



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**ANALISA PERBANDINGAN DAN IMPLEMENTASI
ALGORITMA KRIPTOGRAFI RC4, RC4-2S,
DAN RC4ITZ PADA ARSITEKTUR
MULTIPROSESOR**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar

Sarjana Komputer (S.Kom.)



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

Joshua Alamsyah

12110110094

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2016**

HALAMAN PEGESAIHAN SKRIPSI

ANALISA PERBANDINGAN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4, RC4-2S, DAN RC4ITZ PADA ARSITEKTUR MULTIPROSESOR

Oleh

Nama : Joshua Alamsyah
NIM : 12110110094
Program Studi : Teknik Informatika
Fakultas : Teknologi Informasi dan Komunikasi

Tangerang, 22 Agustus 2016

Ketua Sidang

Dosen Penguji

Seng Hansun, S.Si., M.Cs.

Marcel Bonar Kristanda, S.Kom., M.Sc.

Dosen Pembimbing I

Dosen Pembimbing II



Hargyo Nugroho, S.Kom., M.Sc.



Ranny, S.Kom., M.Kom.

Mengetahui,

Ketua Program Studi
Teknik Informatika



Maria Irmina Prasetyowati, S.Kom., M.T.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Joshua Alamsyah

NIM : 12110110094

Program Studi : Teknik Informatika

Fakultas : Teknologi Informasi dan Komunikasi

menyatakan bahwa skripsi yang berjudul "Analisa Perbandingan dan Implementasi Algoritma Kriptografi RC4, RC4-2S, dan RC4itz pada Arsitektur Multiprosesor" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari ditemukan kecurangan atau penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 22 Agustus 2016



Joshua Alamsyah



KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul “Analisa Perbandingan dan Implementasi Algoritma Kriptografi RC4, RC4-2S, dan RC4itz pada Arsitektur Multiprosesor” dengan baik.

Dalam menyusun skripsi ini penulis mendapat banyak bantuan dari berbagai pihak, oleh sebab itu izinkan penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Dr. Ninok Laksono, selaku Rektor Universitas Multimedia Nusantara.
2. Kanisius Karyono, S.T., M.T., Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Maria Irmina Prasetyowati, S.Kom, M.T., selaku ketua program studi Teknik Informatika Universitas Multimedia Nusantara.
4. Hargyo Nugroho, S.Kom., dan Ranny, S.Kom., M.Kom., M.Sc., selaku dosen-deosen pembimbing yang telah membimbing pembuatan skripsi dan memberi arahan dan saran selama proses skripsi sehingga skripsi ini dapat terselesaikan tanpa adanya halangan.
5. Sahabat-sahabat penulis yang saling memberikan dukungan dan bantuan dalam menyelesaikan skripsi.
6. Dosen dan pegawai Universitas Multimedia Nusantara yang telah membantu penulis sehingga skripsi ini dapat terselesaikan.
7. Orang tua dan keluarga penulis yang telah memberikan banyak bantuan dan dukungan kepada penulis.
8. Pihak-pihak lain yang tidak dapat disebutkan satu per satu dan telah membantu penulis dan memberikan dukungan selama pengerjaan skripsi.

Semoga skripsi ini dapat bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca, terutama rekan-rekan mahasiswa di Universitas Multimedia Nusantara.

Tangerang, Agustus 2016



Joshua Alamsyah



ANALISA PERBANDINGAN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4, RC4-2S, DAN RC4ITZ PADA ARSITEKTUR MULTIPROSESOR

