PERANCANGAN DAN IMPLEMENTASI KRIPTOGRAFI ALGORITMA A5/1 BERBASIS FIELD PROGRAMMABLE GATE ARRAY(FPGA)

Ahmad Qurthobi[1], Muhammad Ary Murti[2], Iwan Iwut Tirtoasmoro[3]

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

---

Abstrak

Sejalan dengan perkembangan teknologi informasi, media komunikasi yang digunakan dan sistem aliran data yang dipakai juga semakin beragam. Perkembangan ini memberikan kemudahan dalam berkomunikasi. Namun, perkembangan ini juga menimbulkan permasalahan baru dibidang keamanan informasi.

Salah satu metode pengamanan data adalah kriptografi. Dengan metode ini, data disamarkan terlebih dahulu sebelum dikirimkan pada media transmisi. Salah satu jenis algoritma kriptografi yang digunakan adalah A5 yang digunakan dalam sistem komunikasi Global System for Mobile communication (GSM). Algoritma A5 dibedakan menjadi 3 jenis yaitu A5/1, A5/2, dan yang terbaru yaitu A5/3.

Pada tugas akhir ini, dilakukan perancangan algoritma A5/1 dengan menggunakan bahasa VHDL dan diimplementasikan pada board Field Programmable Gate Array (FPGA) Virtex-4 seri XC4VLX25-10SF363C. Dilakukan analisa pada keluaran sistem untuk mengetahui nilai avalanche effect, dan frekuensi keluaran dan frekuensi perubahan bit dari informasi yang tersamar. Simulasi dari perancangan dilakukan dengan menggunakan software Aldec-Active HDL 3.5. Sedangkan hasil implementasi akan diamati pada logic analyzer LA- 2124A.

Hasil analisa perancangan menunjukkan sistem memiliki avalanche effect dan frekuensi bit ciphertext yang mendekati 50% dengan frekuensi keluaran bit dan perubahan bit yang mendekati 50%. Hasil synthesis pada bagian enkripsi memerlukan Slices sebanyak 1%, Slice Flip Flops sebanyak 0%, 4 input LUTs sebanyak 1%, bonded IOBs sebanyak 3%, dan GCLKs sebanyak 3% dari resource yang tersedia pada device, dengan frekuensi clock maksimum sebesar 126,173 Mhz. Sedangkan hasil synthesis bagian enkripsi memerlukan Slices sebanyak 1%, Slice Flip Flops sebanyak 0%, 4 input LUTs sebanyak 0%, bonded IOBs sebanyak 2%, dan GCLKs sebanyak 3% dari yang tersedia pada device, dengan frekuensi clock maksimum sebesar 125,796 Mhz.

Kata Kunci : -

Abstract

Along with the expanding of information technology, communication media and data flow system have lot varieties than before. This expand makes make communication easier than before. But, this expands also made a new problem in information security.

One kind of information security method is cryptography. With this method, data is ciphered before it's transmitted. One kind of cryptograph algorithm is A5 which used in Global System for Mobile communication (GSM) and divided into A5/1, A5/2, and the new one, A5/3.

In this final Task will be done a design of A5/1 algorithm using VHDL and then implemented to Field Programmable Gate Array (FPGA) Virtex-4 XC4VLX25-10SF363C series. Encrypt and decrypt process done only for one direction. The output is analyzed to get information about avalanche effect, and the output bit frequency from the ciphered information. Design is simulated using Aldec Active-HDL 3.5 software. And the result of implementation is monitored by using LA-2124A logic analyzer.

The results of design analyzing shows that designed system have almost 50% for avalanche effect ,ciphertext bit frequency, and transformation bit frequency. Synthesis report for encryption part shows the system needs 1% of Slices, 0% of Slice Flip Flops, 1% of 4 input LUTS, 3% of bonded IOBs, and 3% of GLCKs of all resource in device with maximum clock frequency is 126,173 MHz. And synthesis report for decryption part shows the system needs 1% of Slices, 0% of Slice Flip Flops, 0% of 4 input LUTS, 2% of bonded IOBs, and 3% of GLCKs of all resource in device with maximum clock frequency is 125,796 MHz.

Keywords : -

BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah s*ecurity* dalam komunikasi merupakan hal yang sangat penting karena informasi merupakan barang yang sangat berharga bagi setiap individu atau kelompok. Apabila informasi tersebut berhasil didapatkan oleh pihak tertentu secara *illegal* maka akan dapat menimbulkan kerugian. Karena itu, perlu diterapkan suatu cara untuk menjamin keamanan dan legalitas dari pengiriman dan penerimaan informasi.

