PENYUSUNAN ALGORITME OPERASI GRUP YANG DIBANGKITKAN OLEH KURVA HIPERELIPTIK $y^2 + xy = x^5 + x^2 + x$ ATAS LAPANGAN $\mathbb{F}_{2^{97}}$

S. NURMALASARI[1], S. GURITMAN[2], B. P. SILALAHI[2]

Abstrak

Kurva hipereliptik adalah kelas spesial dari kurva aljabar dan dapat dipandang sebagai generalisasi kurva eliptik. Pengembangan kurva hipereliptik dapat diterapkan dalam bidang kriptografi kunci publik, seperti dalam pertukaran kunci Diffie-Hellman. Pemilihan kurva hipereliptik genus dua dengan lapangan berkarakteristik dua sangat menarik untuk dikembangkan. Parameter kurva yang tepat akan membuat kriptografi kunci publik memiliki tingkat keamanan yang tinggi dan bertahan dari serangan-serangan kriptografi seperti serangan Frey Ruck. Dalam penelitian ini akan dipilih kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$. Kemudian diperlukan efisiensi operasi grup yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$. Penelitian ini mempunyai tiga tujuan utama. Pertama menganalisa tingkat keamanan kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$. Kedua membentuk formulasi operasi grup yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$yang efisien. Ketiga membentuk algoritme operasi grup yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$.

Kata kunci: algoritme Cantor, algoritme operasi grup, divisor, formulasi operasi grup, grup kurva hipereliptik.

1 PENDAHULUAN

Perkembangan dan kemajuan teknologi informasi telah menjadi bagian dalam kehidupan manusia, tak terkecuali dalam hal komunikasi. Misalnya saja dengan jaringan internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan mudah. Salah satu contoh sederhana adalah cara masyarakat melakukan pertukaran informasi atau pesan, yang biasanya menggunakan pos sekarang beralih menggunakan email melalui jaringan internet [3]. Salah satu masalah yang dihadapi dalam pemanfaatan jaringan internet adalah keamanan data, karena jaringan internet merupakan media komunikasi umum yang dapat diakses oleh

[1] Mahasiswa S2, Program Studi Matematika Terapan, Sekolah Pascasarjana IPB, Jalan Meranti Kampus IPB Dramaga Bogor, 16680. Email: siskanurmala99@gmail.com

[2] Departemen Matematika, Fakultas Ilmu Matematika dan Pengetahuan Alam, Jalan Meranti Kampus IPB Dramaga Bogor,16680.

siapapun. Sehingga sangat rawan terhadap penyadapan informasi yang bersifat rahasia oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Berlandaskan alasan inilah diperlukan suatu teknik pengamanan yaitu teknik kriptografi. Kriptografi adalah studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi data asli [9].

Untuk mengamankan suatu data, secara umum dalam kriptografi menggunakan sebuah kunci. Awalnya pada kriptografi menggunakan kunci yang sama untuk melakukan proses enkripsi (mengubah pesan dari data awal menjadi sandi) dan dekripsi (mengubah dari sandi menjadi data awal) di mana sistem ini disebut juga sebagai kriptografi kunci simetri. Pada kunci simetri, pengiriman data rahasia antara dua pihak yang akan berkomunikasi melalui saluran tidak aman mustahil dilakukan apabila dua pihak tersebut tidak bertemu secara langsung untuk menetapkan sebuah kunci bersama. Kemudian ditemukan sebuah metode yaitu kriptografi kunci asimetri (kunci publik) . Pada kriptografi kunci publik menggunakan kunci berbeda untuk proses enkripsi dan dekripsi data atau pesan, sehingga dua pihak yang akan berkomunikasi melalui saluran tidak aman tidak harus bertemu untuk saling bertukar kunci. Hal ini merupakan solusi dalam masalah pendistribusian kunci bersama antara dua pihak yang akan berkomunisi melalui saluran tidak aman. Skema pertukaran kunci ini pertama kali diperkenalkan oleh Whitfield Deffi dan Martin Hellman pada tahun 1976 [2].

Metode pertukaran kunci Diffie-Hellman merupakan salah satu komunikasi dengan sistem kriptografi kunci publik, di mana keamanannya didasarkan pada pemecahan masalah logaritma diskret. Masalah logaritma diskret dapat didefinisikan pada sebuah grup perkalian terbatas. Grup perkalian terbatas tersebut berupa lapangan berhingga yang dibentuk oleh bilangan prima $\mathbb{G} = (\mathbb{Z}_p^*, x)$. Himpunan $\mathbb{Z}_p^*$ dikatakan suatu grup perkalian, jika perkalian $\mathbb{Z}_p^*$ dihitung dalam modulo p, operasi perkalian pada $\mathbb{Z}_p^*$ bersifat asosiatif, terdapat elemen identitas yaitu $1 \in \mathbb{Z}_p^*$, dan setiap elemen dalam grup $\mathbb{Z}_p^*$ memiliki invers. Jika diketahui suatu nilai misalkan x di dalam grup $\mathbb{Z}_{p-1}$ maka akan mudah menghitung $a^x mod\, p = y \in \mathbb{Z}_p^*$ dengan a adalah generator dari $\mathbb{Z}_p^*$, akan tetapi mencari logaritma $log_a\, y = x$ sulit untuk diselesaikan. Bilangan integer x seperti ini disebut dengan logaritma diskret dari y dengan basis a. Masalah logaritma diskret akan menjadi lebih sulit apabila menggunakan grup dengan order prima p yang sangat besar, di mana nilai p tersebut minimal 1024 bit [10]. Akan tetapi, dengan nilai prima p yang begitu besar masih ada serangan yang secara signifikan mampu menyelesaikan masalah logaritma diskret grup perkalian $\mathbb{Z}_p^*$ tersebut, yaitu serangan kriptografi indeks kalkulus. Oleh karena itu, sistem kriptografi berbasis kurva eliptik memberikan alternatif untuk mewujudkan sistem kriptografi asimetri dengan ukuran kunci yang lebih kecil dan mampu bertahan dari serangan indeks kalkulus. Standar nilai prima p pada kriptografi grup kurva eliptik adalah sebesar 160 bit [10].

