

# 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

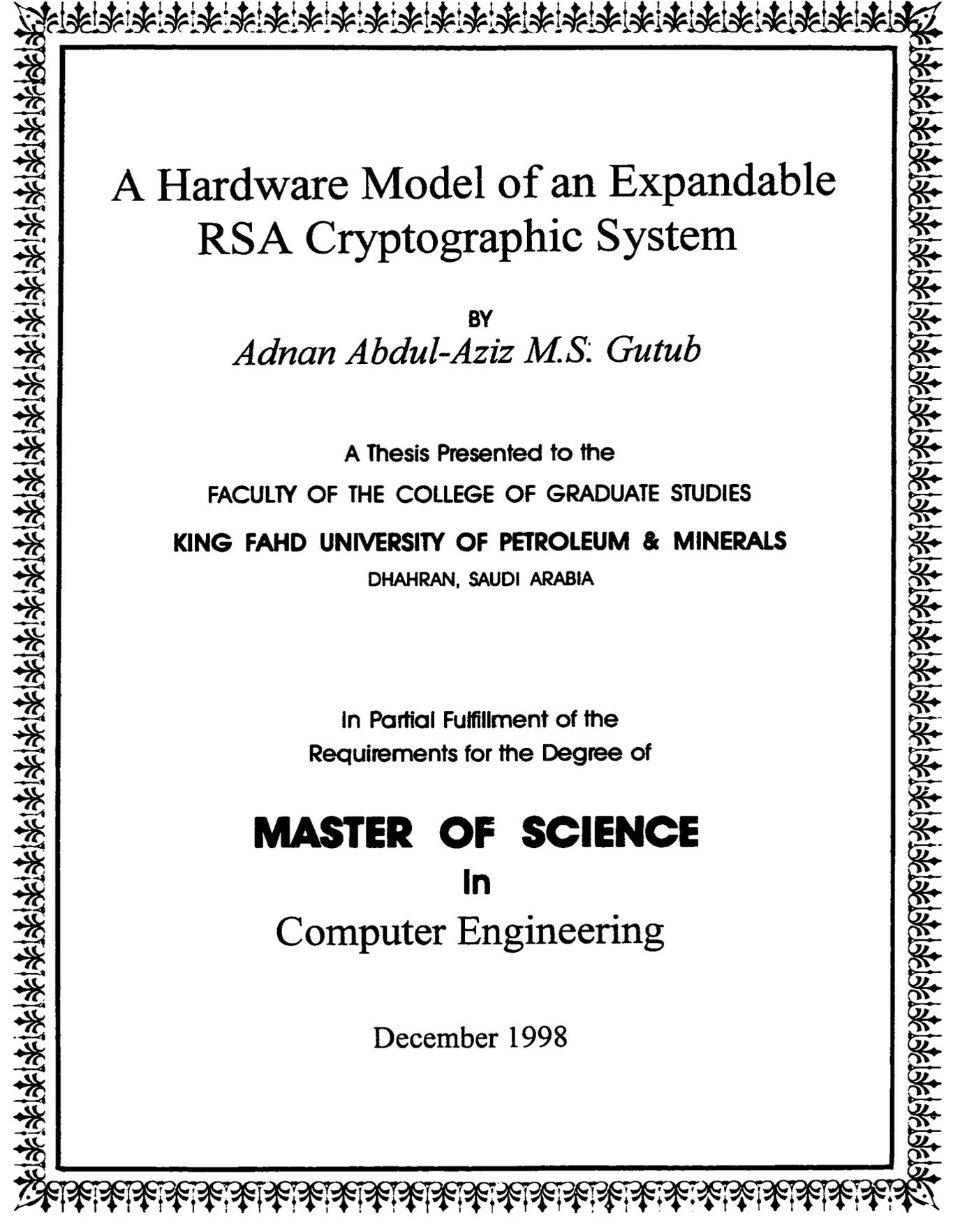
In Partial Fulfillment of the  
Requirements for the Degree of

