Hyper Elliptic Curve Cryptography for e-Commerce Channel

Sonny Theo Tumbur | 13510027[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510027@std.stei.itb.ac.id

***Abstract*—Dengan berkembangnya penggunaan perangkat *mobile* untuk melakukan transaksi secara elektronik, dibutuhkan suatu terobosan baru dalam hal pengamanan transaksi elektronik. Karateristik transaksi yang membutuhkan properti privasi, otentikasi, dll dan karakteristik perangkat *mobile* yang memiliki sumber daya terbatas membawa penulis kepada suatu pendekatan lain, yaitu kriptografi *hyperelliptic curve*. Kriptografi ini memiliki tingkat keamanan yang setara dengan algoritma kunci publik lain yang telah muncul sebelumnya seperti RSA dan *elliptic curve*. Hanya saja, hyperelliptic curve memiliki kelebihan dari sisi kompleksitas komputasinya yang lebih efisien membuat kriptografi ini lebih cocok digunakan untuk bertransaksi menggunakan perangkat *mobile*.**

***Index Terms*—*hyperelliptic curve*, kriptografi kunci publik, *digital envelope*, *e-commerce*, perangkat *mobile*.**

I. PENDAHULUAN

Perdagangan eletronik (*e-commerce*) telah menjadi suatu kecenderungan (*trend*) tertentu dewasa ini. Berbagai penjangkauan dan penawaran terhadap pasar telah dilakukan melalui berbagai jenis media seperti sosial media, situs *e-commerce*, dan lain sebagainya. Terkait dengan semakin banyaknya transaksi yang dilakukan baik yang dilakukan dalam lingkungan pendidikan, maupun bisnis, seluruhnya membutuhkan tingkat keamanan tertentu yang spesifik.

Secara umum transaksi elektronik membutuhkan karakteristik keamanan sebagai berikut.

- privasi,
- otentikasi,
- integritas data dan transaksi,
- anti penyangkalan (akuntabilitas).

Pada dasarnya, keempat atribut ini dapat dicapai dengan menerapkan teknik kriptografis yang tepat sasaran. Penggunaan algoritma RSA dan Elliptic Curve yang telah digunakan selama ini sedikit banyak telah menjadi solusi untuk beberapa jenis permasalahan tertentu.

Penggunaan perangkat mobile phone yang semakin marak digunakan dalam masyarakat sekarang ini juga sedikit banyak membawa perubahan terhadap cara pengembang (*developer*) melakukan pendekatan terhadap masalah. Dewasa ini, banyak sekali transaksi yang dilakukan melalui media *mobile* ini. Berbagai aplikasi *native* yang khusus menangani transaksi elektronik pun mulai bermunculan dan berkembang terus menerus. Dalam kasus mobile phone, diperlukan suatu sistem yang dapat menyelesaikan masalah dengan tingkat keamanan yang paling tidak sama kuat tetapi dengan menggunakan *resource* yang lebih efisien, terkait dengan terbatasnya sumber daya yang dimiliki oleh perangkat *mobile*.

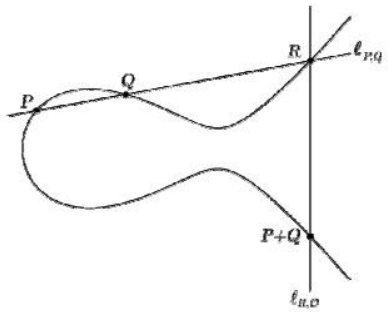
II. DIGITAL ENVELOPE

Digital Envelope (DE) merupakan suatu kerangka kerja (*framework*) yang dikenalkan oleh RSA Laboratories yang menangani permasalahan pertukaran kunci pada *secret-key cryptosystem*. Komponen dalam DE mencakup pesan yang dienkripsi dengan menggunakan kriptografi kunci privat dan kunci rahasia yang dienkripsi menggunakan kriptografi kunci publik.

