# MODEL PROYEKSI ($X/Z^2$, $Y/Z^2$) PADA KURVA HESIAN SECARA PARALEL MENGGUNAKAN MEKANISME KRIPTOGRAFI KURVA ELIPTIK

**Winsy Weku**[1)]

[1)]**Program Studi Matematika FMIPA Universitas Sam Ratulangi**
**Jl. Kampus Unsrat Manado, 95115**
**e-mail: wincy24@yahoo.com**

## ABSTRAK

Suatu kunci publik, *Elliptic Curve Cryptography (ECC)* dikenal sebagai algoritma yang paling aman yang digunakan untuk memproteksi informasi sepanjang melakukan transmisi. ECC dalam komputasi aritemetika didapatkan berdasarkan operasi inversi modular. Inversi modular adalah operasi aritmetika dan operasi yang sangat panjang yang didapatkan berdasar *ECC crypto-processor*. Penggunaan koordinat proyeksi untuk menentukan Kurva Eliptik/ *Elliptic Curves* pada kenyataannya untuk memastikan koordinat proyeksi yang sebelumnya telah ditentukan oleh kurva eliptik $E: y^2 = x^3 + ax + b$ yang didefinisikan melalui *Galois field GF(p)*untuk melakukan operasi aritemtika dimana dapat diketemukan bahwa terdapat beberapa multiplikasi yang dapat diimplementasikan secara paralel untuk mendapatkan performa yang tinggi. Pada penelitian ini, akan dibahas tentang sistem koordinat proyeksi Hessian ($X/Z^2$, $Y,Z^2$) untuk meningkatkan operasi penggandaan ECC dengan menggunakan pengali paralel untuk mendapatkan paralel yang maksimum untuk mendapatkan hasil maksimal.

**Kata kunci:** Elliptic Curve Cryptography, Public-Key Cryptosystem, Galois Fields of Primes GF(p

# PROJECTION MODEL ($X/Z^2$, $Y/Z^2$) ON PARALLEL HESIAN CURVE USING CRYPTOGRAPHY ELIPTIC CURVE MECHANISM

## ABSTRACT

As a public key cryptography, Elliptic Curve Cryptography (ECC) is well known to be the most secure algorithms that can be used to protect information during the transmission. ECC in its arithmetic computations suffers from modular inversion operation. Modular Inversion is a main arithmetic and very long-time operation that performed by the ECC crypto-processor. The use of projective coordinates to define the Elliptic Curves (EC) instead of affine coordinates replaced the inversion operations by several multiplication operations. Many types of projective coordinates have been proposed for the elliptic curve E: $y^2 = x^3 + ax + b$ which is defined over a Galois field GF(p) to do EC arithmetic operations where it was found that these several multiplications can be implemented in some parallel fashion to obtain higher performance. In this work, we will study Hessian projective coordinates systems ($X/Z^2$, $Y,Z^2$) over GF (p) to perform ECC doubling operation by using parallel multipliers to obtain maximum parallelism to achieve maximum gain.

**Keywords:** Elliptic Curve Cryptography , Public-Key Cryptosystem , Galois Fields of Primes GF(p)

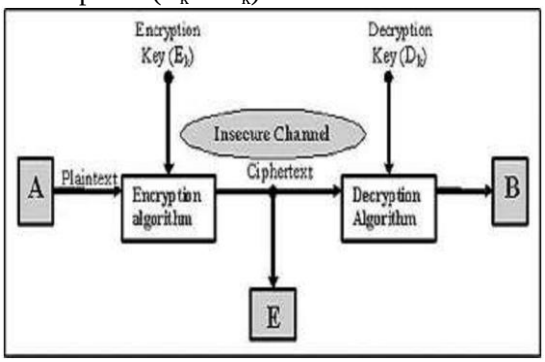
## PENDAHULUAN

Informasi merupakan masalah yang paling penting disaat ini. Informasi yang update dan tersedia setiap saat sangat penting untuk terjadinya proses transaksi dan komunikasi manusia. Keamanan informasi merupakan yang sangat dilindungi oleh perusahaan dan mengamankan sistem, media dan fasilitas yang memproses dan menjaga informasi vital terhadap operasinya.

