PERANCANGAN DAN IMPLEMENTASI KRIPTOGRAFI ALGORITMA A5/2 BERBASIS FPGA (FIELD PROGRAMMABLE GATE ARRAYS)

Surya Lasmara[1], M.ary Murti[2], Iwan Iwut Tirtoasmoro[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Metoda kriptografi yang digunakan untuk meningkatkan keamanan informasi baik suara maupun teks pada sistem telepon seluler GSM (Global System for Mobile Communication) adalah dengan menggunakan algoritma kriptografi A5. Algoritma A5 merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama. Algoritma A5 dibagi menjadi A5/1, A5/2, dan Versi terbarunya yaitu A5/3.

Tugas akhir ini merepresentasikan rancangan algoritma A5/2 yang dapat melakukan proses enkripsi dan deskripsi dalam satu sistem. Rancangan ini menggunakan mode operasi LFSR (Liniear Feedback Shift Register) yang digunakan untuk pembangkit deretan bilangan acak, dan akan dimodelkan dengan menggunakan bahasa VHDL (Very High Speed Integrated Circuit Hardware Language). Rancangan ini akan disimulasikan menggunakan Aldec Active HDL 3.5 serta disintesis menggunakan Xilinx ISE 8.1i,dan devais target menggunakan FPGA Virtex-4 seri XC4VLX25-10SF363C

Hasil implementasi rancangan tugas akhir ini dengan menggunakan target divais FPGA Virtex-4 seri XC4VLX25-10SF363C menunjukkan top level entity mampu bekerja pada frekuensi maksimum 198,159 MHz dan membutuhkan slices sebanyak 2% (292 dari10752 slices yang tersedia), serta membutuhkan 6% IOBs (15 dari 240 IOB yang tersedia)

Kata Kunci : Cryptography, GSM (Global System for Mobile Communications, A5,

Abstract

Cryptography method which is used to increasing of information security voice and also teks on GSM communications mobile system is using with A5 algorithm cryptography. A5 algorithm is kind symetry algoritm where key is use for encryption and decryption process is same. A5 algorithm is divided into A5/1, A5/2, and the new version is A5/3..

This final project presents a design of A5/2 algorithm which can doing encryption and decryption process in one system. The design is using LFSR (Linear Feedback Shift Register) operation mode which used as generating concevutive random number, and will be modeled with using VHDL (Very High Speed Integrated Circuit Hardware Language) language. The design is will be simulated using Aldec Active HDL 3.5 and also synthesized using Xilinx ISE 8.1i, and device target using FPGA Virtex-4 XC4VLX25- 10SF363C series.

This final project design implementation result by using device target FPGA Virtex-4 XC4VLX25-10SF363C series show top level entity capable work on maximum frequency 198,159 MHz and required slices 2% (292 out of 10,752), and also required 6% IOBs (15 out of 240).

Keywords : Cryptography, GSM (Global System for Mobile Communications, A5, A5/2,

BAB I
PENDAHULUAN

1.1 Latar Belakang

Komunikasi suara dalam sistem seluler GSM (*Global System for Mobile Communication*) merupakan suatu jenis informasi yang paling banyak diakses selain informasi data teks. Untuk informasi yang bernilai sangat penting, proses pertukarannya harus memperhatikan aspek keamanan dan kerahasiaan. Salah satu metode untuk meningkatkan keamanan informasi baik suara maupun teks adalah dengan teknik kriptografi, dimana data diolah menurut algoritma tertentu sehingga dihasilkan suatu pola data dalam bentuk yang lain sebelum dikirimkan. Pada sistem seluler GSM dibutuhkan suatu algoritma kriptografi yang mampu melakukan pemrosesan data yang cukup cepat dan juga menawarkan tingkat keamanan yang tinggi. Salah satu algoritma kriptografi yang direkomendasikan oleh vendor GSM untuk mengamankan data antara MS (*Mobile Station*) dan BS(*Base Station*) adalah algoritma A5/2.

Algoritma kriptografi A5/2 merupakan teknik kriptografi simetris dan termasuk jenis algoritma *streamchiper* yang merupakan implementasi dari LFSR (*Linear Feedback Shift Register*) dimana proses enkripsi dan deskripsi dilakukan berdasarkan posisi bit per bit dalam aliran data secara seketika (*real time*). Algoritma A5/2 terdiri dari empat LFSR, yaitu: R1, R2, R3, dan R4 dengan panjang bit setiap registernya adalah 19 bit, 22 bit, 23 bit dan 17 bit secara berurutan.

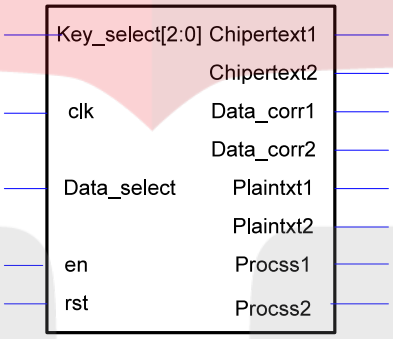
Dalam Tugas Akhir ini dilakukan perancangan dan implementasi sistem kriptografi dengan menggunakan algoritma A5/2 berbasis FPGA.