**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:

*Alaa Amin* 27.12.98  
Dr. Alaaeldin Amin (Chairman)

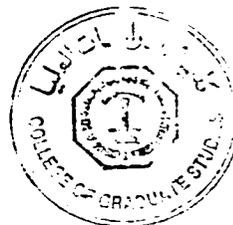
*Khalid Elleithy* 27.12.98  
Dr. Khalid Elleithy (Member)

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

*Abdullah Almajed*  
Department Chairman

*[Signature]*  
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

- الاسم : عدنان بن عبدالعزيز بن محمد صديق قطب  
عنوان الرسالة : تصميم دائرة إلكترونية دقيقة قابلة للتطوير حسب الحاجة لعملية  
التشفير بنظام RSA  
التخصص : هندسة الحاسب الآلي  
تاريخ الشهادة : شعبان ١٤١٩هـ

التشفير (Cryptography) هو الأسلوب الأمثل لحماية المعلومات والحفاظ على سريتها. وأحد أنجح طرق 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، وهي 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 الدقيقة حسب الحاجة، بحيث تم تمثيل هذا التصميم باستعمال نموذج محاكاة التصميم الإلكتروني باستخدام لغة (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 التصميم الثلاثة من حيث كفاءة الأداء والسرعة و التكلفة (التكلفة = المساحة × السرعة)، وأظهر التصميم المقترح نتائج مقارنة 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 . . . . .	ix
List of Tables . . . . .	xi
Abstract (English) . . . . .	xii
Abstract (Arabic) . . . . .	xiii
<b>1 Introduction</b>	<b>1</b>
1.1 Thesis Objective . . . . .	2
1.2 Thesis Outline . . . . .	2
<b>2 Cryptographic Systems</b>	<b>4</b>
2.1 Introduction . . . . .	4
2.1.1 Substitution . . . . .	5
2.1.2 Transposition . . . . .	6
2.2 Public Key Cryptosystems . . . . .	6
2.2.1 Fundamental Operators . . . . .	7
2.2.2 Historical Background . . . . .	8
2.3 The RSA System . . . . .	9
2.3.1 RSA Encryption . . . . .	10
2.3.2 Generation of the RSA Keys . . . . .	10
2.3.3 Example on Encryption Using RSA System . . . . .	10
2.3.4 The RSA Digital Signature Scheme . . . . .	11
2.3.5 Security of the RSA Cryptosystem . . . . .	12
2.3.6 RSA Speed . . . . .	12

2.4	Summary . . . . .	12
<b>3</b>	<b>Review of RSA Hardware Implementations</b>	<b>13</b>
3.1	Introduction . . . . .	13
3.2	General Techniques for Modular Operations . . . . .	14
3.2.1	The Repeated Squaring Algorithm . . . . .	14
3.2.2	General Modular Multiplication Techniques . . . . .	15
3.3	Logarithmic Speed Implementation . . . . .	17
3.3.1	The Algorithm . . . . .	17
3.3.2	The Implementation . . . . .	18
3.4	Implementations of Montgomery's Algorithm . . . . .	18
3.4.1	Montgomery's Algorithm For Exponentiation . . . . .	18
3.4.2	Montgomery's Algorithm Hardware Designs . . . . .	19
3.5	Full RSA Implementations . . . . .	20
3.6	Systolic Arrays for Modular Exponentiation . . . . .	21
3.6.1	Systolic Array for Multiplication . . . . .	21
3.6.2	Montgomery Reduction by the Systolic Multiplier . . . . .	22
3.7	Summary . . . . .	24
<b>4</b>	<b>A Hardware Model of an Expandable RSA Cryptographic System</b>	<b>26</b>
4.1	Introduction . . . . .	26
4.2	The Systolic Multiplier . . . . .	27
4.2.1	The Basic Cell of The Systolic Multiplier . . . . .	28
4.2.2	The b-bit Parallel Multiplier . . . . .	29
4.3	Montgomery Product Design . . . . .	29
4.3.1	Montgomery Product Implementation . . . . .	31
4.3.2	Expandability of the parallel MP Implementation . . . . .	32
4.3.3	The Expandable MP Design . . . . .	33
4.4	The Modular Exponentiation System . . . . .	35
4.4.1	The Basic Exponentiation Processor . . . . .	36