Ilmu untuk melindungi informasi dari operasi yang tidak diinginkan disebut Kriptografi. Ilmu ini mempelajari proses

ilegal sepanjang terjadi transmisi. Skenario komunikasi mendasar untuk suatu sistem kriptografi berdasarkan pada dua bagian utama, yaitu: ***satu***, mentransformasikan pesan orisinil yang menyangkut informasi *(plaintext)* kedalam *enchiper* dan *chipertext* menggunakan suatu algoritma dan suatu kunci pada prosesnya, yang disebut enkripsi; ***kedua***, mentransformasikan *chipertext* kedalam *Plaintext*, yang disebut dengan dekripsi.

Menurut kunci enkripsi/deksripsi, kriptosistem dibagi menjadi dua bagian, yaitu kunci simetris dan kunci asimetris. Pada algoritma kunci simetris, kunci enkripsi dan dekripsi adalah sama dan diketahui oleh kedua pihak ($E_k = D_k$).




Gambar 1. Skenario komunikasi dasar untuk sistem kriptografi

Pada algoritma *Public Key Cryptography* (PKC) yang menggunakan dua kunci berbeda (Ek≠Dk), kunci enkripsi (Ek) dipublikasikan dan kunci dekripsi (Dk) dijaga tetap rahasia tetapi dalam perhitungannya tetap terbuka untuk mendapatkan kunci dekripsi (Dk) tanpa informasi diketahui hanya oleh para penggagas (mereka yang akan menerima pesan dari sesamanya). Operasi inilah yang membuat metode PKC menjadi sangat kuat dan fleksibel untuk digunakan. Pada sisi lainnya, PKC membutuhkan kemampuan komputasi yang cukup tinggi dibandingkan dengan komputasi yang dibutuhkan oleh algoritma kunci simetris yang berakibat juga pada performa kriptosistem.

Kurva elliptik pada ruang terbatas digunakan sebagai konjungsi dengan skema kriptografi seperti skema Diffie-Hellman, skema ElGamal dan skema RSA. Sejak diketemukannya, ECC telah digunakan secara luas diantara pengguna kriptografi untuk keamanan relatif yang lebih baik dan lebih mudah untuk diimplementasikan. Ukuran dari kurva eliptik menentukan tingkat kesulitan dari masalah yang ada. Telah diyakini bahwa tingkat keamanan dengan sistem berbasis RSA dengan modulus yang besar dapat dicapai dengan grup kurva eliptik yang lebih kecil. Dengan menggunakan kelompok yang kecil mengurangi penyimpanan dan kebutuhan transmisi. Diketahui bahwa pada tingkat keamanan 80 bit, ukuran kunci 1024 untuk RSA maka pada ECC hanya pada 160 bit. Berdasarkan faktor inilah, komputasi pada kurva eliptik telah menjadi daerah amatan yang menarik selama beberap tahun ini.

Pada jurnal ini akan dibahas tentang desain dan implementasi dari suatu algoritma untuk komputasi ECC seperti komputasi inverse di GF(p) berdasar pada efisiensi proyeksi sistem koordinat. Selanjutnya akan dibahas pula penggunaan koordinat proyeksi Hessian untuk menghitung operasi ECC dan mengekspolitasi banyaknya paralel maksimal untuk didapatkan beserta pengalinya. Sistem koordinat proyeksi Hessian yang digunakan pada GF (p) adalah proyeksi ($X/Z^2$, $Y/Z^2$).

