#### Prototipe Sistem Enkripsi Dan Dekripsi Berbasis FPGA Menggunakan Algoritma Stream Cipher Grain-128

**PROPOSAL TUGAS AKHIR**

**Kelompok Peminatan : Keamanan Sistem**

**Oleh**

**Afildo Kurnia Ilahi**

**1104130045**

****

**Program Studi Sarjana Sistem Komputer**

**Fakultas Teknik Elektro**

**Universitas Telkom**

**Bandung**

**2017**

# LEMBAR PERSETUJUAN

**PERANCANGAN DAN SIMULASI**

**PERLINDUNGAN PROPERTI INTELEKTUAL MENGGUNAKAN ALGORITME OBFUSCATION FILTER DIGITAL**

***Design and Simulation of Intelectual Properties Protection using Digital Filter Obfuscation Algorithm***

**Hanjara Cahya Adhyatma**

**1104130045**

Disusun dalam rangka memenuhi persyaratan dalam mengajukan Tugas Akhir pada Program Studi Sarjana Sistem Komputer

Fakultas Teknik Elektro

Universitas Telkom

Proposal ini disetujui untuk menyelesaikan Tugas Akhir

Bandung, September 2017

Calon Pembimbing 1 Calon Pembimbing 2

**Fairuz Azmi, S.T., M.T. Surya Michrandi Nasution, S.T., M.T.**

NIP : 13860021 NIP : 15890008

# ABSTRAK

Saat ini perkembangan teknologi mengalami kemajuan begitu pesat. Setiap perkembangan teknologi tersebut juga terdapat penyebaran informasi. Penyebaran informasi dapat dilakukan dengan sangat mudah dan sangat cepat. Tetapi, kerahasiaan informasi tersebut menjadi masalah yang cukup besar. Informasi tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab.

Sistem keamanan komputer menjadi sebuah hal yang sangat penting diperhatikan dalam masalah kerahasiaan informasi tersebut. Ilmu kriptografi sangat berguna dalam sistem keamanan komputer. Dari sekian banyak ilmu kriptografi, salah satunya adalah implementasi kriptografi pada level *prototipe* IC.

Pada penelitian ini dikembangkan prototipe sistem enkripsi dan dekripsi berbasis FPGA dengan menggunakan algoritma stream cipher Grain-128. *Input* yang digunakan pada penelitian ini berupa biner. Metode untuk membangun *stream cipher* yang digunakan adalah NFSR *(Non-Linear Feedback Shift Register)* dan LFSR *(Linear Feedback Shift Register)*. Menggunakan bahasa pemrograman Verilog *Hardware Description Language* (HDL) untuk mendeskripsikan fungsi rangkaian *digital.* Pengujian yang akan dilakukan pada penelitian ini adalah analisa proses enkripsi dan dekripsi, waktu proses enkripsi dan dekripsi, *avalanche effect*, *area*, dan *clock*

Kata Kunci : Prototipe, Kriptografi, Grain-128, FPGA

# KATA PENGANTAR

Dengan memanjatkan puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusuan Proposal Tugas Akhir ini. Proposal Tugas Akhir ini disusun untuk memenuhi syarat lulus mata kuliah Penulisan Karya Ilmiah dan Proposal.

Dalam kelancaran penyusunan Proposal Tugas Akhir ini penulis mendapatakan banyak bantuan, baik itu bantuan langsung maupun bantuan tidak langsung. Dengan segala kerendahan hati izinkanlah penulis menyampaikan terimakasih kepada semua pihak yang telah terlibat dalam penyelesaian Proposal ini. Dan semoga segala bentuk kebaikan yang diberikan oleh semua pihak kepada penulis senantiasa mendapat balasan yang berlipat ganda dari Allah SWT. Amin.

Demikian Proposal Tugas Akhir ini penulis susun, semoga bermanfaat bagi semua pihak yang membaca dan memerlukan Proposal Tugas Akhir ini. Akhir kata penulis mohon maaf karena Proposal Tugas Akhir ini masih terdapat kekurangan dan jauh dari kata sempurna. Oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan penyelesaian Tugas Akhir.