ABSTRAK

Kriptografi atau enkripsi merupakan salah satu metode pengamanan dokumen berbentuk digital. Salah satu algoritma enkripsi berbentuk *stream cipher* adalah RC4. Kecepatan dari algoritma RC4 dalam melakukan proses enkripsi merupakan salah satu hal yang disegani oleh pengguna. Namun, seiring waktu, terdapat serangan-serangan yang memanfaatkan kelemahan dari algoritma RC4 seperti serangan korelasi *state tables*. Oleh sebab tersebut, dirancanglah varian dari algoritma RC4 yaitu RC4-2S dan RC4itz. Arsitektur multiprosesor merupakan sebuah arsitektur yang menggunakan prosesor dari CPU dan juga GPU untuk melakukan komputasi. Implementasi algoritma-algoritma kriptografi RC4 dan variannya dalam arsitektur multiprosesor dipilih untuk meningkatkan performa dari algoritma RC4 dan variannya. Dari permasalahan sebelumnya, disusunlah penelitian untuk menganalisa perbandingan RC4, RC4-2S, dan RC4itz dalam sebuah implementasi arsitektur multiprosesor dengan menggunakan API CUDA. Penelitian dilakukan dalam empat uji coba dan mengenkripsi dokumen digital berbentuk pdf dengan ukuran berbeda. Setelah uji coba telah selesai dilaksanakan, diperoleh hasil akhir berupa rata-rata peningkatan tertinggi sebesar 1585% untuk algoritma RC4, peningkatan tertinggi sebesar 2808% untuk algoritma RC4-2S, dan peningkatan tertinggi sebesar 5181% untuk algoritma RC4itz dalam implementasi algoritma pada arsitektur multiprosesor serta hasil analisa perbandingan performa dari algoritma kriptografi RC4, RC4-2S, dan RC4itz.

Kata Kunci: Arsitektur Multiprosesor, CUDA, Kriptografi, RC4, RC4-2S, RC4itz



ANALYSIS AND IMPLEMENTATION OF RC4, RC4-2S, AND RC4ITZ CRYPTOGRAPHIC ALGORITHM IN A MULTIPROCESSOR ARCHITECTURE

ABSTRACT

Cryptography or encryption is a method of securing a digital document. RC4 is a *stream cipher* based encryption algorithm. One of the key factors of RC4 was its speed in encrypting data. As the algorithm was gradually being used, there has been attacks that exploited the weaknesses of the algorithm such as the ‘state-table correlation’ attack. As a result, variants of RC4 algorithm such as RC4-2S and RC4itz were developed to overcome RC4’s weakness and improve its performance. A multiprocessor architecture make use of the processing power of CPU and GPU to make computations. Implementation of each algorithm in the multiprocessor architecture was proposed in order to increase the performance of RC4 and its variants. For the reasons stated above, a research was conducted in order to analyse the different performance of each encryption algorithm in a multiprocessor architecture implementation using the CUDA API. Four experiments were conducted to implement RC4, RC4-2S and RC4itz in the multiprocessor architecture by encrypting different sized digital documents. The result of the research was a maximum average increase of 1585% for RC4’s performance, 2808% increase for RC4-2S’ performance, and 5181% increase for RC4itz’s performance for their implementation in a multiprocessor architecture as well as a performance analysis for each encryption.

Key Words: CUDA, Cryptography, Multiprocessor Architecture, RC4, RC4-2S, RC4itz



DAFTAR ISI

HALAMAN PEGESAHAN SKRIPSI.....	ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	iii
KATA PENGANTAR.....	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xiii
DAFTAR RUMUS	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah	6
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan	7
BAB II LANDASAN TEORI.....	9
2.1 Enkripsi	9
2.2 Stream Cipher Encryption.....	9
2.3 RC4	10
2.4 RC4-2S.....	13
2.5 RC4itz	17
2.6 Arsitektur Multiprosesor	22
2.6.1 Single-instruction Stream, Single-data Stream	23
2.6.2 Single-instruction Stream Multiple-data Stream.....	24
2.6.3 Multiple-instruction Stream, Single-data Stream.....	24
2.6.4 Multiple-instruction Stream, Multiple-data Stream	25
2.7 GPGPU.....	25
2.8 CUDA	26
2.9 Arsitektur Memori GPU dan Sistem Memori CUDA	30
BAB III METODE DAN PERANCANGAN IMPLEMENTASI PROGRAM....	32