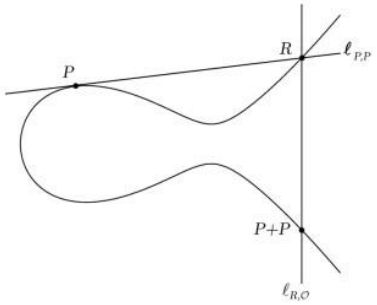
Misalkan Alice akan mengirimkan pesan kepada Bob menggunakan kriptografi kunci privat untuk isi dari pesan sedangkan kriptografi kunci publik untuk kunci rahasia kriptografi kunci privat yang sebelumnya dilakukan. Alice terlebih dahulu menentukan kunci rahasia yang akan digunakan dan melakukan enkripsi terhadap pesan yang akan dikirim menggunakan kunci rahasia tersebut, lalu mengenkripsi kunci rahasia tersebut dengan kunci publik milik Bob. Setelah itu, ketika menerima pesan terenkripsi tersebut, Bob terlebih dulu akan melakukan dekripsi terhadap kunci rahasia menggunakan kunci privat milik Bob sendiri. Setelah Bob mendapatkan kunci rahasia tersebut barulah Bob dapat melakukan dekripsi untuk mendapatkan isi pesan yang sesungguhnya.

III. ELLIPTIC CURVE (EC)

Elliptic Curve Cryptography (ECC) merupakan salah satu algoritma kriptografi kunci publik yang ditemukan sekitar delapan tahun setelah algoritma RSA ditemukan. Algoritma ECC ini banyak digunakan pada berbagai bidang mulai dari teori bilangan hingga fisika matematika. Istilah '*elliptic'* pada EC tidak berhubungan dengan bentuk geometri oval. Begitu juga dengan istilah '*curve'* yang tidak sepenuhnya berkaitan dengan garis lengkung. EC merupakan kumpulan nilai yang membentuk suatu grup (*group*). Gambar 1 dan gambar 2 memberikan ilustrasi untuk aturan *chord-and-tangent* dalam *elliptic curve*.



Gambar 1 Chord Rule on Elliptic Curve



Gambar 2 Tangent Rule on Elliptic Curve

Operasi-operasi yang ada pada kriptografi ini menggunakan aritmetika modulo dengan bilangan prima sebagai elemen utamanya. Operasi-operasi yang ada juga menggunakan bilangan bulat dengan lingkup berhingga (*finite field*) yang umumnya diberi notasi F_p. Alasan digunakannya bilangan prima dalam kriptografi ini kurang lebih serupa dengan digunakannya bilangan prima pada kriptografi lain, seperti RSA, yaitu karena untuk menentukan faktor prima sebuah bilangan yang sangat besar, dibutuhkan waktu dan *resource* yang sangat besar pula. Besarnya usaha yang dibutuhkan untuk menentukan faktor prima dari bilangan yang amat besar inilah yang menjadi kekuatan utama dari kriptografi ini. Satu hal yang penting adalah bahwa bilangan-bilangan yang digunakan pada kriptografi ini bukan merupakan bilangan *integer* standar dengan panjang 32 atau 64 bit, melainkan *big integer* dengan panjang hingga lebih dari 200 bit. Operasi-operasi yang dapat diterapkan pada bilangan-bilangan dalam kriptografi ini antara lain operasi penambahan (*addition*), pengurangan (*substraction*), perkalian (*multiplication*), pembagian (*division*), perpangkatan (*exponentiation*), dan pengakaran (*square root*).

Berikut ini merupakan persamaan umum dari EC:

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

yang mana a dan b merupakan koefisien yang menjadi penentu karakteristik dari kurva yang terbentuk. Kedua koefisien tersebut juga harus memenuhi persamaan berikut ini.

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

Dengan pemenuhan terhadap persamaan di atas, dapat dipastikan kurva yang dihasilkan tidak mengandung singularitas (*singularities*).

IV. HYPER ELLIPTIC CURVE

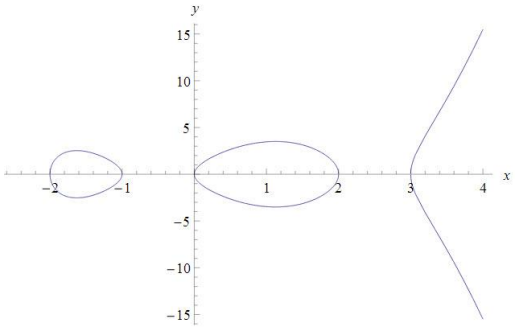
Dalam aljabar geometri, *hyperelliptic curve* merupakan kurva aljabar dengan bentuk persamaan sebagai berikut.

$$y^2 = f(x),$$

yang mana $f(x)$ merupakan fungsi polinom dengan derajat n lebih dari 4. Gambar 3 menunjukan contoh kurva hyperelliptic dengan dengan persamaan sebagai berikut.

$$f(x) = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x.$$

Pangkat dari persamaan polynomial pada ruas kanan menentukan genus dari hasil kurva yang terbentuk. Polinom dengan derajat $2g + 1$ akan membentuk kurva yang dinamakan *imaginary hyperelliptic curve*, sedangkan polinom dengan derajat $2g + 2$ akan membentuk kurva yang dinamakan *real hyperelliptic curve*.