Bandung, September 2017

Penulis

# **DAFTAR ISI**

[LEMBAR PERSETUJUAN ii](#_Toc493061342)

[ABSTRAK iii](#_Toc493061343)

[KATA PENGANTAR iv](#_Toc493061344)

[DAFTAR ISI v](#_Toc493061345)

[DAFTAR GAMBAR vi](#_Toc493061346)

[DAFTAR TABEL vii](#_Toc493061347)

[BAB I PENDAHULUAN 1](#_Toc493061348)

[1.1. Latar Belakang 1](#_Toc493061349)

[1.2. Rumusan Masalah 2](#_Toc493061350)

[1.3. Tujuan 2](#_Toc493061351)

[1.4. Batasan Masalah 2](#_Toc493061352)

[1.5 Hipotesis 3](#_Toc493061353)

[BAB II PEKERJAAN SEBELUMNYA DAN KETERKAITAN (KAJIAN PUSTAKA) 4](#_Toc493061354)

[BAB III METODOLOGI PENELITIAN 6](#_Toc493061355)

[3.1 Studi Literatur 6](#_Toc493061356)

[3.2 Analisis 6](#_Toc493061357)

[3.3 Perancangan 6](#_Toc493061358)

[3.4 Implementasi 14](#_Toc493061359)

[3.5 Pengujian 14](#_Toc493061360)

[3.6 Keluaran yang diharapkan 15](#_Toc493061361)

[BAB IV JADWAL KEGIATAN 16](#_Toc493061362)

[DAFTAR PUSTAKA 17](#_Toc493061363)

DAFTAR GAMBAR

[Gambar 3. 1 Konsep *Stream Cipher*[9] 7](#_Toc493061302)

[Gambar 3. 2 Struktur *Stream Cipher* Grain-128[10] 7](#_Toc493061303)

[Gambar 3. 3 Proses Enkripsi Dekripsi 10](#_Toc493061304)

[Gambar 3. 4 Diagram Proses Perancangan 11](#_Toc493061305)

[Gambar 3. 5 Block Diagram 12](#_Toc493061306)

[Gambar 3. 6 Skematik Alur Data 12](#_Toc493061307)

[Gambar 3. 7 FPGA Altera Cyclone IV 13](#_Toc493061308)

[Gambar 3. 8 Arduino UNO 13](#_Toc493061309)

DAFTAR TABEL

[Table 4. 1 Jadwal Kegiatan 16](#_Toc464625031)

# BAB I PENDAHULUAN

## Latar Belakang

Dunia teknologi sekarang ini semakin berkembang. Pada teknologi khususnya prototipe IC mengalami perkembangan yang begitu pesat. Salah satu contoh perkembangan tersebut adalah sebuah prototipe IC yang bisa melakukan proses enkripsi dan dekripsi. Dimana pengertian enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli atau yang disebut *plain text* diubah menjadi kode-kode yang tidak dapat dimengerti atau biasa disebut *cipher text*. Sedangkan dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya[1].

Dalam hal ini, prototipe IC yang menunjang adalah berbasis FPGA. FPGA adalah singkatan dari *Field-Programmable Gate Array*. FPGA adalah komponen terpadu elektronika yang terbuat dari semikonduktor dan dirancang untuk dapat diprogram secara berulang-ulang oleh pengguna. FPGA diprogram dengan menggunakan bahasa *Hardware Description Language* (HDL). FPGA dapat melakukan proses logika dan matematika sesuai dengan *Verilog* yang ditanamkan[2].

Dalam penelitian dikembangkan prototipe sistem enkripsi dan dekripsi berbasis FPGA dengan menggunakan algortima stream cipher Grain-128. Kemudian nantinya akan dibandingkan performansi dari implentasi algoritma tersebut dengan algoritma berorientasi *hardware* lainnya sesuai dengan aspek pengujian.