Pada tahun 1987 Neal Koblitz dalam paper nya berjudul "*Elliptic Curve Cryptosystem*" , pertama kali memperkenalkan bahwa solusi untuk meningkatkan keamanan masalah logaritma diskret grup multiplikatif $\mathbb{Z}_p^*$, yaitu dengan mendefinisikan sistem kriptografi berbasis kurva eliptik [6]. Selanjutnya, Neal Koblitz juga menulis paper dengan judul "*Hyperelliptik Cryptosystem*", dalam paper tersebut dipaparkan bahwa solusi alternatif untuk meningkatkan derajat keamanan dari skema Diffie-Hellman adalah mendefinisikan sistem kriptografi berbasis kurva hipereliptik [7]. Pada sistem kriptografi berbasis grup kurva hipereliptik tersebut, diharapkan mampu menawarkan tingkat keamanan lebih tinggi dengan ukuran kunci yang lebih kecil dibandingkan grup multiplikatif $\mathbb{Z}_p^*$ dan grup kurva eliptik. Oleh karena itu, sistem kriptografi kurva hipereliptik sangat menarik untuk dikembangkan, akan tetapi masih terkendala oleh perhitungan operasi grup yang menyebabkan waktu komputasi menjadi semakin lama. Sehingga untuk mempercepat waktu komputasi pada grup kurva hipereliptik secara umum menggunakan algoritme Cantor [1]. Dalam kasus khusus, kurva hipereliptik genus dua atas lapangan biner memberikan efisiensi waktu komputasi yang lebih cepat dibandingkan menggunakan algoritme Cantor [5]. Kasus khusus lain pada penelitian Vijayakumar et al. [11] yaitu, memilih kurva hipereliptik terbaik dan menganalisis efisiensi waktu komputasi kurva hipereliptik dengan genus 2,3,4,5, dan 6 atas lapangan tertentu.

Pada penulisan ini akan mengkonstruksi operasi grup dengan mengoptimumkan formulasi operasi ganda dan operasi adisi kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$ yang diperoleh dari hasil ekplorasi kurva. Dari hasil formulasi tersebut dapat disusun algoritme operasi ganda dan operasi adisi, sehingga implementasinya dapat dilakukan dengan menggunakan sumber komputasi yang tersedia saat ini.

Adapun tujuan dari penelitian ini adalah

1. Memilih dan menganalisa keamanan kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$.
2. Membentuk formulasi operasi grup yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$.
3. Menyusun algoritme operasi grup yang dibangkitkan oleh kurva $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$.

2 TINJAUAN PUSTAKA

Kurva Hipereliptik

Misalkan K adalah suatu lapangan dan $\bar{K}$ adalah ketertutupan aljabar (*algebraic closure*) dari K. Suatu kurva hipereliptik *(hyperelliptic curve)* C dengan genus g atas K $(g > 1)$ adalah suatu persamaan yang berbentuk

$$C: y^2 + h(x)y = f(x) \text{ di dalam } K[x, y]$$

dengan $h(x), f(x) \in K[x], deg_x(h(x)) < g$ sedangkan $f(x)$ adalah monik dan $deg_x f(x) = 2g + 1$, serta C memilik sifat tidak memuat titik singular. Ini berarti tidak ada $(u, v) \in \overline{K} \times \overline{K}$ yang secara simultan memenuhi ketiga persaman berikut ini:

$$y^2 + h(x)y = f(x)$$
$$2y + h(x) = 0$$
$$h'(x) = f'(x)$$ [7].

Representasi Divisor Semi Tereduksi

Lema 1

Jika $T = (u, v)$ adalah titik biasa pada C, maka untuk setiap integer $k \geq 1$, ada tepat satu polynomial $b_k(x) \in \overline{K}[x]$ sedemikian sehingga:

1. deg $(b_k) < k$
2. $b_k(u) = v$
3. $b_k^2(x) + h(x)b_k(x) \equiv f(x) \bmod (x - u)^k$ [7].

Representasi Divisor Tereduksi

Misalkan $D = \sum m_i T_i - (\sum m_i)\infty$ adalah divisor semi tereduksi. Jika $\sum m_i < g$ dengan g adalah genus dari C, maka D disebut divisor tereduksi [7].

