# IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK PADA SISTEM KEAMANAN SMART CARD

**Sahbuddin Abdul Kadir[1)] dan Andi Muis[2)]**
[1,2)]*Dosen Jurusan Teknik Elektro Politeknik Negeri Ujung Pandang*

## ABSTRACT

This research proposed to get security system implementation method on smart card by using Elliptic Curve Cryptography. The Elliptic Curve Cryptography designed by system on chip using Hardware Description Language (HDL) verilog with binary and Non-Adjacent Form (NAF). As result it got core processor that have to be simulated to show the validation of the data after cryptographic process. The simulation show that the data is valid and ready to implementation on the next term to get probability of security system secure for smart card.
**Keywords:** Elliptic Curve Cryptography, Binary, Non-Adjacent Form, smart card, Processor.

## 1. PENDAHULUAN

Smart card adalah kartu yang memiliki sistem embedded di dalamnya. Sistem Embedded tersebut berupa IC mikrokontroller untuk memproses aliran data yang keluar dan masuk pada memori chip. Smart card biasa digunakan dalam transaksi pembayaran barang non-tunai, pembayaran ongkos alat transportasi umum, SIM card dalam handphone, atau dalam sistem pembayaran lainnya sebagai penyimpan informasi elektronis identitas pengguna. Dalam smart card, data-data yang disimpan dalam memori terenkripsi atau diacak secara algoritmis matematis yang biasa disebut dengan kriptografi. Jika orang lain mencoba membaca langsung informasi penting yang terkandung dalam memori s mart card tersebut, data yang dibaca seakan-akan telah diacak-acak urutannya sehingga sangat sulit untuk diartikan. Maka, untuk membaca isi informasi dalam smart card, card reader harus berhubungan dengan mikroprosesor yang terdapat dalam kartu dahulu dan meminta mikroprosesor untuk menerjemahkan atau mendekripsi data dalam memori menjadi data utuh yang akan disampaikan ke reader. Sebelum mikroprosesor dapat memproses dalam memori, mikroprosesor meminta kode kunci kepada card reader terlebih dahulu, seperti password, gambar sidik jari, retina, atau tanda-tanda identifikasi personal lainnya yang sulit diketahui atau dipalsukan orang kecuali pemilik smart card itu sendiri. Oleh karena itu, tingkat keamanan data yang tersimpan dalam s mart card lebih tinggi dibanding kartu pita magnetik biasa. Tetapi pada saat smart card digunakan, prosesornya akan memancarkan informasi tambahan *(side effect)* yang dapat dimamfaatkan orang lain untuk mendapatkan pesan-pesan rahasia yang semestinya aman malalui analisis waktu, komsumsi daya dan radiasi elektromagnetik (Clemens. 2008). Oleh karena itu, Pada implementasi sistem keamanan diperlukan analisis kemungkinan penyerangan terhadap perangkat yang menggunakan sistem keamanan tertsebut. Penyerangan ini biasa dilakukan dengan perangkat lunak untuk memecahkan proses matematis kriptografi. Namun cara ini me merlukan waktu yang lama karena proses matematis kriptograpi kurva eliptik sangat kompleks. Sebaliknya waktu yang diperlukan menjadi lebih singkat jika dilakukan dengan perangkat keras yang memamfaatkan informasi tambahan dan dapat dideteksi sebagai *Side Channel Attack* atau SCA *(Zulkipli,* 2009*)*.Pada penelitian ini, akan dilakukan implementasi dan percobaan serangan terhadap prosesor sistem kriptografi kurva eliptik atau *Elliptic Curve Cryptography* (ECC) menggunakan Algoritma Binary dan NAF *(Non-Adjacent-Form)* pada FPGA Altera Cyclone II sebagai prototipe smart card untuk mendapatkan metode implementasi kriptografi kurva eliptik sebagai sistem keamanan *Smart Card* yang lebih *resistant* terhadap serangan SCA. Sehingga informasi yang tersimpan dalam smart card tetap aman.

## 2. KAJIAN LITERATUR DAN PEGEMBANGAN HIPOTESIS

### 2.1 Smart Card

*Smart card* sering disebut sebagai *chip card* atau *integrated circuit* (IC) *card*. Definisi *chip card* sendiri yaitu kategori umum yang mencakup *smart card* dan *memory card*. *Smart card* adalah *plastic card* yang mengandung *memory chip* dan *microprocessor*. Kartu ini bisa menambah, menghapus, mengubah informasi yang terkandung. Keunggulannya adalah *smart card* tidak perlu mengakses *database* di server karena sudah ada sebagian terkandung di kartu. Sedangkan *memory* dipasangi memory silicon tanpa microprocessor.