## Rumusan Masalah

Rumusan masalah dalam penelitian yang berjudul Implementasi Algoritma *Stram Cipher* Grain-128 pada FPGA Altera Cyclone IV adalah seperti yang dijelaskan di bawah ini :

1. Kurangnya sistem keamanan dalam penyebaran informasi.
2. Banyaknya algoritma kriptografi berorientasi pada *hardware* yang bisa digunakan pada sistem keamanan.

## Tujuan

Pada penelitian yang berjudul Implementasi Algoritma *Stram Cipher* Grain-128 pada FPGA Altera Cyclone IV, bertujuan untuk:

1. Merancang prototipeIC dan diimplementasi algoritma *stream cipher* yang bisa melakukan proses kriptografi.
2. Merancang algoritma *stream cipher* Grain-128 dengan bahasa pemrograman Verilog dan diimplementasikan pada FPGA Altera Cyclone IV.

## Batasan Masalah

Batasan masalah pada penelitian berjudul Implementasi Algoritma *Stram Cipher* Grain-128 pada FPGA Altera Cyclone IV, sebagai berikut:

1. Algoritma kriptografi yang digunakan adalah algoritma *stream cipher* Grain-128.
2. Prototipe IC yang digunakan adalah FPGA Altera Cyclone IV.
3. Perancangan yang dilakukan adalah proses enkripsi dan dekripsi tanpa kompresi.
4. Desain penelitian ini dilakukan pada RTL dan gate level, tidak sampai layout level.
5. Pada simulasi dan implementasi, kunci yang digunakan adalah data biner sepanjang 128 bit.
6. Pada simulasi dan implementasi, inputan yang digunakan adalah data biner sepanjang 40 bit.

## Hipotesis

Tercipta sebuah prototipeIC yang dapat melakukan proses kriptografi (enkripsi dan dekripsi) menggunakan algoritma *stream cipher* Grain-128 dengan parameter keberhasilan waktu proses kriptografi yang cepat.

# BAB II PEKERJAAN SEBELUMNYA DAN KETERKAITAN (KAJIAN PUSTAKA)

Algoritma *stream cipher* Grain-128 merupakan *stream cipher* biner tambahan yang memiliki panjang kunci 128 bit dan panjang IV 96 bit. Grain-128 menggunakan LFSR *(Linear Feedback Shift Register)* untuk memastikan statistik yang baik dan untuk menjamin batas bawah untuk periode *keystream*. Untuk memperkenalkan *non-linear*, sebuah NFSR *(Non-linear Feedback Shift Register)* digunakan bersama dengan filter *non-linear*. Filter *non-linear* mengambil *input*  dari kedua *shift register*[3].

Algoritma *stream cipher* Grain-128 merupakan salah satu algoritma kriptografi yang kompatibel pada level prototipeIC. Sangat memberi ketika algoritma ini diimplementasikan pada level prototipeIC.

Pada penelitian ini akan dikembangkan prototipe sistem enkripsi dan dekripsi berbasis FPGA dengan menggunakan algoritma stream cipher Grain-128. FPGA setelah diimplementasi algoritma *stream cipher* Grain-128 akan dapat melakukan proses enkripsi dan dekripsi. FPGA akan dianalisa berdasarkan pengujian *area, clock, efficiency,* dan verifikasi IC (menggunakan *single stuck at fault*).

Peneltian ini merujuk pada kajian sebelumnya yaitu pada jurnal “FPGA Implementations of eSTREAM Phase-2 Focus Candidates with Hardware Profile” yang menganalisa perbandingan pada implementasi algoritma *stream cipher* pada FPGA. Algoritma *stream cipher* yang digunakan adalah Trivium, Grain-128, MICKEY-128 2.0, dan Phelix. Sedangkan FPGA yang digunakan adalah Xilinx Virtex-II XC2V6000-4ff1152. Hasil dari penilitian jurnal ini adalah menunjukkan bahwa Trivium dan Grain-128 memiliki kompleksitas terkecil untuk implementasi *hardware*. Pada jurnal ini juga melakukan pengujian pada *resource area* yang digunakan pada rangkain. Hasil dari pengujiannya adalah *area* yang digunakan pada penelitian ini sebanyak 48 *slices* pada implementasi algoritma Grain-128[4].