Representasi Komputasi Anggota H

Berikut ini akan difokuskan pada kurva genus dua dan atas lapangan biner $\mathbb{F}_{2^m}$, maka notasi kelas divisor $D = div\,(a, b) \in \mathbf{H}$ berarti $a(x)$ dan $b(x)$ adalah polinomial atas $\mathbb{F}_{2^m}$, dengan $a(x)$ monik, dan memenuhi syarat berikut:

1. deg $(a(x)) < 2$
2. deg $(b(x)) <$ deg $(a(x))$
3. $a(x)$ membagi $b^2(x) + h(x)b(x) + f(x)$ [7].

Demi kepentingan komputasi yang pada gilirannya untuk diterapkan dalam bidang kriptografi, pada penulisan ini akan merepresentasikan anggota **H** dan mengklasifikasikannya sebagai berikut dengan $\alpha, \beta, \gamma,$ dan δ diasumsikan anggota $\mathbb{F}_{2^m}$.

1. $D_2 = [[1, \alpha, \beta], [\gamma, \delta]]$ merupakan representasi dari $div\,(a, b)$, dimana
   $$a(x) = x^2 + \alpha x + \beta \text{ dan } b(x) = \gamma x + \delta \text{ dengan } \alpha \neq 0.$$
   Dalam makna geometri, jika $\alpha \neq 0$, D_2 terdiri dari dua titik rasional berhingga yang berbeda, dan jika $\alpha = 0$, D_2 terdiri dari dua titik rasional berhingga yang sama.
2. $D_1 = [[0,1, \beta], [0, \delta]]$ merupakan representasi dari $div\,(a, b)$, dengan
   $$a(x) = x + \beta \text{ dan } (x) = \delta\ .$$
   Dalam makna geometri, D_1 terdiri dari tepat satu titik rasional berhingga dan jika $\delta = 0$, D_1 terdiri dari tepat satu titik khusus.

3. $D_0 = [[0,0,1],[0,0]]$ merupakan representasi dari $div\ (a,b)$, dengan
$$a(x) = 1 \text{ dan } b(x) = 0$$
yang merupakan unsur identitas dari **H.** Dalam makna geometri, N titik di tak-hingga [4].

Lema 2

Diberikan kurva hipereliptik C atas lapangan $\mathbb{F}_{2^m}$ sebagai
$$y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$
Untuk $1 \le k \le 4$, jika dimisalkan $y \equiv b(x) \bmod (x+u)^k$ dengan
$$b_k = \sum_{i=0}^{k-1} c_1(x+u)^i.$$
Menurut Lema 1, maka c_0 dihitung sebagai salah satu solusi dari persamaan kuadrat
$$y^2 + h(u)y + f(u) = 0.$$
Berikutnya, c_i, untuk $1 \le i \le 3$, dihitung secara rekursif berdasarkan formulasi
$$c_1 = \frac{u^4 + f_3x^2 + f_1 + c_0h_1}{h(u)}$$
$$c_2 = \frac{uf_3 + f_2 + c_0h_2 + c_1h_1 + c_1}{h(u)}$$
$$c_3 = \frac{f_3 + c_1h_2 + c_2}{h(u)} \qquad [4].$$

Algoritme Cantor

Algoritme cantor adalah dasar algoritme yang digunakan untuk operasi grup, seperti operasi adisi dan operasi ganda dari dua divisor pada grup jacobian dari kurva hipereliptik. Algorime ini diberikan dalam dua tahap sebagaimana diberikan berikut ini.

a. Tahap Semi Tereduksi

Input: Divisor tereduksi $D_1 = div(a_1, b_1)$ dan $D_2 = div(a_2, b_2)$ didefinisikan pada kurva $y^2 + h(x)y = f(x)$ atas lapangan umum K.

Output: Divisor semi tereduksi $D = div(a,b)$ dengan $D \sim D_1 + D_2$.

1. Gunakan algoritme euclidean diperluas untuk menghitung polinomial d_1, e_1, dan e_2 dengan $d_1 = \gcd(a_1, a_2)$ dan $d_1 = e_1a_1 + e_2a_2$.
2. Gunakan algoritme euclidean diperluas untuk menghitung polinomial d, c_1, dan c_2 dengan $d = \gcd(d_1, b_1 + b_2 + h)$ dan $d = c_1d_1 + c_2(b_1 + b_2 + h)$.
3. Definisikan nilai $s_1 = c_1e_1$, $s_2 = c_1e_2$ dan $s_3 = c_2$ sehingga
$$d = s_1a_1 + s_2a_2 + s_3(b_1 + b_2 + h).$$
4. Hitung nilai
$$a = \frac{a_1a_2}{d^2}$$

dan

$$b = \frac{s_1 a_1 + s_2 a_2 + s_3(b_1\, b_2 + f)}{d} \bmod a.$$

5. *Output* (a, b).

b. Tahap Tereduksi

Input: Divisor semi tereduksi $D = div(a, b)$ sebagai *output* algoritme semi tereduksi.

Output: Secara tunggal divisor tereduksi $D' = div(a', b')$ dengan $D' \sim D$.