## TINJAUAN PUSTAKA

### Kriptografi Kunci Publik *(Public Key Cryptography)*

Sebuah kemajuan besar dalam kriptografi terjadi dengan penemuan kriptografi kunci publik. Fitur utama dari kriptografi kunci publik adalah bahwa ia menghilangkan bentuk penggunaan tombol yang sama untuk enkripsi dan dekripsi. Dengan kriptografi kunci publik, kunci masuk di pasang kesesuaian "publik" dan "pribadi" tombol. Bagian publik dari pasangan kunci dapat didistribusikan secara umum tanpa mengorbankan bagian utama, yang harus dirahasiakan oleh pemiliknya. Suatu operasi (misalnya, enkripsi) dilakukan dengan kunci publik hanya dapat dibatalkan dengan kunci privatnya. Sebelum penemuan kriptografi kunci publik, pada dasarnya tidak mungkin untuk menyediakan pengaturan kunci untuk jaringan skala besar. Dengan kriptografi simetrik, karena jumlah pengguna meningkat pada jaringan, jumlah kunci yang

dibutuhkan untuk menyediakan komunikasi yang aman di antara para pengguna meningkat pesat. Sebagai contoh, sebuah jaringan 100 pengguna akan membutuhkan hampir 5000 kunci jika digunakan hanya kriptografi simetris. Penggandaan seperti jaringan untuk 200 pengguna meningkatkan jumlah kunci ke hampir 20.000. Jadi, ketika hanya menggunakan kriptografi simetrik, pengaturan yang cepat menjadi sangat berat bahkan untuk jaringan skala dalam kecil.

Penemuan kriptografi kunci publik adalah kepentingan pusat untuk bidang kriptografi dan memberikan jawaban atas banyak masalah manajemen kunci untuk jaringan skala besar. Untuk semua manfaatnya, namun, kriptografi kunci publik tidak memberikan solusi yang komprehensif untuk masalah manajemen kunci. Memang, kemungkinan melahirkan dengan kriptografi kunci publik meningkatkan kebutuhan canggih sistem manajemen kunci untuk menjawab pertanyaan seperti berikut: "Bagaimana saya bisa dengan mudah mengenkripsi file sekali untuk sejumlah orang yang berbeda dengan menggunakan kriptografi kunci publik? "Jika saya kehilangan kunci saya, bagaimana saya bisa mendekripsi semua file saya yang dienkripsi dengan kunci-kunci?" Bagaimana saya tahu bahwa saya benar-benar memiliki kunci publik Alice dan bukan kunci publik seseorang berpura-pura menjadi Alice "Bagaimana saya tahu bahwa kunci publik masih dapat dipercaya?"

## Kurva Elliptik

Kurva elliptik telah dipelajari selama beberapa tahun dan telah terdapat sejumlah besar topik literatur. Tahun 1985, Neal Koblitz dan V. S. Miller, masing-masing mengajukan kriptosistem publik-key. Mereka tidak menemukan suatu algoritma kriptografi yang baru menggunakan kurva eliptik pada bidang terbatas, tetapi mereka mengimplementasikan keberadaan algoritma publik-key, seperti Diffie-Hellma menggunakan kurva elliptik. Kurva elliptik sangat menarik karena menyediakan suatu teknik dalam membangun ‘elemen-elemen’ dan ‘aturan penggabungan’ yang menghasilkan banyak grup. Grup ini memiliki syarat cukuo yang sesuai untuk membangun algoritma kryptografi, tetapi tidak memiliki sifat tertentu yang dapat menghasilkan kryptanalisis. Sebagai contoh, tidak ada kata *‘smooth’* didalam kurva elliptik. Ini berarti, tidak ada kumpulan elemen kecil dengan elemen acak yang memiliki kesempatan untuk diekspresikan menggunakan algoritma yang sederhana. Akibatnya indeks algoritma logaritma diskret kalkulus tidak bekerja.

Kurva elliptik pada bidang terbatas $GF(2^n)$ merupakan bidang yang sangat menarik. Prosesor aritmetika pada bidang cakupan itu merupakan wilayah sederhana untuk dibangun dan relatif sederhana untuk diimplementasikan untuk n didalam jangkauan 130 sampai 200. Mereka memiliki potensi untuk menyediakan kriptosistem publik-key yang lebih cepat dengan ukuran kunci yang lebih kecil. Berbagai algoritma publik-key seperti Diffie-Hellman, ElGamal, dan Schnorr, dapat diimplementasikan dalam kurva elliptik pada bidang terbatas.

