Pengembangan Kriptografi Kurva Eliptik dengan Kurva Eliptik Tiga Dimensi

Marcelinus Henry M.
Teknik Informatika
Institut Teknologi Bandung
Bandung, Indonesia
henrymenori@yahoo.com

***Abstrak*—Makalah ini mengandung dasar teori dan konsep-konsep yang dipakai untuk mengembangkan kurva eliptik tiga dimensi, serta cara pemakaiannya dalam algoritma kriptografi kunci public saat ini.**

Keywords—kurva eliptik; tiga dimensi; proyeksi; kriptografi kunci publik

I. PENDAHULUAN

Pada zaman ini, hampir semua hal berhubungan dengan internet. Informasi yang tersedia sangat banyak dan bisa diakses semua orang. Tetapi, diantara informasi-informasi tersebut, ada yang sifatnya rahasia dimana hanya orang-orang tertentu yang boleh mengetahuinya. Informasi rahasia tersebut kadang diambil oleh orang lain untuk kepentingannya sendiri yang mungkin akan membahayakan si pemilik informasi. Maka dari itu, dibentuklah algoritma kriptografi dengan menggunakan kurva eliptik agar lebih aman informasi tersebut sampai di tangan penerima. Namun sampai di mana tingkat keamanannya?

Pada makalah ini akan dibahas mengenai kurva eliptik yang digunakan dalam kriptografi dengan sedikit pengubahan agar meningkatkan keamanannya. Pengubahan ini terlihat dari dimensi kurva eliptik yang ada. Makalah ini juga akan membahas metodanya, cara pemakaian, dan analisis keamanan dibanding kurva eliptik dua dimensi.

II. DASAR TEORI

A. Grup

Grup adalah sistem aljabar yang terdiri dari sebuah himpunan *G* dan sebuah operasi biner * sedemikian sehingga untuk semua elemen *a*, *b*, dan *c* di dalam *G* berlaku aksioma berikut

- Closure

  $a * b$ harus berada di dalam *G*
- Asosiatif

  $a*(b*c) = (a*b)*c$
- Elemen netral

  Terdapat $e \in G$ sedemikian sehingga $a*e = e*a = a$
- Elemen invers

  Terdapat $a' \in G$ sedemikian sehingga $a'*a = a*a' = e$

Sebuah grup <*G*, *> dikatakan grup komutatif atau grup abelian jika berlaku aksioma komutatif untuk semua nilai pada grup *G*.

B. Medan (field)

Medan (field) adalah himpunan elemen *F* dengan dua operasi biner, biasanya disebut penjumlahan (+) dan perkalian (x). Sebuah struktur aljabar <*F*, +, x> disebut medan jika dan hanya jika

- <*F*, +> adalah grup abelian
- <*F* – {0}, x> adalah grup abelian
- Operasi x menyebar terhadap operasi + (distributif)

Medan berhingga sering dinamakan *Galois Field*, dimana himpunannya memiliki jumlah elemen yang berhingga.

C. Kurva Eliptik

Kurva eliptik adalah kurva dengan bentuk umum persamaan

$$y^2 = x^3 + ax + b$$

Dimana

$$4a^3 + 27b^2 \neq 0$$

Penjumlahan titik pada kurva eliptik

$$\lambda = \frac{y_p - y_q}{x_p - x_q}$$

$$x_r = \lambda^2 - x_p - x_q$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Penggandaan titik pada kurva eliptik

$$\lambda = \frac{dy}{dx} = \frac{3x_p^2 + a}{2y_p}$$

$$x_r = \lambda^2 - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

III. PENGEMBANGAN KURVA ELIPTIK TIGA DIMENSI

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Penurunan rumus

- Persamaan umum

  Persamaan untuk kurva eliptik dalam bentuk tiga dimensi sangat sulit untuk didapatkan. Maka dari itu, kurva eliptik yang digunakan tetap dalam bentuk dua dimensi dengan melakukan proyeksi titik tiga dimensi menjadi dua dimensi. Dalam metode ini, penulis menggunakan Jacobian Projection untuk mengubah titik tiga dimensi menjadi dua dimensi.