Selain itu ada jurnal “An Improved Hardware Implementation of the Grain Stream Cipher” yang menganalisa dan menunjukkan bagaiman untuk meningkatkan efisiensi *hardware*. Jurnal ini juga membandingkan Grain-80 dan Grain-128, yang mana salah satu yang asli sesuai dengan konfigurasi Fibonacci dan yang baru sesuai dengan konfigurasi Galois. Hasil yang didapat adalah peningkatan efisiensi *hardware* pada Grain-128 lebih tinggi dibanding Grain-80. Pada jurnal ini sama-sama menggunakan NFSR *(Non-linear Feedback Shift Register)* dengan penelitian ini[5].

Jurnal “Efficient FPGA Implementationts of High-Dimensional Cube Testers on the Stream Ciper Grain-128” juga sebagai bahan acuan peneltian ini, karena menganalisa implementasi algoritma *stream cipher* Grain-128 pada FPGA dan juga melibatkan perhitungan *clocking*.[6]

Kemudian ada jurnal “Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates” menjelaskan tentang perbandingan beberapa algoritma kriptografi yang diimplementasikan pada FPGA Xilinx. Hasil dari penelitian ini adalah Trivium dan Grain-128 yang paling efisien dalam hal *resources area* dan *maximum throughput per area*[7].

Jurnal “Grain and Trivium Ciphers Implementation Algorithm In FPGA Chip and AVR Micro Controller” juga memiliki keterkaitan dengan penelitian ini. Perbedaannya terletak pada FPGA yang digunakan. Pada jurnal ini menggunakan menggunakan FPGA *chip* dan AVG *micro controller.* Hasil yang bisa diambil dan dikaitkan dengan penelitian pada jurnal ini adalah pada pengujian *number of slice*[8].

# BAB III METODOLOGI PENELITIAN

## Studi Literatur

Studi literatur adalah metodolgi yang bertujuan untuk mendapatkan gambaran teori tentang penelitian yang telah dilakukan sebelumnya dan bagaimana pengerjaan penelitian tersebut, kemudian dibandingkan dengan penelitian yang akan kita lakukan. Hal tersebut dapat diperoleh melalui berbagai sumber, seperti internet dan juga jurnal atau paper yang berkaitan dengan algoritma kriptografi *stream cipher*.

## Analisis

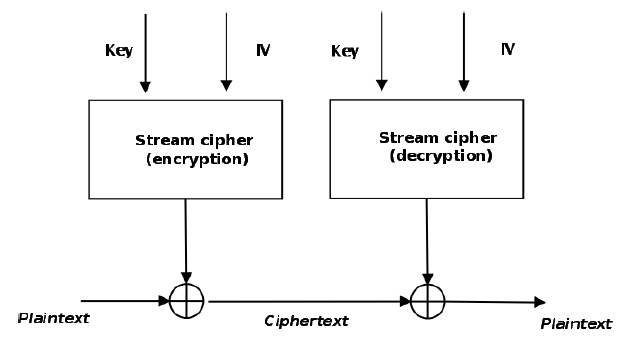
Analisis yang dilakukan dalam penelitian ini adalah menganalisa proses enkripsi dan enkripsi, waktu proses enkripsi dan dekripsi, *avalanche effect,* *area,* dan *clock* yang dihasilkan oleh algoritma *stream cipher* Grain-128 yang diimplementasikan pada FPGA.

## Perancangan

Setelah menganalisa batasan masalah, maka akan dilakukan implementasi algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV agar bisa melakukan proses kriptografi. Pemilihan Grain-128 sebagai algoritma kriptografi yang akan diimplementasikan karena Grain-128 merupakan algoritma kriptografi berbasis *stream cipher* yang dikembangkan oleh Martin Hell, Thomas Johansson, dan Willi Meier pada tahn 2004 yang menjadi salah satu kandidat eSTREAM project yang kompatibel pada *hardware*.