1. Hitung

$$a' = \frac{(b^2 + b - f)}{a}$$
$$b' = (-h - b) mod\ a'.$$

2. Jika $\deg(a') > 2$ dan didefinisikan $a \leftarrow a', b \leftarrow b'$, kembali ke langkah 1.
3. Misalkan c adalah koefisien pemuka dari a', definisikan
$$a' \leftarrow c^{-1} a'.$$
4. *Output* (a', b') [1].

3 METODE

Langkah-langkah umum yang akan dilakukan pada penelitian ini adalah sebagai berikut:

1. Memilih dan menganalisa keamanan kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$.
2. Membentuk formulasi operasi ganda efisien dengan menggunakan algoritme Cantor dari grup yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$atas lapangan $\mathbb{F}_{2^{97}}$.
3. Menyusun algoritme operasi ganda yang dibangkitkan oleh kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$atas lapangan $\mathbb{F}_{2^{97}}$.

Pemilihan Kurva

Pada pemilihan kurva, terlebih dahulu tetapkan nilai m sebelum polinomial tak teruraikan dibangkitkan. Tetapkan genus g sebesar dua, selanjutnya eksplorasi kurva untuk membangkitkan kurva hipereliptik dengan genus dua di mana proses pembangkitan kurva tersebut dengan membangkitkan polinomial $h(x)$ dan $f(x)$ secara acak. Pada polinomial $h(x)$ terdiri dari tiga parameter h_0, h_1, dan h_2 yang akan dibangkitkan secara acak, dengan $h_0, h_1, h_2 \in \{0,1\}$. Sedangkan polinomial $f(x)$ parameter yang harus dibangkitkan secara acak terdiri dari lima parameter yaitu, f_0, f_1, f_2, f_3, dan f_4 serta penetapan parameter f_5 yang bernilai 1, dengan $f_0, f_1, f_2, f_3, f_4 \in \{0,1\}$. Selanjutnya, uji kurva tersebut berdasarkan definisi kurva hipereliptik dengan menggunakan *software* simbolik.

Analisis Keamanan

Untuk menerapkan sistem kriptografi logaritma diskret menggunakan kurva hipereliptik, haruslah memilih kurva C dengan lapangan yang sesuai. Berikut diberikan sifat-sifat untuk memilih lapangan yang sesuai pada kurva tersebut.

1. Aritmatik dalam lapangan K harus efisien untuk diimplementasikan, lapangan hingga berkarakteristik dua sangat menarik untuk dipilih.
2. Orde grup Jacobian $J(K)$ dari C, dinotasikan sebagai $\#J(K)$ harus terbagi oleh bilangan prima yang besar. Berdasarkan tekhnologi komputer saat ini untuk memastikan keamanan kurva, $\#J(K)$ harus terbagi oleh bilangan prima r yang mempunyai minimal 45 digit. Selanjutnya untuk menghindari serangan Frey dan Rück, r haruslah tidak dapat dibagi oleh q^{k-1} untuk semua k, dimana masalah logaritma diskret didalam $\mathbb{F}_{q^k}$ ada jika $(1 \leq k \leq 2000/(log_2 q))$.

4 HASIL DAN PEMBAHASAN

Grup Jacobian Kurva $y^2 + xy = x^5 + x^2 + x$ atas Lapangan $\mathbb{F}_{2^{97}}$

Berikut merupakan orde dari grup Jacobian **H** dengan kasus kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$. Orde dari grup **H** yang dinotasikan sebagai #**H** adalah 59 digit, yaitu sebesar $251084069415467379963903548856251249433764395706842274777 54$ dan memiliki subgrup non-trivial berorder prima besar, dalam hal ini faktorisasi prima dari #**H** adalah sebagai berikut:

$$1847339246386882691031879467675407194071690990701961 9 * (2 * 3 * 1747).$$

Faktorisasi prima besar ini menunjukkan bahwa sistem kriptografi kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$ dapat bertahan dari serangan Poligh Helman dan karena faktorisasi prima besar dari #**H** adalah sebesar 53 digit, maka sistem kriptografi kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$ dapat bertahan dari serangan Polard Rho. Selanjutnya, prima besar dari faktorisasi #**H** tidak terbagi oleh $2^{97^{k-1}}$ untuk semua k, maka system kriptogragi kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$ dapat bertahan dari serangan Frey Ruck, di mana masalah logaritma diskret didalam $\mathbb{F}_{2^{97k}}$ ada jika $(1 \leq k \leq 2000/(log_2 2^{97}))$.

Formulasi Operasi Ganda

Berikut ini akan menerapkan hasil formulasi operasi divisor untuk menurunkan algoritme operasi grup Jacobian **H** dari kasus kurva hipereliptik $\boldsymbol{y^2 + xy = x^5 + x^2 + x}$ atas lapangan $\mathbb{F}_{2^{97}}$. Untuk memudahkan formulasi operasi dari grup H, dapat dibedakan dalam dua kasus kasus berikut ini.