  Misalkan sebuah titik $A(x_A, y_A, z_A)$ akan diproyeksikan menjadi titik $P(x_P, y_P)$. Dengan metode Jacobian Projection, titik tersebut akan diproyeksikan sebagai berikut

$$x_P = \frac{x_A}{(z_A)^m}$$

$$y_P = \frac{y_A}{(z_A)^n}$$

  Dimana nilai *m* dan *n* relatif prima, disesuaikan dengan kurva yang akan digunakan. Karena kurva yang akan digunakan adalah kurva eliptik, maka dicari nilai *m* dan *n* yang cocok untuk kurva eliptik tersebut. Berikut penurunan untuk mencari nilai *m* dan *n* yang cocok

$$y_P^2 = x_P^3 + ax_P + b$$

$$\left(\frac{y_A}{z_A^n}\right)^2 = \left(\frac{x_A}{z_A^m}\right)^3 + a\left(\frac{x_A}{z_A^m}\right) + b$$

$$\left(\frac{z_A^{3m}}{z_A^{2n}}\right) y_A^2 = x_A^3 + ax_A z_A^{2m} + bz_A^{3m}$$

  Agar persamaan di atas menjadi persamaan yang normal dan nilai *m* dan *n* relatif prima, maka solusi yang tepat yaitu *m* = 2 dan *n* = 3, sehingga persamaannya menjadi

$$y_A^2 = x_A^3 + ax_A z_A^4 + bz_A^6$$

  Atau lebih umumnya

$$y^2 = x^3 + axz^4 + bz^6$$

- Penjumlahan titik

  Karena adanya dimensi ketiga yaitu *z*, maka penjumlahan titik yang pada awalnya hanya melibatkan *x* dan *y*, kini harus diturunkan kembali agar sesuai dengan titik tiga dimensi yang didefinisikan.

  Misalkan untuk penjumlahan titik $A(x_1, y_1, z_1) + B(x_2, y_2, z_2) = C(x_3, y_3, z_3)$ atau dalam proyeksi dua dimensinya yaitu $p(x_p, y_p) + q(x_q, y_q) = r(x_r, y_r)$. Pertama, gradien λ dihitung diturunkan dari rumus umumnya sebagai berikut

$$\lambda = \frac{y_p - y_q}{x_p - x_q}$$

$$= \frac{\frac{y_1}{z_1^3} - \frac{y_2}{z_2^3}}{\frac{x_1}{z_1^2} - \frac{x_2}{z_2^2}}$$

$$= \left(\frac{y_1 z_2^3 - y_2 z_1^3}{x_1 z_2^2 - x_2 z_1^2}\right)\left(\frac{1}{z_1 z_2}\right)$$

  Kemudian dimisalkan

$$\alpha = \left(\frac{y_1 z_2^3 - y_2 z_1^3}{x_1 z_2^2 - x_2 z_1^2}\right)$$

  Sehingga gradien λ menjadi

$$\lambda = \frac{\alpha}{z_1 z_2}$$

  Selanjutnya, dari nilai gradien yang sudah didapat, dilakukan perhitungan untuk nilai *x* dan *y* pada titik *r* atau titik hasil. Berikut proses penurunan rumus untuk nilai *x* dan *y* pada titik *r* dari rumus umum kurva eliptik dua dimensi.

$$x_r = \lambda^2 - x_p - x_q$$

$$= \left(\frac{\alpha}{z_1 z_2}\right)^2 - \frac{x_1}{z_1^2} - \frac{x_2}{z_2^2}$$

$$= \frac{\alpha^2 - x_1 z_2^2 - x_2 z_1^2}{(z_1 z_2)^2}$$

$$
\begin{aligned}
y_r &= \lambda\left(x_p - x_r\right) - y_p \\
&= \left(\frac{\alpha}{z_1 z_2}\right)\left(\frac{x_1}{z_1^2} - \frac{\alpha^2 - x_1 z_2^2 - x_2 z_1^2}{\left(z_1 z_2\right)^2}\right) - \frac{y_1}{z_1^3} \\
&= \left(\frac{\alpha}{z_1 z_2}\right)\left(\frac{-\alpha^2 + 2x_1 z_2^2 + x_2 z_1^2}{\left(z_1 z_2\right)^2}\right) - \frac{y_1}{z_1^3} \\
&= \frac{\alpha\left(-\alpha^2 + 2x_1 z_2^2 + x_2 z_1^2\right)}{\left(z_1 z_2\right)^3} - \frac{y_1}{z_1^3} \\
&= \frac{\alpha\left(-\alpha^2 + 2x_1 z_2^2 + x_2 z_1^2\right) - y_1 z_2^3}{\left(z_1 z_2\right)^3}
\end{aligned}
$$

Sesudah mendapatkan titik hasil *r* yang merupakan proyeksi dua dimensi dari titik *C*, saatnya mengubah nilai *x* dan *y* pada titik *r* menjadi *x*, *y*, *z* pada titik *C*. Pengubahan ini terlihat jelas dari pembagi *x* ataupun *y* yang sudah berbentuk sama seperti Jacobian Projection. Pengubahan dapat dilakukan sebagai berikut.

$$x_3 = \alpha^2 - x_1 z_2^2 - x_2 z_1^2$$

$$y_3 = \alpha(-\alpha^2 + 2x_1 z_2^2 + x_2 z_1^2) - y_1 z_2^3$$

$$z_3 = z_1 z_2$$

- Penggandaan titik

Penggandaan titik juga tak luput dari transformasi akibat dari proyeksi ini.