3.1 Metode Penelitian	32
3.2 Analisa Program	34
3.2.1 Perancangan Analisa Algoritma RC4.....	35
3.2.2 Perancangan Analisa Algoritma RC4-2S	37
3.2.3 Perancangan Analisa Algoritma RC4itz.....	39
3.3 Perancangan Program pada Arsitektur Multiprosesor	42
3.3.1 Perancangan Uji Coba Menggunakan File-Splitting.....	44
3.3.2 Perancangan Uji Coba Menggunakan File-Indexing	49
3.3.3 Perancangan Uji Coba File-Indexing dengan Pengurangan Jumlah Array.....	54
3.3.4 Perancangan Uji Coba dengan Perubahan Jumlah Proses Paralel	60
3.3.5 Perancangan Analisa Hasil Implementasi	60
BAB IV IMPLEMENTASI DAN ANALISA PROGRAM.....	61
4.1 Implementasi Uji Coba Menggunakan File-Splitting.....	61
4.2 Implementasi Uji Coba Menggunakan File-Indexing	69
4.3 Implementasi Uji Coba File-Indexing dengan Pengurangan Jumlah Array	78
4.4 Implementasi Uji Coba dengan Perubahan Jumlah Proses Paralel	89
4.4.1 Analisa Algoritma RC4 pada Uji Coba Penambahan Proses Paralel....	91
4.4.2 Analisa Algoritma RC4-2S pada Uji Coba Penambahan Proses Paralel.....	95
4.4.3 Analisa Algoritma RC4itz Pada Uji Coba Penambahan Proses Paralel	98
4.5 Analisa Perbandingan Algoritma RC4, RC4-2S, dan RC4itz.....	102
BAB V SIMPULAN DAN SARAN.....	109
5.1 Simpulan	109
5.2 Saran	110
DAFTAR PUSTAKA	111
LAMPIRAN	113

DAFTAR GAMBAR

Gambar 2.1 Struktur sederhana <i>stream-cipher</i>	10
Gambar 2.2 Pseudocode <i>key-scheduling</i>	11
Gambar 2.3 Pseudocode <i>pseudo-random generation</i>	12
Gambar 2.4 Pseudocode <i>key-scheduling</i> RC4-2S.....	14
Gambar 2.5 Pseudocode PRG RC4-2S	15
Gambar 2.6 Pseudocode <i>key-scheduling</i> RC4itz	18
Gambar 2.7 Pseudocode fungsi ‘SkipOutput’ RC4itz	19
Gambar 2.8 Pseudocode PRG RC4itz.....	21
Gambar 2.9 Arsitektur SISD	23
Gambar 2.10 Arsitektur SIMD	24
Gambar 2.11 Arsitektur MISD	24
Gambar 2.12 Arsitektur MIMD	25
Gambar 2.13 Alur proses kerja pada CUDA	27
Gambar 2.14 Arsitektur CUDA	29
Gambar 3.1 <i>Flowchart</i> Alur Algoritma RC4	36
Gambar 3.2 <i>Flowchart</i> Alur Algoritma RC4-2S	38
Gambar 3.3 <i>Flowchart</i> Alur Algoritma RC4itz.....	41
Gambar 3.4 Alur Pelaksanaan Uji Coba	43
Gambar 3.5 <i>Flowchart</i> Proses Program pada <i>Host</i> dalam Uji Coba menggunakan <i>File-Splitting</i>	46
Gambar 3.6 <i>Flowchart</i> Algoritma pada <i>Device</i> dalam Uji Coba menggunakan <i>File-Splitting</i>	48
Gambar 3.7 <i>Flowchart</i> Proses Program pada <i>Host</i> pada Uji Coba menggunakan <i>File-Indexing</i>	51
Gambar 3.8 <i>Flowchart</i> Algoritma pada <i>Device</i> dalam Uji Coba menggunakan <i>File-Indexing</i>	53
Gambar 3.9 <i>Flowchart</i> Proses Program pada <i>Host</i> pada <i>Uji Coba</i> menggunakan <i>File-Indexing</i> dengan Pengurangan <i>Array</i>	56
Gambar 3.10 <i>Flowchart</i> Algoritma pada <i>Device</i> dalam Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	58
Gambar 4.1 Deklarasi <i>Library</i> dan Variabel pada <i>Host</i>	61
Gambar 4.2 Fungsi ‘Allocate_Memory’ <i>Host</i>	62
Gambar 4.3 Alokasi Memori <i>Device</i>	63
Gambar 4.4 Pemanggilan Proses <i>Device</i>	64