1. **Kasus** $D = \left[[1, \alpha, \beta], [\gamma, \delta]\right]$.
   Representasi D dapat ditulis sebagai div(a,b), dengan
   $$a = x^2 + \alpha x + \beta \text{ dan } b = \gamma x + \delta.$$
   Misalkan
   $$q = \text{Quo(a,h)} = x + \alpha \text{ dan } r = a \bmod h = \beta,$$
   maka perhatikan dua kasus berikut ini.
   (a) Jika $r = 0$ berarti $\beta = 0$, maka diperoleh $d = \gcd(a, h) = h$. Sehingga
   $$d = 0 \cdot a + 1 \cdot h \text{ dan } a = qd.$$
   Oleh karena itu,
   $$a' = \frac{a^2}{d^2} = q^2 = (x + \alpha)^2 = x^2 + \alpha^2$$
   $$b' = c_0 + c_1(x + \alpha) = c_1 x + c_1\alpha + c_0.$$
   Dari Lema 2, diperoleh
   $$c_0 = b(\alpha) = \gamma\alpha + \delta$$
   $$c_1 = \frac{\alpha^4 + \gamma\alpha + \delta + 1}{\alpha}.$$
   Jika $\alpha \neq 0$, sehingga diperoleh
   $$D \boxplus D = \left[[1,0,\beta'], [\gamma', \delta']\right]$$
   dengan formulasi
   $$\beta' = \alpha^2$$
   $$\gamma' = \frac{\alpha^4 + \gamma\alpha + \delta + 1}{\alpha}$$
   $$\delta' = \alpha^4 + 1.$$
   Jika $\alpha = 0$ berarti $a = x^2$, sehingga $D \sim N$. Oleh karena itu $D \boxplus D = N$.
   (b) Jika $r \neq 0$, sehingga diperoleh
   $$d = \gcd(a, h) = r \text{ dan } d = 1 \cdot a + q \cdot h\,.$$
   Dari algoritme tahap semi tereduksi, diperoleh
   $$a' = \frac{a^2}{d^2}$$
   $$b' = \frac{ab + q(b^2 + f)}{d} \bmod a'.$$
   Misalkan
   $$b' = \frac{y_3 x^3 + y_2 x^2 + y_1 x + y_0}{d},$$
   sehingga diperoleh
   $$y_3 = (\gamma + 1)\gamma + \alpha^3 + 1$$

$$y_2 = (\alpha^3 + 1)\alpha + \beta^2 + \delta + 1$$
$$y_1 = \delta^2 + \beta\gamma + \alpha(\beta^2 + \delta + 1)$$
$$y_0 = \beta\delta + \alpha(\beta^2\alpha + \delta^2).$$

Dari algoritme tahap tereduksi, misalkan

$$c_2x^2 + c_1x + c_0 = \frac{b^2 + bh + f)}{a}.$$

Sehingga diperoleh,

$$c_2 = y_3^2$$
$$c_1 = \beta^2$$
$$c_0 = (\alpha^2 y_3 + \beta)y_3 + y_2^2.$$

Kasus $c_2 = 0$ maka $y_3 = 0$, oleh karena itu

$$D \boxplus D = \left[[1,0,\beta'],[0,\delta']\right].$$

dengan formulasi

$$\beta' = \frac{c_0}{c_1} = \left(\frac{y_2}{\beta}\right)^2$$
$$\delta' = b(\beta') + h(\beta') = \frac{y_2(\beta')^2 + (y_1 + d)\beta' + y_0}{d}.$$

Kasus $c_2 \neq 0$, maka γ' dan δ' dihitung sebagai berikut

$$\gamma'x + \delta = \frac{y_3x^3 + y_2x^2 + (y_1 + d)x + y_0}{d} \bmod (x^2 + \alpha'x + \beta').$$

Oleh karena itu,

$$D \boxplus D = \left[[1,\alpha',\beta'],[\gamma',\delta']\right]$$

dengan formulasi

$$\alpha' = \frac{c_1}{c_2} = \left(\frac{\beta}{y_3}\right)^2$$
$$\beta' = \frac{c_0}{c_2} = \alpha^2 + \frac{\beta}{y_3} + \left(\frac{y_2}{y_3}\right)^2$$
$$\gamma' = \frac{\alpha'(\alpha' y_3 + y_2)^2 + \beta' y_3 + y_1 + d}{d}$$
$$\delta' = \frac{\beta'(\alpha' y_3 + y_2)^2 + y_0}{d}.$$

2. **Kasus** $D = \left[[0,1,\beta],[0,\delta]\right]$.

Representasi D dapat ditulis sebagai div(a,b), dengan

$$a = x + \beta \text{ dan } b = \delta.$$

Dari Lema 1, diperoleh

$$a' = a^2 = (x + \beta)^2 = x^2 + \beta^2$$
$$b' = c_0 + c_1(x + \beta) = c_1x + c_1\beta + c_0.$$

Dari Lema 2, diperoleh

$$c_0 = \delta \text{ dan } c_1 = \frac{\beta^4 + \delta + 1}{\beta}.$$

Oleh karena itu,

$$D \boxplus D = \left[[1,0,\beta'],[\gamma',\delta']\right]$$

dengan formulasi

$$\beta' = \beta^2$$
$$\gamma' = \frac{\beta^4 + \delta + 1}{\beta}$$
$$\delta' = \beta^4 + 1.$$

Jika $\beta = 0$, maka

$$D \boxplus D = N.$$

Algoritme Operasi Ganda

Hasil formulasi operasi ganda pada pembahasan diatas dapat disederhanakan dalam bentuk algoritme, yang mana langkah-langkah penyusunan algoritmenya disesuaikan dengan urutan perhitungan formulasi operasi ganda yang telah dioptimumkan.