Misalkan untuk penggandaan titik $2 \times A(x_1, y_1, z_1) = B(x_2, y_2, z_2)$ atau dalam proyeksi dua dimensinya yaitu $2 \times p(x_p, y_p) = r(x_r, y_r)$, dilakukan transformasi sebagai berikut.

$$
\begin{aligned}
\lambda &= \frac{3x_p^2 + a}{2y_p} \\
&= \frac{3\left(\frac{x_1}{z_1^2}\right)^2 + az_1^4}{2\left(\frac{y_1}{z_1^3}\right)} \\
&= \frac{3x_1^2 + az_1^8}{2y_1 z_1}
\end{aligned}
$$

Kemudian dimisalkan

$$\alpha = \frac{3x_1^2 + az_1^8}{2y_1}$$

Sehingga gradien λ menjadi

$$\lambda = \frac{\alpha}{z_1}$$

Selanjutnya penurunan rumus untuk mendapatkan nilai *x* dan *y* pada titik *r* atau titik hasil dengan rumus umum kurva eliptik yang sudah ada.

$$
\begin{aligned}
x_r &= \lambda^2 - 2x_p \\
&= \left(\frac{\alpha}{z_1}\right)^2 - 2\left(\frac{x_1}{z_1^2}\right) \\
&= \frac{\alpha^2 - 2x_1}{z_1^2}
\end{aligned}
$$

$$
\begin{aligned}
y_r &= \lambda(x_p - x_r) - y_p \\
&= \left(\frac{\alpha}{z_1}\right)\left(\frac{x_1}{z_1^2} - \frac{\alpha^2 - 2x_1}{z_1^2}\right) - \frac{y_1}{z_1^3} \\
&= \left(\frac{\alpha}{z_1}\right)\left(\frac{-\alpha^2 + 3x_1}{z_1^2}\right) - \frac{y_1}{z_1^3} \\
&= \frac{\alpha\left(-\alpha^2 + 3x_1\right) - y_1}{z_1^3}
\end{aligned}
$$

Terakhir, mengubah titik *r* menjadi titik *B* dengan Jacobian Projection

$$x_2 = \alpha^2 - 2x_1$$

$$y_2 = \alpha(-\alpha + 3x_1) - y_1$$

$$z_2 = z_1$$

B. Cara penggunaan

Dua pihak yang berkomunikasi menyepakati parameter data sebagai berikut

- Persamaan kurva eliptik yang akan digunakan $y^2 = x^3 + axz^4 + bz^6 \bmod p$, dengan nilai *a*, *b*, dan *p* yang sudah ditentukan pula. Bilangan prima *p* yang akan dipilih sebaiknya cukup besar agar keamanannya terjamin
- Grup eliptik yang dihitung dari persamaan kurva eliptik. Persamaan kurva eliptik yang digunakan untuk menghitung grup eliptik ini dibebaskan di salah satu nilai *z*, namun disarankan untuk menggunakan nilai *z* tidak sama dengan satu untuk meningkatkan keamanannya.
- Titik basis $B(x_B, y_B, z_B)$ yang dipilih dari grup eliptik untuk operasi kriptografi.

Setiap pengguna juga membangkitkan pasangan kunci publik dan kunci privat, yang cara menggunakannya bergantung pada algoritma yang digunakan. Kunci privat adalah sebuah bilangan integer yang dipilih dari selang [1, *p*-1]. Kunci publik adalah sebuah titik tiga dimensi yang merupakan hasil kali antara kunci privat dan titik basis.

Pada umumnya, cara penggunaan kurva eliptik tiga dimensi ini tidak berbeda jauh dengan kurva eliptik dua dimensi. Disini hanya diperjelas tentang rumus untuk operasi-operasi yang terkait pada kurva tersebut.

- Penjumlahan titik

  Untuk penjumlahan titik $A(x_1, y_1, z_1) + B(x_2, y_2, z_2) = C(x_3, y_3, z_3)$ atau dalam proyeksi dua dimensinya yaitu $p(x_p, y_p) + q(x_q, y_q) = r(x_r, y_r)$, dapat dilakukan langkah-langkah sebagai berikut

  1) Hitung nilai *E*, *F*, *G*, *H* dengan rumus berikut

$$E = x_1 z_2^2$$

$$F = x_2 z_1^2$$

$$G = y_1 z_2^3$$

$$H = y_2 z_1^3$$

  2) Hitung nilai α dengan rumus

$$\alpha = \frac{G - H}{E - F} \bmod p$$

  3) Hitung nilai x_3 dengan rumus

$$x_3 = \alpha^2 - E - F \bmod p$$

  4) Hitung nilai y_3 dengan rumus

$$y_3 = \alpha(-\alpha^2 + 2E + F) - G \bmod p$$

  5) Hitung nilai z_3 dengan rumus

$$z_3 = z_1 z_2 \bmod p$$

- Penggandaan titik

  Untuk penggandaan titik $2 \times A(x_1, y_1, z_1) = B(x_2, y_2, z_2)$ atau dalam proyeksi dua dimensinya yaitu $2 \times p(x_p, y_p) = r(x_r, y_r)$, dapat dilakukan langkah sebagai berikut

