدنان بن عبدالعزيز بن محمد صديق قطب
* حصل على درجة بكالوريوس علوم في الهندسة الكهربائية من جامعة الملك فهد للبترول والمعادن، الظهران، المملكة العربية السعودية في شعبان 1415 هـ
* يعمل كمعيد بقسم هندسة الحاسب الآلي في جامعة الملك فهد للبترول والمعادن منذ غرة شهر ذوالحجة 1415هـ
* أكمل متطلبات درجة الماجستير في علوم هندسة الحاسب الآلي في رجب 1419هـ