Gambar 4.5 Proses Enkripsi RC4 pada <i>Device</i>	65
Gambar 4.6 Proses <i>Key-Scheduling</i> RC4-2S pada <i>Device</i>	66
Gambar 4.7 Proses PRGA RC4-2S pada <i>Device</i>	66
Gambar 4.8 Proses Enkripsi RC4itz pada <i>Device</i>	67
Gambar 4.9 Proses cudaFree pada <i>Host</i>	68
Gambar 4.10 Perubahan Deklarasi Variabel dan Struktur pada Uji Coba menggunakan <i>File-Indexing</i>	69
Gambar 4.11 Perubahan pada Fungsi Allocate_Memory Uji Coba menggunakan <i>File-Indexing</i>	70
Gambar 4.12 Perubahan pada Proses Alokasi dan Pegiriman Data Uji Coba dengan <i>File-Indexing</i>	71
Gambar 4.13 Perubahan <i>Parameter</i> pada Fungsi <i>Device</i> pada Uji Coba dengan <i>File-Indexing</i>	72
Gambar 4.14 Perubahan pada Pemanggilan <i>Device</i> pada Uji Coba dengan <i>File-Indexing</i>	72
Gambar 4.15 Perubahan Proses PRGA RC4 pada Uji Coba dengan <i>File-Indexing</i>	73
Gambar 4.16 Perubahan Proses PRGA RC4-2S pada Uji Coba dengan <i>File-Indexing</i>	73
Gambar 4.17 Perubahan Proses PRGA RC4itz pada Uji Coba dengan <i>File-Indexing</i>	74
Gambar 4.18 Grafik Waktu Enkripsi Terhadap Ukuran Data Uji Coba dengan <i>File-Indexing</i>	76
Gambar 4.19 Grafik Selisih Waktu Enkripsi Sekuensial dan Multiprosesor Uji Coba dengan <i>File-Indexing</i>	77
Gambar 4.20 Perubahan Deklarasi Variabel pada Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	79
Gambar 4.21 Perubahan Fungsi Allocate_Memory pada Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	79
Gambar 4.22 Perubahan Proses PRGA RC4 pada Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	81
Gambar 4.23 Perubahan Proses PRGA RC4-2S pada Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	82
Gambar 4.24 Perubahan Proses PRGA RC4itz pada Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	83
Gambar 4.25 Grafik Waktu Enkripsi Terhadap Ukuran Data Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	85