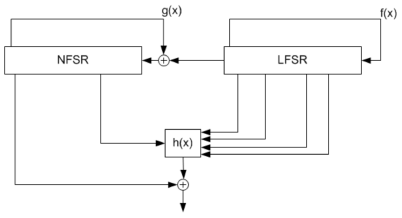
“Data yang tidak dan belum disandikan disebut *plain text*. Sedangkan data yang telah disandikan disebut *cipher text*. Proses mengubah *plain text* menjadi *cipher text* disebut enkripsi. Dan proses mengembalikan *cipher text* menjadi *plai ntext* lagi disebut dekripsi”. Pada proses kriptografi dipenelitian ini tidak melakukan proses kompresi.

“Algoritma kriptografi Grain-128 dirancang terutama untuk hardware yang terbatas. Grain-128 menerima 128-bit kunci dan 96-bit IV”.



Gambar 3. 1 Konsep *Stream Cipher*[9]

Grain adalah *synchoronous stream cipher* yang ditargetkan untuk lingkungan *hardware* diamana menghitung *gate*, daya konsumsi, dan keterbatasan memori. Hal ini mendukung ukuran kunci 128 bit dan IV ukuran 96 bit. Grain-128 adalah algoritma *stream cipher* yang memiliki ukuran kunci 128 bit.



Gambar 3. 2 Struktur *Stream Cipher* Grain-128[10]

Algoritma *stream cipher* Grain-128 menggunakan NFSR *(Non-Linear Feedback Shift Register)* dan LFSR *(Linear Feedback Shift Register)* sebagai pembangkit *keystream*. Pada LFSR *(Linear Feedback Shift Register)* merupakan jenis *feedback polynomial*, yang dinotasikan seabagai f(x).

f(x) = 1 + x32 + x47 + x58 + x90 + x121 + x128

Pembaharuan fungsi LFSR *(Linear Feedback Shift Register)* untuk menghilangkan ambiguitas dilakukan sebagai berikut:

si+128 = si + si+7 + si+38 + si+70 + si+81 + si+96

Pada NFSR *(Non-Linear Feedback Shift Register)* juga merupakan jenis *feedback polynomial*, yang dinotasikan sebagai g(x).

g(x) = 1 + x32 + x37 + x72 + x102 + x128 + x44x60+x61x125 + x63x67 +   
 x69x101+x80x88 + x110x111 + x115x117

Kembali dilihat pembaharuan fungsi NFSR *(Non-Linear Feedback Shift Register)* untuk menghilangkan ambiguitas yang dilakukan sebagai berikut:

bi+128 = si + bi + bi+26 + bi+56 + bi+91 + bi+96+bi+3bi+67 + bi+11bi+13 +   
 bi+17bi+18+bi+27bi+59 + bi+40bi+48 + bi+61bi+65+bi+68bi+84.

Dua inputan diatas, yaitu NFSR *(Non-Linear Feedback Shift Register)* dan LFSR *(Linear Feedback Shift Register)* merupakan fungsi Boolean, yang dinotasikan sebagai h(x).

h(x) = x0x1 + x2x3 + x4x5 + x6x7 + x0x4x8

Keluaran dari fungsi diatas adalah,

Dimana A = {2, 15, 36, 45, 64, 73, 89}[3].

Contoh soal hitungan manual algoritma *stream cipher*:

Diketahui *input plain text* 8 bit, yaitu 01101100. Tentukan *cipher text* dengan melakukan proses enkripsi. Kemudian lakukan proses dekripsi terhadap *cipher text* tersebut. Dengan nilai *key* adalah 01010011.