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*


**Gambar 1. Chip *Smart Card***

Fungsi dasar suatu smart card adalah untuk mengidentifikasi card holder ke sistem komputer. Cardholder di sini adalah pemilik asli kartu tersebut. Identifikasi ini menyangkut otentifikasi organisasi yang membuat kartu tersebut dan cardholder dan hak aksesnya.

## 2.2 Kriptografi

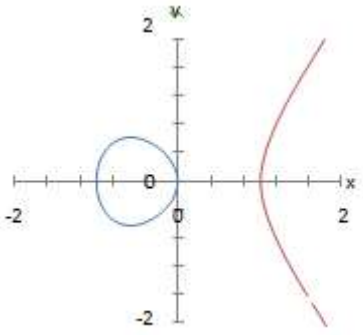
Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

## 2.3 Kriptografi Kurva Eliptik

Kriptografi kurva eliptik menggambarkan setiap titik pada kurva eliptik sebagai pesan yang akan dikirim pada jaringan. Sebelum dikirim, titik ini dikalikan dengan sebuah nilai (k) untuk mendapatkan titik yang lain pada kurva eliptik. Operasi utama yang dilakukan pada proses enkripsi dan dekripsi kurva eliptik adalah point-multipication. Point-multipication adalah perkalian pada kurva untuk mendapatkan Q=k*P. Dimana Q adalah chipper text, P adalah plain text yang merupakan titik pada kurva eliptik dan k adalah kunci pribadi. Seluruh proses pada kurva eliptik dilakukan pada galois field. Proses perkalian k*P dapat dilakukan dengan menjumlahkan nilai P sebanyak k kali. Dalam hal ini, 2P disebut point-doubling, sedangkan P+R disebut dengan point-addition. Kurva eliptik yang digunakan pada prosesor kritografi bukan berarti menggunakan operasi matematis yang biasa dilakukan pada kurva eliptik. Tetapi memamfaatkan sifat kurva eliptik yang mengambil dua titik pada kurva dan melakukan proses penjumlahan dan perkalian untuk mendapatkan titik lain pada kurva yang sama. Persamaan kurva eliptik dinyatakan dengan persamaan Weierstrass, sebagai berikut:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Dari persamaan ini, dibuat berbagai persamaan kurva eliptik. Contoh persamaan kurva eliptik dapat dilihat pada gambar 2.




**Gambar 2. Persaman Kurva Eliptik**

$$E: y^2 = x^3 - x$$

Dengan melakukan penyederhanaan pesamaan Weierstrass, dimana karakteristik K=2 dan a1≠0, maka variable x dan y :

$$(x,y) = \left(a_1{}^2x + \frac{a_3}{a_1},\ a_1{}^3y + \frac{a_1{}^2a_{4+}a_3{}^2}{a_1{}^3}\right)$$

Persamaan Weierstrass dapat disederhanakan menjadi :

$$y^2 \mid xy = x^3 \mid a_2x^2 \mid a_6b$$

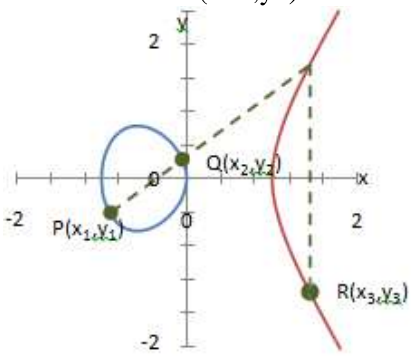
*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*

Persamaan ini disebut dengan persamaan non- supersingular dan akan digunakan pada prosesor kriptogarfi kurva eliptik. Setiap titik di luar field K pada kurva disebut titik tak hingga dan dinotasikan dengaN . Jika titik P dan Q elemen :

$$E: y^2 + xy = x^3 + a_2x^2 + a_6b$$

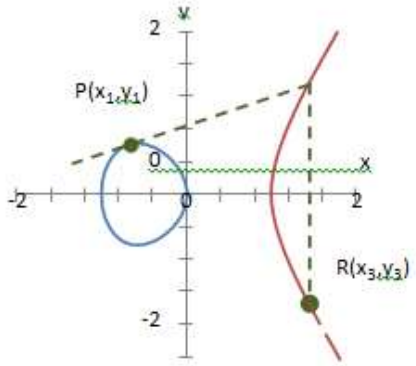
maka akan berlaku hukum kurva eliptik sebagai berikut:

1. Setiap proses $P \mid \sigma_\omega = P$ dan $\sigma_\omega + P = P$, untuk $P \in E$
2. $-\sigma_\omega = \sigma_\omega$
3. Jika P(x,y), maka –P(x,x+y).
4. Point addition, untuk dua titik P(x1,y1 ) dan Q(x2 ,y2) dimana P Q, maka P+Q=R, dengan R(x3,y3) ∈ E seperti pada gambar 2.2.
5. Point doubling, titik P(x1,y1) dan P maka 2P=( x3 ,y3) ∈ E.