4.4.2	The Expansion hardware . . . . .	37
4.4.3	The Expandable MP Module . . . . .	37
4.5	Summary . . . . .	37
<b>5</b>	<b>Other Implementations</b>	<b>39</b>
5.1	Introduction . . . . .	39
5.2	The Merged Exponentiation Hardware . . . . .	39
5.2.1	The Merged Montgomery Product Algorithm . . . . .	40
5.2.2	The Merged MP Implementation . . . . .	41
5.2.3	The Multiplication Loop Implementation . . . . .	43
5.2.4	The Reduction Loop Implementation . . . . .	44
5.2.5	The Merged Exponentiation Implementation . . . . .	46
5.3	The Add/Subtract Exponentiation Design . . . . .	46
5.3.1	The Add/Subtract Reduction Unit Implementation . . . . .	47
5.3.2	The Add/Subtract Multiplication Implementation . . . . .	47
5.3.3	The Modular Add/Subtract Exponentiation Implementation . . . . .	49
5.4	Summary . . . . .	50
<b>6</b>	<b>Modeling and Analysis</b>	<b>51</b>
6.1	Introduction . . . . .	51
6.2	Implementation Area . . . . .	51
6.2.1	Area of The RSA Implementations . . . . .	54
6.3	Speed and Cost . . . . .	55
6.3.1	The Expandable Hardware Cost . . . . .	56
6.3.2	The Merged Exponentiation Design Cost . . . . .	56
6.3.3	The Add/Subtract Exponentiation Design Cost . . . . .	57
6.4	VHDL Modeling . . . . .	57
6.5	Analysis . . . . .	59
6.5.1	Area and Delay . . . . .	59
6.5.2	The Implementations Cost . . . . .	60

6.6 Summary . . . . .	62
<b>7 Conclusion and Future Work</b>	<b>64</b>
7.1 Conclusion . . . . .	64
7.2 Future Work . . . . .	65
Bibliography . . . . .	66
Vita . . . . .	70

# List of Figures

2.1	The information flow in a classical cryptographic system . . . . .	4
2.2	Public key cryptographic system (general concept) . . . . .	8
3.1	The repeated squaring algorithm . . . . .	14
3.2	The improved repeated squaring algorithm . . . . .	15
3.3	The multiplication with reduction modified algorithm . . . . .	16
3.4	Montgomery's algorithm for modular exponentiation . . . . .	18
3.5	The systolic array . . . . .	21
3.6	The algorithm for a cell behavior . . . . .	22
3.7	The systolic Montgomery reduction . . . . .	23
3.8	Sauerbrey's implementation of Montgomery modular multiplication . .	24
4.1	The word-serial multiplier (systolic array) . . . . .	27
4.2	Expandability of the systolic multiplier . . . . .	27
4.3	Hardware design of the cell . . . . .	28
4.4	Hardware design of 4-bits parallel multiplier . . . . .	30
4.5	The MP-algorithm (Montgomery Product) . . . . .	31
4.6	The signal flow graph . . . . .	31
4.7	The signal flow graph MP implementation (parallel hardware) . . . . .	32
4.8	Expandability of the parallel implementation . . . . .	33
4.9	Projecting all parallel and systolic multipliers into one . . . . .	33
4.10	The expandable serial MP implementation . . . . .	34
4.11	Expandable shift registers design . . . . .	34

## 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 1415 هـ
- \* أكمل متطلبات درجة الماجستير في علوم هندسة الحاسب الآلي في رجب 1419 هـ