## *ECC (Elliptic Curve Cryptography) Cryptosystem*

ECC merupakan kriptosistem kunci publik yang berdasarkan pada aritmetika logaritma diskret yang melibatkan titik-titik pada kurva. Kurva aritmetika dinyatakan sebagai yang membawahi *field* terbatas yang disebut sebagai kumpulan elemen yang memiliki derajat terbatas (banyaknya elemen). *Field* terbatas yang sering digunakan pada ECC adalah Galois Fields (GF) yang menyatakan bilangan prima modulo GF(p) atau suatu field berektensikan bilangan biner $GF(2^n)$.

ECC menawarkan keamanan yang sama seperti yang disediakan oleh kriptosistem klasik seperti RSA dan Logaritma Diskrit dengan secara substansi kunci berukuran lebih kecil. Gambar 2 menunjukkan perbandingan ukuran kunci yang menyediakan tingkat keamanan yang sama untuk RSA, DL dan sistem EC pada skema enkripsi kunci simetris 80, 112, 128, 192 dan 256 bit. Kelima tingkat keamanan yang spesifik dipilih karena mereka merwakili jumlah komputasi yang dibutujkan untuk menghasilkan suatu pencarian kunci secara menyeluruh pada skema enkripsi kunci

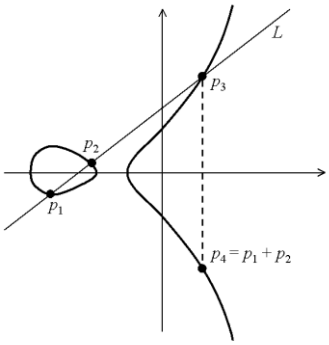
simetris SKIPJACK, Triple DES, AES Small, AES Medium dan AES Large.

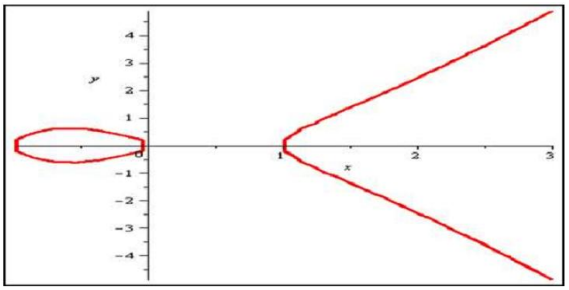
Sebagai contoh, kunci ECC 160 bit menyediakan tingkat keamanan yang sama sebagaimana 1024 bit untuk kunci RSA dan 224 bit ECC sama dengan 2048 bit RSA. Kunci yang semakin kecil akan menghasilkan komputasi yang semakin cepat, konsumsi power yang lebih rendah dan juga dapat menekan penggunaan memory dan *bandwidth*.

Asumsikan p adalah bilangan prima, dan misalkan GF (p) menyatakan ruang terbatas dari bilangan bulat modulo p. Titik pada tak berhingga, dinyatakan dengan ∞, juga dikatakan berada pada kurva. Kumpulan dari semua titik pada E dinyatakan oleh E pada GF(p). Gambar 3 menunjukkan suatu contoh kurva elliptik E: $y^2 = x^3 + ax + b$ dan E:$y^2$=x(x+1)(x-1) yang berada diatas bilangan riil (R).

Tabel 1. Ukuran kunci RSA, DL dan EC pada tingkat keamanan yang sama. Panjang bit untuk parameter DL adalah q dan EC adalah n, kemudian modulus RSA adalah n dan modulus DL adalah p.

| | Tingkat Keamanan (bit) | | | | |
|---|---|---|---|---|---|
| | 80 (SKIPJACK) | 112 (Triple-DES) | 128 (AES-Small) | 192 (AES-Medium) | 256 (AES-Large) |
| DL parameter q<br>EC parameter n | 160 | 224 | 256 | 384 | 512 |
| RSA modulus n<br>DL modulus p | 1024 | 2048 | 3072 | 8192 | 15360 |



Gambar 2. Kurva Eliptik E: y2 = x(x+1)(x-1) pada R

Mekanisme kriptografi berdasar pada kurva eliptik yang bergantung pada aritmetika yang melibatkan titik-titik pada kurva, dimana pesan orsinil dikonversikan ke titik-titik yang berada pada koordinat affine, sehingga operasi dasar aritmetik dibelakang ECC adalah jumlahan titik, penggandaan titik dan perkalian titik (perkalian skalar). Hal terutama dari operasi ini adalah berbasiskan pada multiplikasi modular yang melibatkan pengurangan dengan modulus pada komputasinya. Pembagian modular, bagaimanapun juga merupakan operasi yang sangat mahal.