**Gambar 3. Point addition P+Q=R**

Gambar 3. memperlihatkan proses penjumlahan dua titik P dan Q pada kurva eliptik. Penjumlahan dilakukan dengan menarik garis lurus yang menghubungkan 2 titik tersebut dan memetakan titik potong ketiga (perpotongan garis lurus dengan kurva eliptik). Titik potong ketiga kemudian dicerminkan untuk mendapatkan titik R sebagai hasil penjumlahan titik P dan Q. Proses point doubling dalam bentuk grafik diperlihatkan pada gambar 4. untuk mendapatkan titik R yang menyatakan hasil penjumlahan dua titik yang sama 2P atau point doubling..




**Gambar 4. Point doubling 2P**

Jika P=(x1,y1 ) dan Q=(x2 ,y2), maka R = P+Q = (x3 ,y3) dan P≠Q adalah point addition:

$$\theta = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \theta^2 \mid \theta \mid x_1 \mid x_2 \mid a_2$$

$$y_3 = \theta(x_1 \mid x_3) - y_1$$

Jika P = Q = (x1,y1), maka R = 2.P = (x3,y3 ) dan P = Q adalah point doubling:

$$\theta = x + \frac{y}{x}$$

$$x_3 = \theta^2 + \theta + a_2$$

$$y_3 = x^2 + (\theta + 1)x_3$$

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*

## 2.4. Algoritma Perkalian Kurva Eliptik

Proses perkalian pada kurva eliptik akan dilakukan dalam field F2 m menggunakan normal basis. Sedangkan perhitungan Q = k*P dapat dilakukan dengan perkalian k dari LSB ke MSB atau dari MSB ke LSB menggunakan metode repeated-square-and-multiply (RSAM).

### 2.4.1 Metode Perkalian binary dari LSB ke MSB

1. Masukan: K = (kt-1, ..., k1, k0)
2. Keluaran: k * P
3. Q =
   For i=0 to t-1
   Jika ki = 1 maka Q = Q + P;
   P = 2P;
4. Output Q

### 2.4.2 Metode Perkalian binary dari MSB ke LSB

1. Masukan: K = ($k_{t-1}$, ..., $k_1$, $k_0$)
2. Keluaran: k * P
3. Q = ∞
   For i=t-1 to 0
   Q = 2Q;

Jika ki = 1 maka Q = Q + P;

4. Output

### 2.4.3 Metode Perkalian NAF (Non-Adjacent- Form)

Metode ini akan mengubah nilai k yang dapat mengurangi proses *point addition*. Pada Proses Q = 15*P, dapat dilakukan dengan Q = (16-1)*P. Dimana Q = (16-1)*P = (2P)2*2*2- P, jika dibandingkan dengan Q = 15*P = P+2(P+2(P+2P)) proses yang dilakukan menjadi lebih sedikit dan prosesor dapat bekerja lebih cepat. Algoritma NAF adalah sebagai berikut:

Masukan: K=($k_{t-1}$, ..., $k_1$, $k_0$) positif integer

1. i=0
2. while k 1 ≥

jika k ganjil maka $k_i$=2-(k mod 4), k=k-$k_i$
else $k_i$ = 0 k=k/2

3. output k

Proses NAF melakukan pengecekan teradap bit k, jika terdapat 2 bit terakhir k bernilai 1 maka nilai k, akan diganti dengan -1, sedangkan jika 2 bit terakhir nilai k bernilai 0 atau 1, maka nilai k, akan tetap 0 atau 1. Kemudian k digeser 1 bit ke kanan (k/2), dan proses ini dilakukan hingga k bernilai 1. Metode perkalian NAF(k) dari MSB ke LSB dapat dilakukan sebagai berikut:

Masukan: K = ($k_{t-1}$, ..., $k_1$, $k_0$) Keluaran: k * P

1. Q = ∞
2. For i=t-1 to 0

Q = 2Q;
Jika ki = 1 maka Q = Q + P; Jika ki = -1 maka Q = Q - P;