Semua sistem komunikasi yang ada pada masa sekarang, baik untuk keperluan data, suara, atau multimedia, dituntut untuk menyediakan kemampuan mengacak dalam proses transmisi untuk menghindari pencurian informasi. Tuntutan keamanan ini menyebabkan berkembangnya jenis-jenis algoritma yang digunakan dalam proses pengkodean dengan tujuan menciptakan suatu sistem komunikasi yang aman. Untuk menjaga informasi berupa percakapan atau data penting, salah satu cara yang dilakukan adalah dengan metode kriptografi.

Kriptografi dapat diartikan sebagai suatu metode untuk menyamarkan informasi sehingga tidak mudah diketahui atau dibaca selain pengirim dan penerima yang dituju. Kriptografi telah diterapkan pada banyak hal yang memerlukan tingkat keamanan tinggi untuk pengiriman informasi dalam sistem komunikasi.

Seiring perkembangan teknologi sistem komunikasi, informasi yang dikirimkan pada saluran memiliki karakteristik yang beragam. Sehingga algoritma yang digunakan untuk keperluan keamanan informasi semakin berkembang sesuai dengan karakteristik sistem yang digunakan.

Salah satu jenis algoritma yang dikembangkan dalam komunikasi adalah A5. Algoritma ini dirancang untuk mengamankan transmisi data dalam sistem GSM. Terdapat 3 jenis algoritma A5 yaitu A5/1, A5/2, dan A5/3.

Dalam tugas akhir ini, akan dilakukan perancangan dan implementasi dari algoritma A5/1 pada FPGA dimana proses enkripsi dan dekripsi dibatasi hanya untuk satu arah untuk mengetahui parameter-parameter pada *core* sistem.

1.2 Tujuan

Tujuan dari perancangan sistem yang dilakukan adalah :

1. Melakukan perancangan algoritma A5/1 dengan menggunakan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL).
2. Melakukan *synthesis* dan *implement* terhadap sistem yang dirancang.
3. Mengimplementasikan hasil perancangan kedalam perangkat *Field Programmable Gate Array* (FPGA).
4. Melakukan analisa terhadap kinerja sistem.

1.3 Perumusan Masalah

Permasalahan yang akan dipecahkan dalam tugas akhir ini:

1. Pemodelan algoritma A5/1 dengan menggunakan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL).
2. Jumlah *resource* yang digunakan dalam pengimplementasian pada FPGA.
3. Performansi hasil perancangan dan implementasi pada bagian enkripsi dan deskripsi.

1.4 Batasan Masalah

Pembahasan yang dilakukan dalam tugas akhir ini dibatasi pada:

1. Sistem yang dirancang adalah bagian *stream cipher* dengan menerapkan aturan-aturan sesuai dengan yang terdapat pada algoritma A5/1.
2. Perancangan dilakukan pada bagian enkripsi dan deskripsi.
3. Perancangan dilakukan dengan menggunakan bahasa pemrograman VHDL.
4. Implementasi dilakukan dengan menggunakan FPGA Virtex-4 seri XC4VLX25-10SF363C sebagai devais sasaran.
5. Simulasi dan implementasi menggunakan nilai konstan sebagai kunci.
6. Masukan yang digunakan berbentuk data yang dibangkitkan pada FPGA.
7. Perancangan tidak membahas tentang *smart card* yang diterapkan pada sistem GSM.

1.5 Metodologi

Metode yang dilakukan dalam penyusunan tugas akhir ini adalah:

1. Studi literatur

   Studi literatur mengenai hal-hal yang berhubungan dengan pembahasan algoritma A5/1 dan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL) yang digunakan sebagai bahan referensi.

2. Perancangan dan simulasi

   Perancangan dan simulasi dari tugas akhir ini dilakukan dengan menggunakan software Aldec Active-HDL 3.5.

3. Implementasi

   Implementasi dilakukan pada *board* FPGA Virtex-4 seri XC4VLX25-10SF363C dan kemudian dilakukan pengujian serta analisis kinerja sistem.

1.6 Sistematika Pembahasan

Pembahasan pada perancangan ini akan dibagi menjadi 5 (lima) bab, dengan urutan 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 algoritma kriptografi A5/1 dan penerapannya. Bab ini difokuskan pada teori-teori dasar yang terdapat pada pada mekanisme, kriptografi, algoritma A5/1, dan pengantar dari perangkat yang digunakan.

BAB III : PERANCANGAN SISTEM

Bab ini akan membahas tentang alur perancangan enkripsi dan dekripsi algoritma A5/1 dengan menggunakan *software* VHDL (*Very High Speed Integrated Circuit Hardware Description Language*), dan deskripsi tentang sistem dan sub-sistem yang dirancang.