Jawab:

Proses enkripsi;

*Plain text* : 01101100

*Key* : 01010011

*Cipher text* = *plain text* XOR *Key*

01101100 XOR 01010011

00111111

Proses dekripsi;

*Plain text* = *Key* XOR *Cipher text*

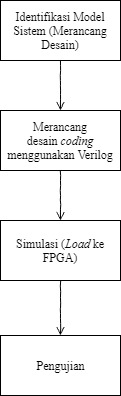
01010011 XOR 00111111

01101100

C:\Users\ASUS\Downloads\proses enkrip dekrip.png

Gambar 3. 3 Proses Enkripsi Dekripsi

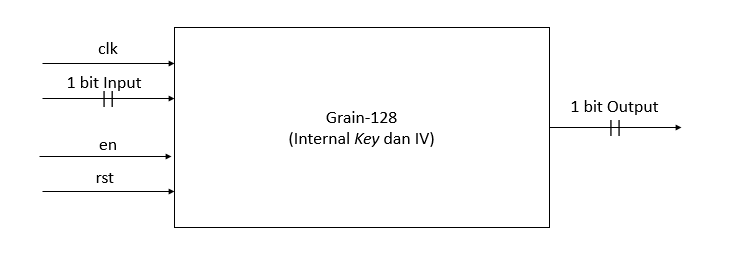
Diagram bentuk proses enkripsi dan dekripsi menggunakan algoritma *stream cipher* Grain-128. Pada penelitian ini dapat dilakukan proses enkripsi dan dekripsi sekaligus. Maksudnya adalah prototipeIC yang digunakan pada penelitian ini dapat melakukan proses enkripsi sehingga didapatkan *cipher text*. Setelah itu prototipeIC juga bisa mengembalikan *cipher text* menjadi *plain text* lagi dengan melakukan proses dekripsi.



Gambar 3. 4 Diagram Proses Perancangan

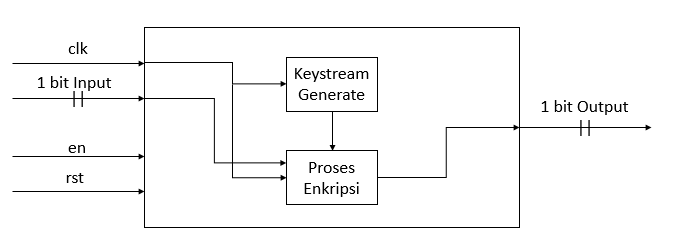
Gambar diatas menjelaskan proses perancangan pada penelitian ini. Hal yang dilakukan adalah melakukan identifikasi pada model sistem yang akan diteliti, dalam hal ini dilakukan desain perancangan sistem. Setelah itu melakukan perancangan desain *coding* menggunakan bahasa pemrograman Verilog *Hardware Description Language* (HDL). Kemudian melakukan simulasi dengan FPGA yang digunakan. Terakhir melakukan pengujian hasil penelitian.

Pada pengujian akan dilakukan analisis perbandingan dua algoritma *stream cipher* yang diimplementasikan pada FPGA Altera Cyclone IV. Analisis yang dilakukan adalah membandingkan poin-poin pengujian dari masing-masing algoritma *stream cipher* yang mana yang lebih baik diimplementasikan pada FPGA Altera Cyclone IV.



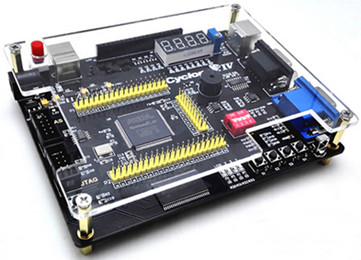
Gambar 3. 5 Block Diagram

Gambar diatas merupakan *block diagram* dari rancangan penelitian ini. Pada *block diagram* diatas terdapat clk yang berfungsi sebagai clock. Kemudian ada data inputan 1 bit yang akan diproses untuk melakukan proses enkripsi dan dekripsi. Lalu ada en sebagai *controller* jika ingin mengaktifkan clock. Kemudian ada rst sebagai fungsi untuk melakukan reset pada sistem. Hasil proses enkripsi akan dikeluarkan melalui *output* 1 bit. Selain itu juga terdapat internal *key* dan IV yang aka dideklarasikan didalam FPGA. Untuk *input* berasal dari external, dimana pada penelitian ini menggunakan Arduino UNO.