I.2 Perumusan Masalah

Dalam penulisan Tugas Akhir ini perumusan masalah akan difokuskan pada beberapa hal, yaitu:

1. Perancangan kriptografi algoritma A5/2 dengan menggunakan bahasa pemrograman VHDL (*Very High Speed Integrated Circuit Hardware Description Language*).
2. Implementasi pada FPGA Virtex-4 seri XC4VLX25-10SF363C

   Secara garis besar diagram blok dari sistem yang akan diimplementasikan adalah sebagai berikut:



Gambar 1.1 Blok Sistem yang akan diimplentasikan pada FPGA.

1.3 Batasan Masalah

Dalam Tugas Akhir ini, batasan masalah yang digunakan adalah:

1. Untuk simulasi dan implementasi, kunci yang digunakan adalah data bit sepanjang 64-bit
2. Untuk simulasi dan implementasi, inputan yang digunakan adalah data bit sepanjang 114-bit
3. Pada perancangan dan implementasi tidak digunakan kode koreksi kesalahan, melainkan menggunakan pembanding sebagai cek bit hasil deskripsi.
4. Target device yang digunakan adalah FPGA Virtex-4 seri XC4VLX25-10SF363C.
5. Analisa sistem dilakukan dengan mengamati dan menyimpulkan data bit hasil keluaran sistem dengan data bit inputan dan *avalanche effect*.

1.4 Tujuan Penulisan

Tujuan dari Tugas Akhir ini adalah:

1 Melakukan perancangan algoritma A5/2 dengan bahasa pemrograman VHDL, simulasi dan merealisasikan sistem kriptografi algoritma A5/2 menggunakan board FPGA virtex-4 seri XC4VLX25-10FS363C.

2 Menganalisa sistem dalam hal analisa uji fungsional (simulasi), analisa perubahan bit, analisa frekuensi bit, analisa *avalanche effect*, analisa penggunaan *resource* dan analisa pengamatan keluaran pada FPGA dengan menggunakan *Logic Analyzer*.

1.5 Metode Penulisan

Metodologi yang dilakukan dalam penyusunan Tugas Akhir ini adalah:

1. Studi Literatur

   Pencarian dan pengumpulan literatur yang langsung berkaitan dengan masalah-masalah yang ada pada Tugas Akhir ini baik mengenai algoritma kriptografi A5/2 atau tentang bahasa pemrograman VHDL.

2. Perancangan Sistem

   Perancangan sistem yang sesuai dengan spesifikasi algoritma kriptografi A5/2 dengan bahasa VHDL dengan bantuan *software* Active Aldec-HDL 3.5 dan Xilinx WebPack Project Navigator 8.i. Metode perancangan yang digunakan adalah gabungan antara *top-down* dan *bottom-up.*

3. Simulasi dan implementasi sistem ke board FPGA Virtex-4 seri XC4VLX25-10SF363C

   Setelah sistem selesai dirancang maka akan dilakukan simulasi untuk mengetahui *timing diagram* apakah sesuai dengan spesifikasi dan meng-implementasikan pada board FPGA.

4. Analisa dan penarikan kesimpulan

   Analisa dilakukan dengan membagi ke dalam beberapa bagian yaitu : analisa uji fungsional (simulasi), analisa perubahan bit, analisa frekuensi bit, analisa *avalanche effect*, analisa penggunaan *resource* dan analisa pengamatan keluaran pada FPGA dengan menggunakan *Logic Analyzer.*

1.6 Sitematika Penulisan

Sistematika penulisan untuk Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, maksud dan tujuan, batasan masalah, rumusan masalah, serta sistematika pembahasan dari perancangan sistem.

BAB II DASAR TEORI

Membahas dasar teori yang berhubungan dengan keamanan GSM (*Global System for Mobile Communications*) menggunakan algoritma kriptografi A5/2. Teori dasar ini difokuskan pada teori-teori dasar pada mekanisme, kriptografi dan algoritma A5/2-nya sendiri.

BAB III PERANCANGAN SISTEM

Bab ini akan membahas perancangan enkripsi dan deskripsi algoritma A5/2 dengan menggunakan *software* VHDL yang siap diimplementasikan pada board FPGA.

