A PARALLEL VERSION OF A BINARY METHOD AND VECTOR ADDITION CHAINS PRECOMPUTATION FOR EXPONENTIATION IN RSA

PREPARED BY:

SITI KHATIJAH NOR BINTI ABDUL RAHIM
SITI ROZANAE BINTI ISMAIL

MARCH 2006

UNIVERSITI TEKNOLOGI MARA
CAWANGAN PERAK
KAMPUS SERI ISKANDAR

PEJABAT PENGARAH KAMPUS
32600 BOTA, PERAK DARUL RIDZUAN

Tel: 05-3742001 Faks : 05-3742211
E-Mail :drabdullah@perak.uitm.edu.my

Surat Kami : 100-CPK(HEA. 9/19)
Tarikh : 10 Jun 2004

Puan Siti Khatijah Nor binti Abdul Rahim
Pensyarah
Fakulti Teknologi Maklumat dan Sains Kuantitatif
UiTM Cawangan Perak.

Tuan/Puan

TAJUK PROJEK : A PARALLEL VERSION OF A BINARY METHOD AND VECTOR ADDITION CHAINS PRECOMPUTION FOR EXPONENTIATION IN RSA.

Dengan hormatnya perkara di atas dirujuk.

Sukacita dimaklumkan bahawa Mesyuarat Jawatankuasa Penyelidikan dan Perundingan UiTM Cawangan Perak pada 13 Mei 2004 telah membuat keputusan seperti berikut:

1. Bersetuju meluluskan cadangan penyelidikan yang telah dikemukakan oleh Puan dan Puan Siti Rozanae bt. Ismail.
2. Tempoh projek penyelidikan ini ialah **12 bulan**, iaitu mulai 15 Jun 2004 hingga 16 Mei 2005.
3. Kos yang diluluskan ialah sebanyak **RM19,955.92.**
4. Penggunaan geran diluluskan hanya akan diproses setelah perjanjian ditandatangani.
5. Semua pembelian peralatan yang kosnya **melebihi** RM500.00 satu item perlu menggunakan pesanan Jabatan Universiti Teknologi MARA (LO). Pihak tuan/puan juga dikehendaki mematuhi peraturan penerimaan peralatan.
6. Kertas kerja boleh dibentangkan setelah 75% deraf awal laporan akhir projek siap. Walaubagaimana pun, tuan/puan perlu membuat permohonan kepada Unit Penyelidikan dan Perundingan untuk pembentangan.
7. Pihak tuan/puan dikehendaki mengemukakan Laporan Kemajuan Projek Penyelidikan dari masa ke semasa. Laporan akhir pula perlu dihantar sebaik sahaja projek penyelidikan disiapkan.

Tarikh : 28 Mac 2006
No. Fail Projek : 100-CPK(HEA.9/19)

Penolong Naib Canselor (Penyelidikan)
Institut Penyelidikan, Pembangunan dan Pengkomersilan
Universiti Teknologi MARA
40450 Shah Alam

Ybhg. Prof.,

LAPORAN AKHIR PENYELIDIKAN "A PARALLEL VERSION OF A BINARY METHOD AND VECTOR ADDITION CHAINS PRECOMPUTATION FOR EXPONENTIATION IN RSA"

Merujuk kepada perkara di atas, bersama-sama ini disertakan 3 (tiga) naskah Laporan Akhir Penyelidikan bertajuk "A Parallel Version of A Binary Method and Vector Addition Chains Precomputation For Exponentiation in RSA".

Sekian, terima kasih.

Yang benar,

SITI KHATIJAH NOR BINTI ABDUL RAHIM
Ketua
Projek Penyelidikan

LIST OF CONTENTS

Surat Tawaran Penyelidikan ii

Surat Penyerahan Laporan v

Daftar Ahli Penyelidik vi

Acknowledgement vii

List of contents viii

List of figures x

List of tables xi

Abstract xii

1.0 Introduction 1

1.1 Cryptography 3

1.1.1 Secret key Cryptography (Conventional) 3

1.1.2 Public Key Cryptography 4

2.0 Exponentiation 7

3.0 An Overview of RSA 9

3.1 RSA Algorithm 10

3.2 Modular Exponentiation 13

3.3 Exponentiation in RSA 14

3.4 The Binary Method 14

3.5 Addition Chains 17

3.6 Vector Addition Chains 18

4.0 An Overview of Parallel Computing 20

4.1 Machine Architectures for Parallel Computing 20

Abstract

Exponentiation is a fundamental operation that exists in most computational number theory. It is one of the dominant parts of algorithms for key exchange, electronic signatures and authentication in cryptography. Encryption and decryption in RSA is achieved through exponentiation. There are various approaches to achieve exponentiation. One of those is the Binary Method. In this project, we implemented a parallel version of this Binary Method. Exponentiation can be time consuming; however it depends on the algorithms and the implementation used. Precomputing some of the powers is an option to speed up exponentiation which can save time too. However, we also constructed an algorithm for a parallel version of Vector Addition Chains to enhance the performance. Prior to that, a study on the existing sequential version was conducted and analyzed. It has been proven that a significant speedup were achieved using this new approach.