INPUT: $D = [[\,x, A, B\,]\,,[\,P, S]]$ sebagai representasi sembarang anggota **H** yang berarti $x \in \{0,1\}$, serta A, B, P, dan S anggota lapangan $\mathbb{F}_{2^{97}}$

OUTPUT: $D \boxplus D = [\,[\,x', A', B'\,]\,,[\,P', S'\,]\,]$ anggota **H** hasil *doubling* dari D.

1. Jika $x = 1$
   a. Untuk $B \neq 0$, hitung

   $Y_3 = (\,P + 1)P + A^3 + 1;$ $\quad Y_2 = (A^3 + 1)A + B^2 + S + 1;$

   $Y_1 = (\,B^2 + S + 1)A + BP + S^2;$ $\quad Y_0 = SB + AS^2 + (AB)^2\,.$

   Jika $Y_3 \neq 0$, maka

   $$K = (B^2)^{-1}; \quad Z = A'Y_3 + Y_2; \quad C = B; \quad J = C^{-1}.$$
   $$x' = 1\,;$$
   $$A' = (\,Y_2K\,)^2;$$
   $$B' = (\,Y_2K)^2 + BK + A^2;$$
   $$P' = (\,A'Z + B'^{Y_3} + Y_1)J + 1;$$
   $$S' = (\,B'Z + Y_0)J.$$

   Return $(\,[\,[\,x', A', B'\}]\,,[\,P', S'\,]\,]\,)$.

   Jika $Y_3 = 0$, maka

   $x' = 0; \quad A' = 1; \quad P' = 0; \quad B' = (Y_2J)^2;$

   $S' = [(\,Y_2B' + Y_1 + B)B + Y_0]J.$

   Return $(\,[\,[\,x', A', B'\}]\,,[\,P', S'\,]\,]\,)$.

   b. Untuk $B = 0$, hitung.

   Jika $A \neq 0$, maka

   $$x' = 1; \quad A' = 0; \quad B' = A^2; \quad T = A^{-1};$$
   $$P' = (\,S + 1)T + P + A^3; \quad S' = A^4 + 1.$$

   Return $(\,[\,[\,x', A', B'\}]\,,[\,P', S'\,]\,]\,)$.

   Jika A=0, maka *return* N.

2. Jika $x = 0$

   Jika $B \neq 0$, maka

   $$x' = 1; \quad A' = 0; \quad B' = B^2;$$

$C = B;\ J = C^{-1};$

$P' = [(B')^2 + \mathrm{S} + 1]\mathrm{J};\ S' = B^4 + 1.$

Return ([[x', A', B'}] , [P', S']]) .

Jika $B = 0$, maka *return* N.

Algoritme Operasi Adisi

Dengan cara seperti pada formulasi operasi ganda, diperoleh formulasi operasi adisi untuk pembentukan algoritme operasi adisi, yang mana langkah-langkah penyusunan algoritmenya disesuaikan dengan urutan perhitungan formulasi operasi adisi yang telah dioptimumkan.

INPUT: $D_1 = [[\ x_1, A_1, B_1]\ , [\ P_1, S_1]]$ dan $D_2 = [[\ x_2, A_2, B_2]\ , [\ P_2, S_2]]$ sebagai representasi sembarang anggota **H.**

OUTPUT: $D_1 \boxplus D_2 = [\ [\ x, A, B]\ , [\ P, S]\ ]$ anggota **H**.

1. Jika $x_1 = x_2 = 1$, hitung

   $A' = A_1 + A_2; \qquad B' = B_1 + B_2;$

   a. Jika $A' \neq 0$, hitung

      $P' = P_1 + P_2; \qquad S' = S_1 + S_2;$

      $Q_1 = (A')^{-1}; \qquad U = B'Q_1; \quad U' = U^2; \qquad R = U' + A_2U + B_2;$

      Jika $R \neq 0$, hitung

      $C = RA'; \qquad J = C^{-1}; \qquad T = (Y_2 + A_2Y_3);$

      $Y_3 = S' + UP'; \qquad Y_2 = (U + A')Y_3 + RP';$

      $Y_1 = CP_2 + A_2T + B_2Y_3; \qquad Y_0 = CS_2 + B_2T.$

      Jika $Y_3 \neq 0$, maka:

      $x = 1; \quad K = {Y_3}^{-1}; \quad W = CK;$

      $A = A' + W^2; \quad B = B' + (A + A_1)A' + (A_1 + Y_2K) + W;$

      $T = AY_3 + Y_2;\ P = (AT + BY_3 + Y_1)J + 1;\ S = (BT + Y_0)J.$

      Return ([[x, A, B}] , [P, S]]) .

      Jika $Y_3 = 0$, maka

      $x = 0; \quad A = 1; \qquad P = 0; \quad B = A' + (Y_2J)^2;$

      $S = [(Y_2B + Y_1 + C)B + Y_0]J.$

      Return ([[x, A, B}] , [P, S]]) .