Kebanyakan algoritma diperkenalkan untuk menurunkan biaya dari operasi invers atau menghilangkannya secara keseluruhan. Beberapa dari algoritma ini mencoba untuk meningkatkan performa dengan mengoptimalkan algoritma yang didesain untuk bekerja pada koordinat affine dan penyelesaian lainnya dibangun menggunakan koordinat proyeksi.

## PEMBAHASAN

### Sistem Persamaan

Komputasi dari operasi penggandaan titik pada koordinat normal adalah (x3, y3);

dan memberikan proyeksi titiknya adalah (X3, Y3, Z3), sehingga kita dapat menggunakan proyeksi yang sama untuk mendapatkan kembali (x3, y3). Perhitungan yang ada menggunakan asumsi X1=X2=X, Y1=Y2=Y.

Misalkan E merupakan sebuah kurva eliptik padar GF (p) yang menggunakan kurva Hessian untuk mewakili ECC sehingga E dapat didefinisikan dengan persamaan:

$E : x^3 + y^3 + 1 = dxy$ (1)

Untuk menurunkan persamaan operasi penggandaan titik, maka kita perlu menentukan slope (m) dimana $m = \frac{dy}{dx}$, sebagai berikut:

$$3x^2 + 3y^2\frac{dy}{dx} = dx\frac{dy}{dx} + dy$$

$$m = \frac{dy}{dx} = \frac{dy-3x^2}{3y^2-dx} \quad (2)$$

Persamaan ini akan digunakan pada perhitungan koordinat affine pada kasus proyeksi koordinat dari kurva tersebut.

## Persamaan Koordinat Affine

Untuk selanjutnya, dipertimbangkan bentuk normal dari kurva Hessian tanpa proyeksi untuk menghasilkan nilai dari penggandaan nilai yang diberikan oleh $P_3=(x_3,y_3)$. Dengan menggunakan persamaan slope (m) yang dihitung sebelumnya (2) maka akan didapatkan:

$$m = \frac{dy}{dx} = \frac{dy-3x^2}{3y^2-dx} \text{ atau } m = \frac{A}{B}$$

Dimana $A = dy - 3x^2 \quad B = 3y^2 - dx$

$x_3 = m^2 - 2x$ atau $x_3 = \left(\frac{A}{B}\right)^2 - 2x$

$y_3 = m(x_1-x_3) - y$

$$y_3 = \left[\frac{A}{B}\right]\left[x - \frac{A^2}{B^2} + 2x\right] - y$$

kemudian dengan menyederhanakan persamaan ini didapatkan hasil untuk $x_3$ dan $y_3$

$$x_3 = \frac{A^2 - 2xB^2}{B^2}$$

$$y_3 = \frac{A[3xB^2 - A^2] - yB^3}{B^3}$$

Dapat dijelaskan disini bahwa penggandaan titik menggunakan kurva Hessian pada koordinatnya memerlukan 8 multiplikasi, 5 penjumlahan dan 2 operasi invers modular. Invers modular (hanya muncul pada kasus koordinat affine) yang dikenal dengan operasi yang sangat panjang, membutuhkan waktu sama dengan sekita 3-4 waktu multiplikasi berurutan, hal ini dapat dihindari kalau diterapkan koordinat proyeksi untuk menggantikan operasi penggandaan titik.