3. Output Q

## 2.6 Studi Pendahuluan

Studi tentang kriptografi kurva eliptik telah dilakukan oleh Zulkifli pada tahun 2009. Penelitian yang dilakukan dengan percobaan penyerangan pada prosesor kriptografi kurva eliptik yang diimplementasikan pada FPGA sebagai prototipe s mart card, untuk mengetahui tingkat probabilitas kunci sistem kriptografi kurva eliptik melalui analisis konsumsi daya. Seperti dikatahui pada proses kriptografi kurva eliptik terdapat dua proses utama yang membangkitkan *side effect* yaitu point addition dan doubling. Kedua proses ini memiliki karakteristik yang berbeda, sehingga dapat diamati dan dianalisis untuk mendapatkan kunci yang digunakan saat kriptografi berlangsung. Hasil penelitian menunjukkan bahwa dengan menganalisis konsumsi daya, kunci dapat ditebak 100% .

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*

Berdasarkan hasil penelitian di atas maka sangatlah penting untuk melakukan penelitian lanjutan dengan desain metode implementasi kriptografi yang tahan terhadap *side channel attack* menggunakan metode Non Adjacent Form pada *smart card*.

## 3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini merupakan metode eksperimen yang dimulai dengan desain prosesor kriptografi kurva eliptik sebagai sistem keamanan pada *samrt card*. Hasil dari perancangan ini disimulasikan untuk memperlihatkan validitas output yang dihasilkan dengan input yang diberikan.

### 3.1 Prosesor Kriptografi Kurva Eliptik

Prosesor kriptografi kurva eliptik didesain untuk melakukan aritmetika dasar kritografi kurva eliptik Q=k*P. Dimana, k adalah kunci pribadi dan P adalah kunci publik. Sedangkan Q adalah chipper text hasil enkripsi. Kurva yang digunakan adalah $y^2 + xy = x^3 + a_2x^2 + a_6b$. Proses kriptografi ini menggunakan optimal normal basis 158 bit. Pemilihan jumlah bit kunci didasarkan pada tingkat keamanan 160 bit kunci.

### 3.2 Datapath Prosesor Kriftografi Kurva Eliptik

Proses ECC dilakukan dengan 158 bit, nilai 158 bit menyatakan jumlah bit kunci. Sedangkan input dan output prosesor ECC ini adalah 32 bit. Operasi matematis prosesor ECC menggunakan normal basis. Operasi matematis terdiri atas AND, XOR dan Cyclic Shift Register.

### 3.3 FSM Perkalian Binary

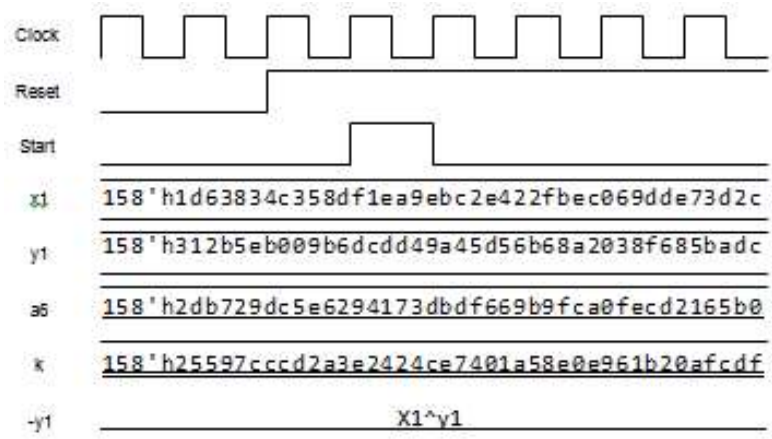
FSM unit kontrol mengatur proses RSAM dan inverse. Proses RSAM akan melakukan perkalian pada kurva eliptik k*P. Proses inversi dilakukan untuk mengembalikan nilai x dan y ke koordinat affine menggunakan metode Itoh. Proses perkalian kP dilakukan selama 158 iterasi dalam koordinat Projective Lopez- Dahab. Dimana setiap iterasi akan dilakukan proses doubling sedangkan proses addition hanya dilakukan saat bit kunci bernilai '1'. Setelah interasi ke 158 akan dilakukan proses inversi.