Gambar 4.26 Grafik Waktu Enkripsi terhadap Ukuran Data Uji Coba <i>File-Indexing</i> dan <i>File-Indexing</i> dengan Pengurangan <i>Array</i>	86
Gambar 4.27 Grafik Selisih Waktu Enkripsi Sekuensial dan Multiprosesor Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah <i>Array</i>	87
Gambar 4.28 Grafik Selisih Waktu Enkripsi Antara Uji Coba <i>File-Indexing</i> dan <i>File-Indexing</i> dengan Pengurangan <i>Array</i>	88
Gambar 4.29 Grafik Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4	92
Gambar 4.30 Grafik Garis Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4	93
Gambar 4.31 Grafik <i>Throughput</i> Untuk Algoritma RC4 Uji Coba Penambahan Jumlah Proses Paralel dan Sekuensial	94
Gambar 4.32 Grafik Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4-2S	95
Gambar 4.33 Grafik Garis Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4-2S.....	96
Gambar 4.34 Grafik <i>Throughput</i> Untuk Algoritma RC4-2S Uji Coba Penambahan Proses Paralel dan Sekuensial	97
Gambar 4.35 Grafik Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4itz.....	99
Gambar 4.36 Grafik Garis Rata-Rata Waktu Enkripsi Jumlah Proses Paralel Terhadap Ukuran Data RC4itz	100
Gambar 4.37 Grafik <i>Throughput</i> Untuk Algoritma RC4-2S Uji Coba Penambahan Proses Paralel dan Sekuensial	101
Gambar 4.38 Grafik Rata-Rata <i>Throughput</i> Algoritma RC4, RC4-2S, dan RC4itz Terhadap Jumlah Proses Paralel	103
Gambar 4.39 Grafik Peningkatan Nilai <i>Throughput</i> Algoritma pada Arsitektur Multiprosesor terhadap Algoritma Sekuensial	104
Gambar 4.40 Grafik Pertumbuhan dari Peningkatan Nilai <i>Throughput</i> Algoritma Untuk Setiap Penambahan Jumlah Proses	106

DAFTAR TABEL

Tabel 2.1 Tabel Flynn's Taxonomy	22
Tabel 4.1 Rata-Rata Waktu Enkripsi Uji Coba menggunakan <i>File-Indexing</i>	75
Tabel 4.2 Rata-Rata Waktu Enkripsi Algoritma RC4, RC4-2S, dan RC4itz Sekuensial	75
Tabel 4.3 Selisih Waktu Enkripsi Sekuensial dan Multiprosesor.....	76
Tabel 4.4 Rata-Rata Waktu Enkripsi Uji Coba <i>File-Indexing</i> dengan Pengurangan Jumlah Array.....	84
Tabel 4.5 Rata-Rata Waktu Enkripsi RC4 Dengan Perubahan Jumlah Proses Paralel.....	90
Tabel 4.6 Rata-Rata Waktu Enkripsi RC4-2S Dengan Perubahan Jumlah Proses Paralel.....	91
Tabel 4.7 Rata-Rata Waktu Enkripsi RC4itz Dengan Perubahan Jumlah Proses Paralel.....	91
Tabel 4.8 <i>Throughput</i> RC4 Dengan Perubahan Jumlah Proses Paralel dan Ukuran Data	93
Tabel 4.9 Nilai <i>throughput</i> Algoritma RC4, RC4-2S, dan RC4itz Sekuensial	94
Tabel 4.10 <i>Throughput</i> RC4-2S Dengan Perubahan Jumlah Proses Paralel dan Ukuran Data.....	97
Tabel 4.11 <i>Throughput</i> RC4itz Dengan Perubahan Jumlah Proses Paralel dan Ukuran Data.....	100
Tabel 4.12 Rata-Rata <i>Throughput</i> Algoritma RC4, RC4-2S, dan RC4itz Terhadap Jumlah Proses Paralel.....	102
Tabel 4.13 Rata-Rata Nilai <i>Throughput</i> Algoritma RC4, RC4-2S, dan RC4itz Sekuensial	103
Tabel 4.14 Peningkatan Nilai <i>Throughput</i> Algoritma pada Arsitektur Multiprosesor terhadap Algoritma Sekuensial	103

DAFTAR RUMUS

Rumus 2.1 Rumus Enkripsi <i>Stream-Cipher</i>	12
Rumus 3.1 Rumus Kompleksitas Algoritma RC4	35
Rumus 3.2 Rumus Kompleksitas Algoritma RC4-2S.....	37
Rumus 3.3 Rumus Kompleksitas Algoritma RC4itz	41
Rumus 3.4 Rumus Perhitungan <i>Index Proses Paralel Device</i>	48
Rumus 3.5 Rumus Perhitungan Posisi Data pada <i>File-Indexing</i>	58