Gambar 3. 6 Skematik Alur Data

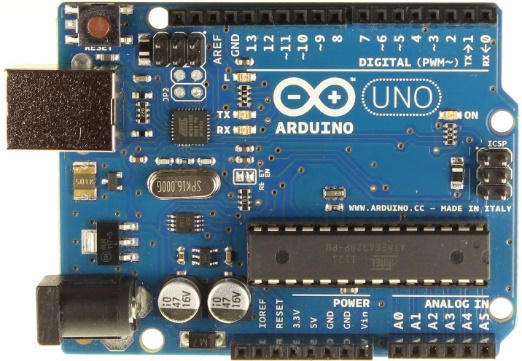
Gambar diatas merupakan diagram skematik alur data. Dimana pada FPGA dilakukan proses *generate keystream* dengan memanfaatkan internal *key* dan IV. Dan juga terdapat proses enkripsi/dekripsi yang diproses dengan *inputan* dan hasil *generate keystream* dan nantinya akan menghasilkan *output*.



Gambar 3. 7 FPGA Altera Cyclone IV

Sumber : https:// http://www.ecyberspaces.com/UploadFile/2016291658568110.jpg

Keluarga baru Cyclone ini (Cyclone IV) merupakan perpanjangan kepemimpinan seri FPGA Cyclone yang memberikan biaya pasar terendah dan kekuatan terendah dari FPGA, sekarang dengan *transceiver variant*. Perangkat Cyclone IV ditargetkan untuk volume tinggi, aplikasi biaya sensitif, memungkinkan perancang sistem untuk memenuhi peningkatan kebutuhan *bandwith* sambil menurunkan biaya.



Gambar 3. 8 Arduino UNO

Sumber : meccanismocomplesso.org

Arduino UNO merupakan board mikrokontroler yang menggunakan ATmega328. Terdiri dari 14 pin digital input/output, 6 input analog, 16 MHz crystal oscillator, USB connection, power jack, header ICSP, dan tombol reset. Arduino UNO dapat diberi daya melalui koneksi USB maupun eksternal power supply yang berasal dari AC-to-DC adapter atau baterai. ATmega328 terdiri dari 32 KB flash memory untuk menyimpan *code* dengan 0,5 KB telah digunakan untuk bootloader, 2 KB SRAM (Static Random Access Memory) dan 1 KB EEPROM (Electrically Erasable Programmable Read-Only Memory).

## Implementasi

Pada tahap implementasi, algoritma *stream cipher* Grain-128 akan langsung diimplementasikan pada FPGA Altera Cyclone IV. Sehingga FPGA tersebut bisa melakukan proses enkripsi dan dekripsi sekaligus. Kemudian akan dianalisa algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV.

## Pengujian

Pada tahap pengujian akan dilakukan serangkaian pengujian hasil implementasi dari algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV. Parameter yang diuji diantaranya :

1. Enkripsi dan dekripsi pada sistem

Pada pengujian ini dilakukan uji kecocokan data antara input dan output pada aplikasi.

1. Waktu proses enkripsi dan dekripsi

Lama proses enkripsi dan dekripsi diukur untuk mendapatkan hasil kecepatan proses enkripsi dan dekripsi Algoritma *Stream Cipher* Grain-128.

1. *Avalanche Effect*

*Avalanche Effect* merupakan perubahan kecil baik pada kunci atau *plain text* yang dapat menyebabkan perubahan yang signifikan terhadap *cipher text*. Dalam kriptografi, nilai avalanche effect suatu algoritma akan dikatakan baik jika perubahan satu bit pada input menghasilkan output setengah bit[13].



1. *Area*

*Area* yang diuji disini adalah *resource* yang digunakan oleh rangkaian selama proses kriptografi. Satuan dari *area* yang digunakan adalah *slice(s).*

1. *Clock*

Pengujian *clock* disini adalah jumlah *clock* yang digunakan pada saat proses kriptografi.

## Keluaran yang diharapkan

Keluaran yang diharapkan antara lain:

1. Sebuah *prototipe* ICyang dapat melakukan proses enkripsi dan dekripsi (proses kriptografi).
2. Hasil dari perancangan dan implementasi beserta pengujian akan di dokumentasikan dalam bentuk buku Tugas Akhir.