## Proyeksi ($X/Z^2$, $Y/Z^2$)

Dalam proyeksi ini akan digunakan substitusi (x,y) menjadi ($X/Z^2$, $Y/Z^2$), sehingga akan berbentuk dari m ke M.

$$M = \frac{\frac{dY}{Z^2} - 3\frac{X^2}{Z}}{3\frac{Y^2}{Z^4} - \frac{dX}{Z^2}} = \frac{dY - 3Z^2X}{Z^2[3Y - dX]}$$

dimana $A = dY - 3Z^2X$

$B = 3Y - dX$

sehingga $M = \frac{A}{Z^2B}$

dengan mensubstitusikan semua nila x, y dan m, maka akan didapatkan bentuk:

$$X_3' = M^2 - 2x = \frac{A^2}{Z^4B^2} - \frac{2X}{Z^2} = \frac{A^2 - 2XZ^2B^2}{Z^4B^2}$$

$$Y_3' = M(y - y_3) - y = \frac{A}{Z^2B}\left(\frac{X}{Z^2} - \frac{A^2 - 2XZ^2B^2}{Z^4B^2}\right) - \frac{Y}{Z^2}$$

$$= \frac{A(3XZ^2B^2 - A^2) - YZ^6B^5}{Z^2B^4}$$

$$X_3 = A^2 - 2XZ^2B^2$$

$$Y_3 = AZ^2B(3XZ^2B^2 - A^2) - YZ^6B^5$$

$$Z_3 = Z^2B$$

$$\alpha_1 = X^2 \quad \alpha_2 = Y^2 \quad \alpha_3 = Z^2 \quad \alpha_4 = B^2$$

$$A = \alpha_3 dY - 3\alpha_1$$

$$B = 3\alpha_2 - \alpha_3 dX$$

$$\alpha_5 = \alpha_3\alpha_4 \quad \alpha_6 = X\alpha_5 \quad \alpha_7 = A^2$$

$$\alpha_8 = \alpha_7\alpha_3 \quad \alpha_9 = X\alpha_4 \quad \alpha_{10} = \alpha_5 Y$$