  1) Hitung nilai α dengan rumus

$$\alpha = \frac{3x_1^2 + az_1^8}{2y_1} \bmod p$$

  2) Hitung nilai x_2 dengan rumus

$$x_2 = \alpha^2 - 2x_1 \bmod p$$

  3) Hitung nilai y_2 dengan rumus

$$y_2 = \alpha(-\alpha + 3x_1) - y_1 \bmod p$$

  4) Nilai $z_2 = z_1$

C. Beberapa metode kriptogafi dengan kurva eliptik tiga dimensi

Kurva eliptik tiga dimensi dapat diaplikasikan seperti kurva eliptik dua dimensi dalam kriptografi. Algoritma kriptografi seperti Elliptic Curve Diffie-Hellman, Elliptic Curve El Gamal, dan Elliptic Curve Digital Signature bisa menggunakan kurva eliptik tiga dimensi untuk meningkatkan keamanannya. Akan tetapi, penggunaan kurva eliptik tiga dimensi masih belum bisa dimaksimalkan apabila tidak terjadi penyesuaian terhadap algoritma kriptografi yang dipakai, dimana elemen z sangat berperan untuk meningkatkan keamanan dari suatu algoritma.

IV. ANALISIS

Keamanan kurva eliptik terletak pada sulitnya mencari nilai *k* dimana $Q = kP$, *Q* dan *P* adalah anggota kumpulan titik pada kurva eliptik. Nilai k yang besar membuat komputasi perkalian titik menjadi mudah apabila *k* diketahui, namun menjadi sangat sulit apabila nilai *k* yang harus dicari. Pencarian nilai *k* dengan menggunakan *brute force* akan memakan waktu yang cukup lama karena besarnya nilai *k* yang harus dicari.

Keamanan kurva eliptik tiga dimensi terletak pada nilai dimensi baru yaitu *z*. Misalkan untuk kurva eliptik yang memiliki nilai orde *n* dan bilangan prima *p*, apabila dengan kurva dua dimensi akan memiliki kemungkinan titik sejumlah orde. Namun, dengan kurva eliptik tiga dimensi, kemungkinan titik menjadi sejumlah orde untuk setiap $z < p$, sehingga total kemungkinannya adalah $n(p\text{-}2)$ kemungkinan. Dengan kemungkinan sebanyak itu, akan mempersulit orang untuk menemukan kunci privat.

Keamanan kurva eliptik tiga dimensi bisa ditingkatkan lagi dengan mengubah algoritma enkripsi yang ada agar dimensi *z* bisa ditingkatkan lagi pemakaiannya sehingga kurva eliptik tiga dimensi bisa menjadi lebih aman lagi. Adapun penambahan dimensi *z* menambah variasi titik menjadi lebih banyak, sehingga bisa membingungkan orang dalam memecahkan kunci privat tersebut.

V. KESIMPULAN

Kurva eliptik tiga dimensi dapat dibilang lebih aman dibandingkan dengan kurva eliptik dua dimensi dari segi usaha yang dilakukan untuk menemukan bilangan pengali yang tepat karena kemungkinan titik yang bertambah dari kurva eliptik dua dimensi menjadi kurva eliptik tiga dimensi.

REFERENSI

[1] Andreas Steffen, Elliptic Curve Cryptography, Zurcher Hochschule Winterthur.

[2] Debdeep Mukhopadhyay, Elliptic Curve Cryptography, Dept of Computer Sc and Engg IIT

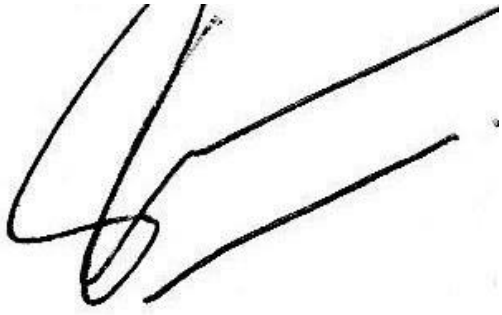
[3] Anoop MS , Elliptic Curve Cryptography, an Implementation Guide

[4] http://www.ideskripsi.com/2014/03/skripsi-implementasi-kriptografi-kurva.html waktu akses 9 Mei 2015 20:00

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah otang lain, dan bukan plagiasi.

Bandung, 10 Mei 2015



Marcelinus Henry M.