# BAB IV JADWAL KEGIATAN

Agar proses pembuatan Tugas Akhir ini berjalan dengan baik dan sesuai dengan target yang telah ditentukan, maka diperlukan perencanaan jadwal kegiatan pembuatan Tugas Akhir. Adapun jadwal yang telah direncanakan adalah sebagai berikut:

Table 4. 1 Jadwal Kegiatan

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No | Rencana Kegiatan | Minggu ke- | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 | Penyusunan Proposal TA |  |  |  |  |  |  |  |  |  |  |
| 2 | Seminar Proposal  TA |  |  |  |  |  |  |  |  |  |  |
| 3 | Studi Literatur |  |  |  |  |  |  |  |  |  |  |
| 4 | Perancangan |  |  |  |  |  |  |  |  |  |  |
| 5 | Implementasi |  |  |  |  |  |  |  |  |  |  |
| 6 | Uji Performansi dan Analisa |  |  |  |  |  |  |  |  |  |  |
| 7 | Penyusunan  Buku TA |  |  |  |  |  |  |  |  |  |  |
| 8 | Sidang TA |  |  |  |  |  |  |  |  |  |  |

# DAFTAR PUSTAKA

[1] *Ariyus, Doni.* 2008. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.

[2] *Dwi Herlambang; Dicki Hugo Joputro; Rudy Susanto.* 2012.Modul Training Praktikum Menggunakan FPGA.

[3] *Martin Hell; Thomas Johansson; Alexander Maximov*. 2006. A Stream Cipher Proposal: Grain-128.

[4] *Philippe Bulens; Kassem Kalach; Francois-Xavier Standaer;, Jean-Jacques Quisquater.* 2007. FPGA Implementations of eSTREAM Phase-2 Focus Candidates with Hardware Profile.

[5] *Shohreh Sharif Mansouri; Elene Dubrova.* 2010. An Improved Hardware Implementation of the Grain Stream Cipher.

[6] *Jean-Philippe Aumasson; Itai Dinur; Luca Henzen; Willi Meier; Adi Shamir.* 2009. Efficient FPGA Implementations of High-Dimensional Cube Testers on Stream Cipher Grain-128.

[7] *David Hwang; Mark Chaney; Shashi Karanam; Nick Ton; Kris Gaj.* 2008. Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates.

[8] *Ahad Jafarpour; Abdollah Mahdlo; Amir Akbari; Kaveh Kianfar.* 2011.Grain dan Trivium Ciphers Implementation Algorithm In FPGA Chip and AVR Micro Controller.

[9] *Hongxu Zhao; Shqi Li.* 2009. Power Analysis Attacks on a Hardware Implementation of the Stream Cipher MICKEY.

[10] *Herlambang, Stephen.* 2010. Studi dan Analisis Grain Cipher.

[11] *Shao Ke, Li Hai-Feng, Mao Jing-Kun, Wang Zhuan-Bin.* 2012. Design and FPGA Implementation of RFID Tag Encryption Algorithm.

[12] *J. M. Marmolejo-Tejada; V. Trujillo-Olaya; J. Velasco-Medina.* 2010. Hardware Implementation of Grain-128, Mickey-128, Decim-128 and Trivium.

[13] *Feistel, Horst*. 1973. Cryptography and Computer Privacy.

[14] *Syahral, Mohamad*. 2011. Perancangan dan Implementasi Algoritma Enkripsi Arcfour pada Perangkat Kriptografi Berbasis FPGA.

[15] *Surya Lasmara; M. Ary Murti; Iwan Itut Tirtoasmoro*. 2007. Perancangan dan Implementasi Kriptografi Algoritma A5/2 Berbasis FPGA (Field Programmable Gate Arrays).

[16] *Muhtadin; Hermann Meuth*. 2009. Hardware Implementation of Stream Ciphers : Grain-128 and F-FCSR-H.

[17] *Mohammad Jumeidi; Dedi Triyanto; Yulrio Brianorman*. 2016. Implementasi Algoritma Kriptografi Vernam Cipher Berbasis FPGA.