$$\alpha_{11} = AC_1 \quad Y_3 = \alpha_{11} \quad \alpha_{12} = B\alpha_4$$

$$\alpha_{13} = \alpha_{12}\alpha_3 \quad Z_3 = \alpha_{13}$$

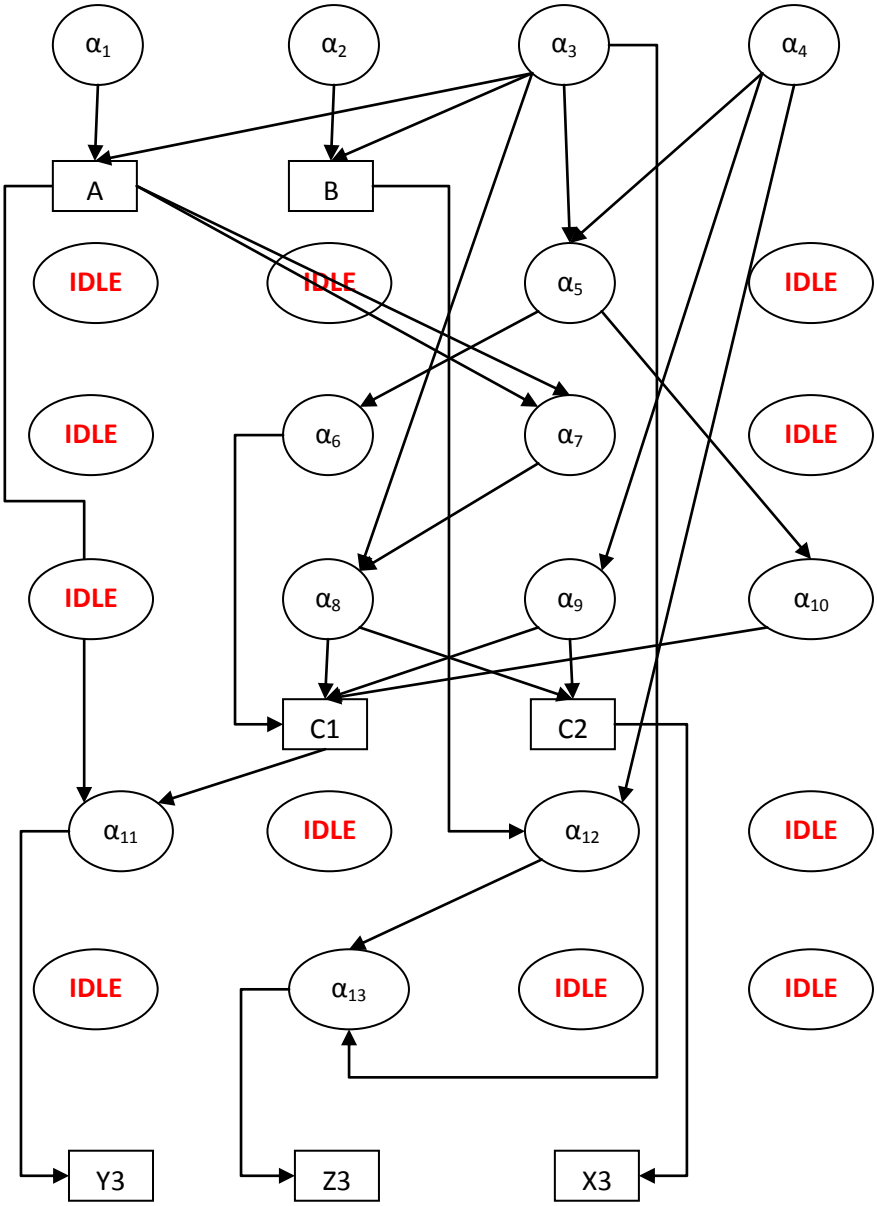
## Pemodelan dan Analisis

Pemodelan sistem dari penelitian ini adalah suatu framework interaktif yang mengekspresikan arsitektur hardware dari suatu *ECC Crypto-Processor* melalui 1 proyeksi ($X/Z^2$, $Y/Z^2$), yang termasuk didalamnya berbagai komponen hardware seperti *multipliers/adders/registers* dan interkoneksi internal dan eksternal dari suatu *ECC Crypto-Processor*.

Pada model sistem ini didapatkan suatu blok diagram untuk mengekspresikan pandangan dari atas ke bawah, dan

memberikan gambaran bagaimana data berjalan mulai dari input sampai ke output dengan menggunakan *Data Flow Diagram* (DFD) untuk operasi ECC.
Model Proyeksi ($X/Z^2$, $Y/Z^2$) yang didapatkan adalah:
Kurva Hessian: X3 + Y3 = 3dXY dengan proyeksi pada ($X/Z^2$, $Y/Z^2$)

Dari gambar 3 dapat dikatakan bahwa terdapat diagram blok menggunakan 4 multipliers yang muncul jika digunakan kurva proyeksi Hessian yang dipilih yaitu ($X/Z^2$, $Y/Z^2$). Dari model tersebut juga, dapat dikatakan bahwa multiplikasi berurutan sebanyak 6.




Gambar 3. DFD untuk Point Doubling – ($X/Z^2$, $Y/Z^2$)

## KESIMPULAN

Dalam jurnal ini diperkenalkan suatu algoritma yang baru untuk komputasi kriptografi kurva eliptik yang menggunakan kurva Hessian pada GF(p). Di mana ECC didapatkan dari operasi invers modular pada perhitungannya, dan penelitian ini hanya menggunakan satu koordinat proyeksi yaitu $(X/Z^2, Y/Z^2)$. Proyeksi $(X/Z^2, Y/Z^2)$ jika diterapkan pada kurva Hessian akan memiliki 6 multiplikasi berurutan.

## DAFTAR PUSTAKA

Anonim. 1999. *Recommended Elliptic Curves For Federal Government Use*

Basu, S. 2011. A New Parallel Window-Based Implementation of the Elliptic Curve Point Multiplication in Multi-Core Architectures. *International Journal of Network Security Vol.13 No.3, PP.234.*

Certicom Research. 2000. *Standards For Efficient Cryptography - SEC 2: Recommended Elliptic Curve Domain Parameters,* secg-talk@lists.certicom.com.

Fahad Bin Muhaya, Qasem Abu Al-Haija', Loai Tawalbeh. 2010. Applying Hessian Curves in Parallel to improve Eliptic Curve Scalar Multiplication Hardware. *International Jurnal of Security and It's Applications Vol. 4 No.2.*