BAB IV : IMPLEMENTASI DAN ANALISIS

Bab ini menjelaskan tentang pengujian yang dilakukan terhadap sistem kriptografi A5/1 dan menganalisis hasil implementasi tersebut.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil-hasil yang diperoleh pada perancangan yang telah dilaksanakan dan mengemukakan saran-saran yang berguna bagi pengembangan sistem kedepannya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian yang dilakukan dalam pengerjaan Tugas Akhir berjudul "Perancangan dan Implementasi Kriptografi Menggunakan Algoritma A5/1 Berbasis *Field Programmable Gate Array* (FPGA)" diperoleh kesimpulan sebagai berikut:

1. Proses enkripsi dilakukan dengan meng-*xor* data masukan awal dengan *stream cipher* yang dihasilkan oleh blok penghasil *stream cipher* yang menggunakan algoritma A5/1 sebagai penghasil nilainya. Dan dengan menggunakan nilai strem cipher yang sama, dekripsi dilakukan untuk mengembalikan data hasil enkripsi ke bentuk semula.
2. Hasil simulasi dan implementasi menunjukkan terjadinya *delay* yang diakibatkan oleh adanya waktu yang diperlukan saat terjadi pembacaan sinyal dimana *delay* yang terjadi pada proses enkripsi dan dekripsi sebesar 1 siklus *clock*. Sehingga diperlukan sinkronisasi untuk menyesuaikan pembacaan.
3. Nilai *avalanche effect* untuk perubahan 1 bit *key* atau perubahan 1 bit *frame number* mendekati 50%.
4. Frekuensi keluaran bit yang dihasilkan pada *ciphertext* dari hasil pengujian menunjukkan nilai yang mendekati 50% baik untuk bit '0' atau bit '1'. Ini menunjukkan sinyal teracak cukup baik. Namun, nilai ini tidak berlaku untuk masukan *key* dan *frame number* bernilai '0' pada semua bitnya karena nilai *ciphertext* adalah sama dengan data awalnya.
5. Hasil *synthesis* menunjukkan sistem dirancang menggunakan *entity* pada *top level* menggunakan *slices, slice flip flop,* dan 4 *input LUT's* sebanyak 1% dari jumlah *slices, slice flip flop,* dan 4 *input LUT's* yang tersedia pada *device*. Sedangkan penggunaan IOBs dan GCLKs masing-masing hanya menggunakan 5% dan 3% dari yang tersedia. Sehingga sistem yang dirancang dapat diimplementasikan pada *target device* yaitu FPGA Virtex-4 seri XC4VLX25.
6. Hasil implementasi pada 2 *device* mengalami kendala karena adalnya pengaruh *delay* yang terjadi pada saat komunikasi antar *device*. Sedangkan implementasi pada 1 *device* memberikan hasil yang sama dengan simulasi yang dilakukan.

5.2 Saran

Adapun saran yang dapat diberikan untuk pengembangan Tugas Akhir ini kedepannya antara lain:

1. Perlu diadakan kajian baik untuk mengetahui cara kerja atau memodifikasi sistem yang telah ada untuk menciptakan algoritma kriptografi baru.
2. Masukan yang diberikan bukan hanya di-*generate* dari FPGA, namun juga dilakukan percobaan untuk masukan yang berasal dari *device* lain.
3. Pelu dilakukan penelitian agar *resource* yang digunakan dalam implementasi lebih optimal.
4. Pada implementasi dengan dua *device*, diperlukan pengaturan sinkronisasi dan *handshaking* pada proses komunikasi kedua *device* agar sistem dapat bekerja dengan baik.

DAFTAR PUSTAKA

[1] Ashdeen, Peter J. (1990). *The VHDL Cookbook*, Adelaide: University of Adelaide

[2] Edwards, Stephen A. (1999). *The VHDL Hardware Description Language*. Columbia: Columbia University

[3] Ekdahl, Patrik, Thomas Johansson. (2002). *Another Attack on A5/1*. Submission to IEEE Transactions on Infromation Theory

[4] Erguler, Imran and Emin Anarem. (2004). *A Modified Stream Generator for The GSM Encryption Algorithm A5/1 and A5/2*. Istanbul: Department of Electronics and Communications Engineering, Dogus University. pp 1-2.

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

[6] Kurniawan, Yusuf. (2004). ”Kriptografi Keamanan Internet dan Jaringan Telekomunikasi”, Bandung : Informatika.

[7] Sumaryo, Sony. (2005).*Diktat Mata Kuliah Elektronika Digital*. Bandung : Sekolah Tinggi Teknologi Telkom, 2005.

[8] "A5/1." Wikipedia. 3 Mei 2007 <http://en.wikipedia.org/wiki/A5/1>.

[9] "Field-programmable gate array." Wikipedia. 10 Mei 2007 <http://en.wikipedia.org/wiki/FPGA>.

[10] "Linear Feedback Shift Register." Wikipedia. 10 Juni 2007 <http://en.wikipedia.org/wiki/LFSR>.