      Jika $R = 0$.

      Untuk kasus $U = 0$, hitung

      $x = 1; \qquad A = A'; \qquad B = A_1A_2;$

      $P = P_1 + P'A_2Q_1; \qquad S = S_2 + (P + P_2)A_2.$

      Return ([[x, A, B}] , [P, S]]) .

      Untuk kasus $U \neq 0$, hitung

      $B_1' = (U + A_1)(U + A_2); \qquad P_1' = P_1 + (P'A_2Q_1);$

      $T_0 = P_1U + S_1 \qquad Z = U^{-1}; \quad P_2' = \left({U'}^2 + T_0 + 1\right)Z;$

      $P_G = P_1' + P_2'; \qquad L = U + Q_1A_1A_2; \qquad U_L = L + U;$

      $C_1 = (Q_1A_1A_2)^2; \qquad C = A'C_1; \qquad J = C^{-1}.$

$Y_3 = U_L P_G + A_2(P_1' + P_2)$; $Y_2 = P_G C_2 + (A' + L)Y_3$;
$Y_1 = CP_2 + A_2 T + B_2 Y_3$; $Y_0 = C(UP_2' + T_0) + U'Y_2$.
Jika $Y_3 \neq 0$, maka:
$x = 1$; $K = Y_3^{-1}$; $W = CK$; $A = A' + W^2$;
$B = AA' + B_1' + W + (Y_2 K + U)^2$; $T = AY_3 + Y_2$;
$P = (AT + BY_3 + Y_1)J + 1$; $S = (BT + Y_0)J$.
Return ([[x, A, B}] , [P, S]]) .
Jika $Y_3 = 0$, maka
$x = 0$; $A = 1$; $P = 0$; $B = A' + (Y_2)^2$;
$S = [(Y_2 B + Y_1 + C)BY_0]J$.
Return ([[x, A, B}] , [P, S]]) .

b. Jika $A' = 0$ dan $B' \neq 0$, hitung
$C = B'$; $J = C^{-1}$; $S' = S_1 + S_2$;
$Y_3 = P_1 + P_2$; $Y_2 = A_1 Y_3 + S'$;
$Y_1 = S'A_1 + CP_2 + B_2 Y_3$; $Y_0 = B_1 S_2 + B_2 S_1$.
Jika $Y_3 \neq 0$, maka:
$x = 1$; $K = Y_3^{-1}$; $W = CK$; $A = W^2$;
$B = C + W + (Y_2 K + A_1)^2$; $T = AY_3 + Y_2$;
$P = (AT + BY_3 + Y_1)J + 1$; $S = (BT + Y_0)J$.
Return ([[x, A, B}] , [P, S]]) .
Jika $Y_3 = 0$, maka
$x = 0$; $A = 1$; $P = 0$; $B = (Y_2 J)^2 + \mathrm{Y_3 J}$;
$S = [(Y_2 B + Y_1 + C)B + Y_0]J$.
Return ([[x, A, B}] , [P, S]]) .

c. Jika $A' = 0$ dan $B' = 0$, hitung
$B_H = P_1 + P_2 + 1$.
Jika $B_H \neq 0$ maka $D = D_1 \boxplus D_1$, sehingga *Return* (D).
Jika $B_H = 0$ maka *Return* (N).

2. Jika $x_1 = 1$ dan $x_2 = 0$.
a. Jika $A_2 = 1$, hitung
$Q_0 = A_1 + B_2$; $R = B_2 Q_0 + B_1$.
Jika $R \neq 0$, hitung
$Y_2 = B_2 P_1 + S_1 + S_2$; $Y_1 = A_1 Y_2 + RP_1$; $Y_0 = B_1 Y_2 + RS_1$.
$x = 1$; $J = R^{-1}$; $A = Q_0 + (Y_2 J)^2$; $B = Q_0 A + B_2^2 + R + Y_2 J$.
Jika $Y_2 = 0$, maka
$P = Y_1 J + 1$; $S = Y_0 J$.
Return ([[x, A, B}] , [P, S]]) .
Jika $Y_2 \neq 0$, maka
$P = (AY_2 + Y_1)J + 1$; $S = (BY_2 + Y_0)J$.
Return ([[x, A, B}] , [P, S]]) .
Jika $R = 0$, hitung
$T = B_2$.
Jika $B_2 \neq 0$ dan $A_1 = 0$, maka