### 3.4 FSM Perkalian NAF

FSM unit kontrol mengatur proses NAF(k), RSAM dan inverse. Proses NAF(k) akan membuat nilai $k_i$ positif dan negatif. Sedangkan proses RSAM akan melakukan perkalian pada kurva eliptik k*P. Proses inverse dilakukan untuk mengembalikan nilai x dan y ke koordinat affine menggunakan metode Itoh.

## 4. HASIL DAN PEMBAHASAN

Prosesor kriptografi kurva eliptik didesain menggunakan bahasa verilog sesuai dengan datapath yang telah dibuat sebelumnya. Untuk menjalankan prosesor kriptografi dibuatkan testbench sebagai berikut:

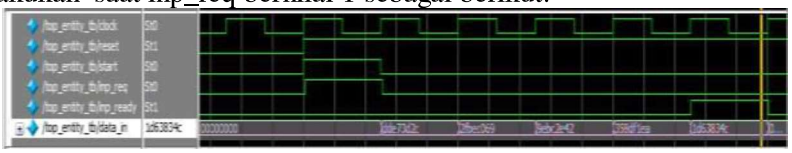



**Gambar 5. Testbench prosesor ECC**

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*

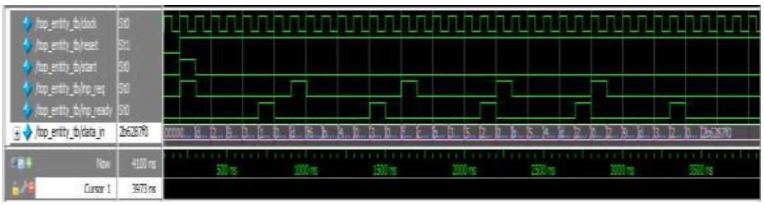
### 4.1 Data Input

Setiap data input akan diproses dengan 5 clock cycle. Urutan proses data input adalah x, y, a6, k dan –y. Proses input dilakukan saat inp_req bernilai 1 sebagai berikut:



**Gambar 6. Input data x**

Setelah 5 clock cycle inp_ready bernilai 1 dan proses input berikutnya dapat dilakukan. Proses data input dilakukan setiap 32 bit dari LSB ke MSB. Proses ini berlangsung hingga seluruh data input masuk sesuai dengan urutan sebagai berikut:



**Gambar 7. Data input x, y, a6, k, dan –y**

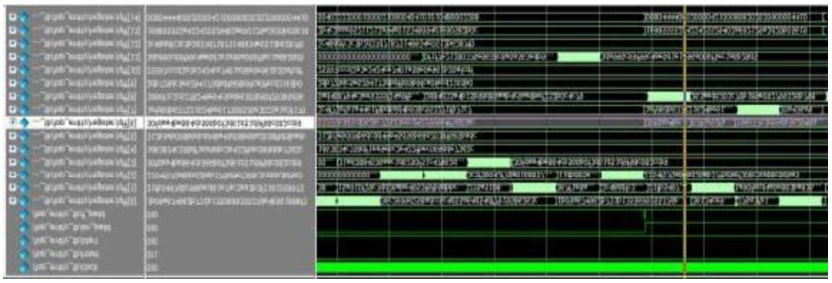
### 4.2 Proses Kriptografi Kurva Eliptik (NAF)

Proses kriptografi kurva eliptik terdiri atas point doubling dan addition. Proses ini dapat diketahui dengan mengamati sinyal en_pdoub (enable poit doubling) dan en_padd (enable point addition) sebagai berikut:

X = 183924ec885553bd474d4f610707a159babd9101

Y = 3dd22058d2dea93bf390aef7d6995d0e6c05a31b

Nilai ini masih dalam koordinat proyektif LD karena belum dilakukan proses inversi. Demikian pula nilai untuk point addition dan subraction.



**Gambar 10. Point addition**

Nilai point addtition juga sama dengan simulasi ECC Binary seperti gambar 10. pada register 6 dan 7 yaitu:

X = 30fdaa4be864cb566b0f3d61d51d9f98c082ccb9

Y = 1def60b637221624be617308530e3022a1a3f170

**Gambar 11. Point subraction**

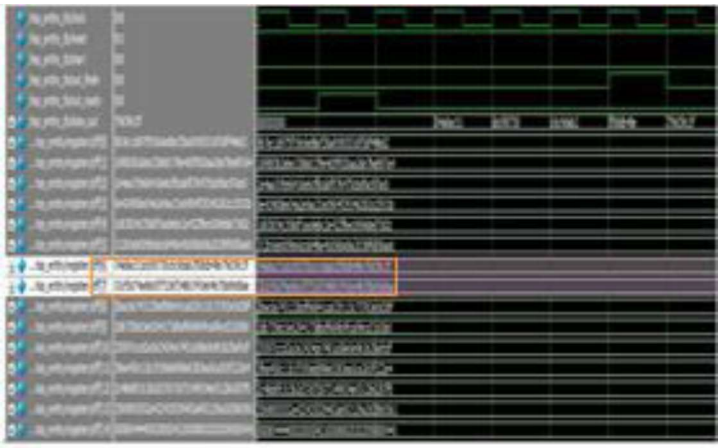
Proses point substraction sama dengan point addition tetapi nilai y yang digunakan adalah negative y pada register 12. Sedangkan untuk point addition nilai y yang digunakan adalah positif y pada register 4. Nilai x dan y point substraction juga disimpan pada register 6 dan 7 seperti pada gambar 11. yaitu: X = 03687db2b4a96fea850e5b84a7f660262b844fc7, Y = 1f86afb503b59b03130aa13a8c0676a3edd978a

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com* 

### 4.3 Data Output

Proses data output dilakukan dengan 5 clock cycle saat out_ready bernilai 1 dan out_finish bernilai 1. Setiap cycle akan diperoleh data 32 bit pada port data_out. Proses data out dilakukan pertama pada 32 bit MSB dan terakhir pada 32 bit LSB data out kriptografi seperti pada gambar 12. Nilai ini telah dikembalikan ke koordinat affine dengan proses inversi pada akhir kriptografi. Data output hasil simulasi ECC NAF juga diperoleh nilai yang sama dengan hasil simulasi ECC Binary yaitu:

X = 04a8ac51dc6fd730c6c9dab2f08db48e79d39c3f, Y = 03cf0d74a9b65f7536f34881f43e64b70b89d8ae



**Gambar 12. Data output kriptografi**

Proses simulasi kriptograpi kurva eliptik dengan algoritma NAF menunjukan keluaran yang sama dengan algoritma binary. Tetapi jika pada binary hanya terdapat point doubling dan addition. Maka pada NAF selain kedua point tersebut, terdapat point subraction yang memancarkan side effect yang sama dengan point addition yang membuat probabilitas ECC resistan terhadap side channel attack meningkat.

## 5. KESIMPULAN

Implementasi Kriprtografi Kurva Eliptik pada *Smart Card* menggunakan algoritma perkalian NAF memerlukan register tambahan untuk menyimpan nilai kunci NAF yang dibangkitkan sebelumnya dari nilai biner. Selain itu, juga ditambahkan operasi substraction atau penngurangan karena algoritma NAF menggunakan bilangan bertanda (sign). Penggunaan operasi pengurangan pada kriptografi kurva Eliptik akan meningkatkan kemanan sistem dengan adanya dua kemungkian operasi ( penambahan dan pengurangan) pada setiap bit ”1” kunci enkripsi dengan tampilan visuasasi phisik *side channel* yang sama.

## 6. REFERENSI

Andrias, Tomy. 2012. Pengertian dan Contoh Kriptografi (Cryptography) dengan Proses Enkripsi dan Dekripsi http://asalkena.blogspot.com/2012/11/pengertia n-dan-contoh.html (diakses tanggal 29 April 2015)

Fahim. 2009. Smart Card. https://fahim007.wordpress.com/2009/01/14/smart-card/#more-86 (diakses tanggal 3 April 2015)

Hankerson, Darrel., Menezes, Alfred., Vanstone, Scott. 2014. Guide to Elliptic Curve Cryptography. New York: Springer-Verlag

Heuberger, Clemens. 2008. Hamming Weight of the Non-Adjacent-Form under Various Input Statistics, University of Stellenbosch, South Africa.

Fran¸cois-Xavier Standaert, Lo¨ıc van Oldeneel tot Oldenzeel, David Samyde, Jean-Jacques Quisquater. 2003. Power Analysis of FPGAs: How Practical is the Attack?. UCL Crypto Group Laboratoire de Micro´electronique Universit´e Catholique de Louvain, Belgium.

Zulkifli. Muhammad. 2009. Aplikasi Timing dan Simple Power Analysis Attack Terhadap Prosesor Kriptografi Kurva Eliptik pada implementasi FPGA. Institut Teknologi Bandung.

Smart Card. 2009. Smart Card. http://smartcardkomas.blogspot.com/2009/11/s mart-card.html (diakses tanggal 3 April 2015)

*Corresponding : sahbuddin.ak@poliupg.ac.id, andi_muis57@yahoo.com*