Gambar 3 Hyperelliptic Curve

Tidak seperti pada *elliptic curve*, titik-titik pada *hyperelliptic curve* tidak membentuk suatu *group* g. Secara formal, dasar dari kriptografi hyperelliptic curve dijelaskan sebagai berikut. Misalkan F_q adalah suatu medan berhingga dengan q elemen. Diberikan 2 pembagi (*divisor*) dalam Jacobian, D_1 dan D_2, tentukan $m \in Z$ sedemikian hingga terpenuhi persamaan berikut.

$$D_2 = mD_1.$$

Jacobian dari suatu *hyperelliptic curve* C adalah suatu grup $J = D^0/P$, yang mana D^0 merupakan himpunan pembagi (*divisor*) berderajat nol, sedangkan P adalah himpunan pembagi dari fungsi rasional.

V. ANALISIS

Berikut adalah salah satu skema algoritma kriptografi kunci publik dan pembangkitan kunci. Misalkan ditentukan parameter yang bersifat publik adalah kurva eliptik C, suatu bilangan prima p, dan pembagi D. Untuk menghasilkan kunci publik P_A dan kunci privat a_A, digunakan skema berikut[1].

1. $a_A \in N$
2. $P_A \leftarrow [a_A]D$

3. Hasilkan nilai P_A dan a_A

Untuk pembangkitan bilangan acak pada tahapan nomor (1), ada beberapa uji bilangan prima yang dapat diterapkan seperti uji Rabin-Miller, maupun AKS; namun, penelitian telah membuktikan bahwa dibutuhkan waktu eksponensial untuk menentukan keprimaan suatu bilangan, khususnya pada bilangan besar.

Berikut ini adalah contoh metodologi yang dapat digunakan untuk melakukan enkripsi dan dekripsi. Misalkan suatu pesan m telah di-*encode* menjadi sekumpulan titik yang diacu sebagai E_m. Langkah-langkah yang dilakukan oleh pengirim pesan mencakup

1. Memilih nilai k sebagai bilangan positif prima sembarang.
2. $Q \leftarrow [k]D$ (D merupakan *divisor* dari *hyperelliptic curve*)
3. $P_k \leftarrow [k]P_B$ (P_B merupakan kunci publik penerima pesan)
4. $C_m \leftarrow \{Q, E_m + P_k\}$ (C adalah cipherteks yang akan dikirimkan)

Untuk melakukan dekripsi, penerima pesan menerapkan operasi seperti berikut

$$\begin{aligned} E_m + kP_B - a_B(Q) &= E_m + kP_B - a_B(kD) \\ &= E_m + kP_B - k(a_B D) \\ &= E_m + kP_B - kP_B = E_m \end{aligned}$$

VI. KESIMPULAN

Berdasarkan pemaparan sebelumnya, dapat disimpulkan bahwa kriptografi *hyperelliptic curve* dapat digunakan dengan tingkat keamanan yang serupa dengan *elliptic curve*. Kriptografi *hyperelliptic curve* ini juga memiliki tingkat efisiensi komputasi yang relatif tinggi, memerlukan kunci yang relatif lebih pendek. Model ini akan cocok digunakan untuk environment yang terbatas baik dari segi kompleksitas komputasi maupun *resource*, seperti perangkat *mobile*.

REFERENCES

[1] http://www.emc.com. RSA Laboratories. May, 19th, 2014.

[2] R, Ganesan, Vivekanandan. 2009. *A Novel Hybrid Security Model for E-Commerce Channel*. Coimbatore.

[3] Scholten, Jasper, Vercouteren. *An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem*. Belgium.

PERNYATAAN

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

Bandung, 19 Mei 2014

ttd

Sonny Theo Tumbur
13510027