$Y_1 = (B_1^2 + S_2 + 1)J;$
$Y_2 = (Y_1^2 + Y_1 + 1)J;$
$Y_0 = (Y_2 B_2^2 + Y_1 B_2 + S_2);$
$x = 1; \quad A = Y_2^2 + B_2; \quad B = (B_2 Y_2 + 1)Y_2;$
$P = AY_2 + Y_1 + 1; \quad S = BY_2 + Y_0.$
Return ([[x, A, B}] , [P, S]]) .
Jika $B_2 \neq 0$ dan $A_1 \neq 0$, maka
$K_1 = B_1^2 + S_2 + 1; \quad K = K_1 J; \quad L = (K_1 B_2 + TS_2)J;$
$W = A_1^{-1}; \quad M = TA_1^2; \quad Z = M^{-1};$
$Y_1 = K_1 A_1^2; \quad Y_2 = K_1 A_1 + P_1 A_1 T; \quad Y_0 = (Y_2 B_2 + Y_1)B_2 + TA_1^2 S_2.$
Jika $Y_2 = 0$, maka
$x = 1; \quad A = Q_0; \quad B = AQ_0 + B_2^2;$
$P = Y_1 Z + 1; \quad S = Y_0 Z.$
Return ([[x, A, B}] , [P, S]]) .
Jika $Y_2 \neq 0$, maka
$x = 1; \quad A = Q_0 + (Y_2 J)^2 W; \quad B = Q_0 A + B_2^2 + Y_2 Z.$
$P = (AY_2 + Y_1)Z + 1; \quad S = (BY_2 + Y_0)Z.$
Return ([[x, A, B}] , [P, S]]) .

b. Jika $A_2 = 0$ maka $D_2 = N$, sehingga *return* (D_1).

3. Jika $A_1 = 1$ dan $A_2 = 1$, hitung
$A = (B_1 + B_2).$
a. Jika $(B_1 + B_2) \neq 0$, maka
$x = 1; \quad W = A_1^{-1}; \quad B = B_1 B_2;$
$P = (S_1 + S_2)W; \quad S = (S_1 B_2 + S_2 B_1)W.$
Return ([[x, A, B}] , [P, S]]) .
b. Jika $(B_1 + B_2) = 0$, maka
$B_H = P_1 + P_2 + 1.$
Jika $B_H \neq 0$, maka $D = D_1 \boxplus D_1$, sehingga *return* (D).
Jika $B_H = 0$ maka *return* (N).
4. Jika $A_1 = 1$ dan $A_2 = 0$, maka *return* (D_1).
5. Jika $A_2 = 1$ dan $A_1 = 0$ maka *return* (D_2).
6. Jika $A_1 = 0$ dan $A_2 = 0$ maka *return* (N).

5 SIMPULAN

Dari hasil eksplorasi diperoleh kurva $y^2 + xy = x^5 + x^2 + x$ merupakan kurva hipereliptik dengan genus dua yang terdefinisikan atas lapangan $\mathbb{F}_{2^{97}}$. Berdasarkan hasil analisis keamanan kurva, faktorisasi prima dari order #**H** dapat terbagi atas prima besar sehingga sistem kriptografi kurva hipereliptik $y^2 + xy = x^5 + x^2 + x$ atas lapangan $\mathbb{F}_{2^{97}}$ dapat bertahan dari serangan Poligh Helman dan karena faktorisasi prima besar dari #**H** adalah sebesar 53 digit maka dikategorikan

sebagai sistem kriptografi kurva hipereliptik yang aman dari serangan Polard Rho. Selanjutnya, prima besar dari faktorisasi #**H** tidak terbagi oleh $2^{97^{k-1}}$ untuk semua k, di mana masalah logaritma diskret didalam $\mathbb{F}_{2^{97^k}}$ ada jika $(1 \leq k \leq 2000/97)$ maka sistem kriptografi kurva hipereliptik dapat bertahan dari serangan Frey Ruck. Dari kurva diperoleh formulasi operasi grup yang efisien untuk menyusun suatu algoritme operasi grup.

DAFTAR PUSTAKA

[1] Cantor DG. 1987. Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation.* 48: 95-101.
[2] Diffie H, Hellman M. 1976. New direction in cryptography. *IEEE Transaction on Information Theory*. 22(6): 644-654.
[3] Estuningsih RD, Guritman S, Silalahi BP. 2014. Konstruksi Algoritme Fungsi Hash HLI [Tesis]. Bogor (ID): Institut Pertanian Bogor.
[4] Guritman S. 2016. *Kurva Eliptik dan Hipereliptik*. Bogor (ID):Institut Pertanian Bogor.
[5] Lange T. 2003. Efficient arithmetic on genus 2 hyperelliptic curve over finite fields via explicit formulae. *IACR Cryptology ePrint Archive* [Internet]. [diunduh 2016 Agustus 12]. *Tersedia pada: https://ePrint.iacr.org/2002/121.pdf*
[6] Koblitz N. 1987. Elliptic curve criptosystems. *Mathematics of Computation.* 48(177): 203-209.
[7] Koblitz N. 1989. Hyperelliptic curve criptosystems. *Mathematics of Computation.* 1(3): 139-150.
[8] Menezes AJ, Yi-Hong W, Zuccherato RJ. 1996. *An Elementary Introduction to Hyperelliptic Curve*. Ontario (CA): Univ Waterloo.
[9] Menezes, Oorcshot, dan Vanstone. 1996. *Handbook of Applied Cryptoography*. Florida: CRC Press.
[10] [NIST] National Institute for Standar and Technology. 2007. Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. *NIST SP 800-56A*. Marryland(US):NIST.
[11] Vijayakumar P, Vijayalakshmi V, Zayaraz G. 2014. Comparative study of hyperelliptic curve cryptosystem over prime field and its survey. *International Journal of Hybrid Information Technology*. 7: 137-146.