BAB IV ANALISIS SISTEM

Bab ini akan menjelaskan tentang analisa sistem yang telah dibuat, sehingga dapat diketahui hasil yang didapat pada perancangan dan realisasi sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan terhadap hasil yang diperoleh dari penelitian yang telah dilakukan serta membicarakan saran–saran untuk pengembangan sistem ini lebih lanjut

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari Tugas Akhir yang berjudul : "Perancangan dan Implementasi Kriptografi Algoritma A5/2 Berbasis FPGA *(Field Programmable Gate Array)*" antara lain :

1. Hasil simulasi perancangan menunjukkan bahwa sistem *(top level entity)* dapat melakukan proses enkripsi dan deskripsi yang sesuai dengan spesifikasi perancangan.
2. Berdasarkan analisa statistik chiperteks didapatkan kesimpulan bahwa barisan bit dari chiperteks memiliki jumlah bit '0' dan '1' yang relative sama untuk inputan menggunakan digit '0' semua dan digit '1' semua, serta untuk inputan yang acak output yang diberikan menunjukkan frekuensi kemunculan digit '0' dan digit '1' yang relative sama.
3. Perubahan satu bit kunci memberikan nilai *avalanche effect* untuk algoritma A5/2 dengan pengacakan yang cukup baik (mendekati 50%), karena kunci digunakan sebagai inputan dari algoritma A5/2 yang diiterasi satu persatu secara acak kedalam register A5/2.
4. Perubahan satu bit frame number memberikan nilai *avalanche effect* untuk algoritma A5/2 dengan pengacakan yang cukup baik (mendekati 50%), karena frame number juga digunakan sebagai inputan dari algoritma A5/2 yang diiterasi satu persatu secara acak kedalam register A5/2.
5. Hasil implementasi menggunakan Xilix-ISE Project Navigator 8.1i menunjukkan bahwa maksimum frekuensi *clock* yang boleh digunakan untuk *top level entity* adalah sebesar 198,159 MHz.
6. Slice yang dibutuhkan untuk implementasi dengan menggunakan Xilinx Virtex-4 XC4VLX25 sebanyak 292 *slices* dari 10,752 *slices*, sedangkan IOB total yang digunakan adalah sebanyak 15 IOB dari 240 IOB.
7. Pengamatan pada FPGA dengan menggunakan *Logic Analyzer* didapatkan hasil yang sama dengan hasil simulasi menggunakan Aldec-HDL 3.5.
8. Kemungkinan ditemukannya kunci oleh orang yang tidak diinginkan (Brute Force Attack) dengan asumsi menggunakan PC 3 GHz mampu melakukan enkripsi pertahun sebanyak $3 \times 10^9 \times 3600 \times 24 \times 365 = 94608000000000000$, maka untuk mencoba 2^{64}

kunci membutuhkan waktu sebanyak $(2^{64}/109 * 3)/(60 \times 60 \times 24 \times 365)$ ˜ 194.9808 tahun

5.2 Saran

Setelah melakukan tugas akhir ini ada beberapa saran yang perlu dipertimbangkan untuk pengembangan lebih lanjut, yaitu:

1. Pelu dikembangkan sistem yang mampu *meng-generate* kunci yang lebih dinamis dan lebih banyak kombinasinya.
2. Perlu diperhatikan agar pengkodean dengan menggunakan bahasa VHDL harus dilakukan dengan baik sesuai dengan referensi, dan menghindari penggunaan *type data integer* dan penggunaan *procedure* agar dapat menghemat *slices* yang dipakai di FPGA.

DAFTAR PUSTAKA

[1] Kurniawan, Yusuf, ”Kriptografi Keamanan Internet dan Jaringan Telekomunikasi”, Informatika, Bandung, 2004.

[2] Barkan, Elad; Biham, Eli; Keller, Nathan. *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication.*

[3] Biryukov, A. Shamir, D. Wagner, “Real time cryptanalysis of A5/2 on a PC”, *Lecture Notes in Computer Science*, vol. 1978, 2001, pp. 1–18, (FSE’2000).

[4] E. Biham, O. Dunkelman, “Cryptanalysis of the A5/2 GSM stream Cipher”, *Lecure Notes in Computer Science*, vol. 1977, 2000, pp. 43–51, (Indocrypt 2000).

[5] GSM World, “GSM Security Algorithm”, ICRA GSM Association, 2004, http://www.GSM-World.org

[6] Heine. Gunnar, “GSM Network : Protocols, Terminology and Implementation”, Artech House, Boston London, 1998.

[7] Ian Goldgerg, David Wagner, “ Architectural considerations for cryptanalytic hardware”, http://www.cs.berkeley.edu/iang/isaac/hardware.html, 2004

[8] J. Golic, “Criptanalysis of Alleged A5 Stream Cipher”, proceedings of Eurocrypt’97, LNCS 1233, pp.239(Springer-Verlag 1997).

[9] M. Briceno, I. Goldberg, D. Wagner, “A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms”, scard.org, May 1999.

[10] Tahar Ktari (tahar.ktari@epfl.ch), David Mayor (david.mayor@epfl.ch), “SECURITY IN GSM, GPRS AND 3GPP”, Swiss Federal Institute of Technology, 2004.

[11] http://www.ciphersbyritter.com/RES/SBOXDESN.HTM#Feistel73

[12] http://ww1.microchip.com/downloads/en/AppNotes/91002a.pdf