Model Pengamanan *End-to-End* pada *M-Banking* Berbasis Algoritma Kurva *Hyper Elliptic*

Putra Wanda
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Respati Yogyakarta
Jl. Laksda Adisucipto, KM.6.5, Depok, Sleman, Yogyakarta
E-mail: wpwawan@gmail.com

Masuk: 20 Januari 2016; Direvisi: 2 Februari 2016; Diterima: 2 Februari 2016

Abstract. *Currently, banking transactions using mobile banking has grown rapidly. The increasing the number of mobile application users becomes one of the main factors. Several approaches have been developed to improve the transaction security. Problems of message security still requires a solution to achieve computing speed and leverage security level. In this paper, we propose a security algorithms used to improve the mobile banking security with hyperelliptic curve algorithm. It will create a safe and an efficient transactions while message will be sent via public internet. Hyperelliptic curve algorithm will run a processes for authentication and encryption. it will produce fast computation and has good security level. This research produced little computing time on m-banking application while it run on Android. Hyperelliptic curve algorithm use a smaller key to achieve a good security level at m-banking application.*
Keywords: *hyperelliptic curve algorithm, security, mobile banking.*

Abstrak. *Saat ini, transaksi perbankan baik di dalam dan di luar menggunakan Mobile Banking semakin pesat, meningkatnya jumlah pengguna aplikasi mobile menjadi salah satu faktor utamanya. Beberapa pendekatan telah dikembangkan untuk meningkatkan keamanan transaksi pesan selama komunikasi. Masalah yang masih memerlukan solusi adalah kecepatan komputasi dan tingkat keamanan pada algoritma pengamanan yang digunakan. Penelitian ini dilakukan untuk meningkatkan keamanan pesan mobile banking dengan memanfaatkan algoritma kurva hyper elliptic. Hal ini dilakukan untuk mewujudkan transaksi yang aman dan efisien dengan penerapan metode kriptografi pada pesan. Dengan menggunakan algoritma kurva hyper elliptic maka proses autentikasi dan enkripsi pesan bisa dilakukan dengan cepat dan memiliki level keamanan yang tinggi. Penelitian ini menghasilkan waktu komputasi yang cukup cepat pada aplikasi m-banking berbasis Android. Hal ini karena, algoritma kurva hyper elliptic menggunakan panjang kunci yang lebih kecil untuk mencapai level keamanan yang baik pada aplikasi m-banking.*
Kata Kunci: *algoritma kurva hyper elliptic, keamanan, mobile banking.*

1. Pendahuluan

Saat ini penggunaan transaksi perbankan sudah banyak digunakan pada aplikasi *mobile* (Kumar, dkk., 2013). Aspek keamanan pada sistem operasi *mobile* seperti Android masih banyak ditemukan, terutama dengan munculnya berbagai serangan berupa virus dan *malware* terhadap sistem operasi Android (Faruki, dkk., 2015). Saat ini hampir 62% bank di seluruh dunia telah menerapkan *mobile banking (m-banking)* dalam layanannya kepada pelanggan. Tetapi, sejumlah 72% bank yang menerapkan layanan *m-banking* masih khawatir dengan aspek keamanan dari layanan yang diberikan tersebut. Hal ini tentu memerlukan solusi dari aspek penerapan teknologi yang akan digunakan pada layanan *m-banking* tersebut (Vasco, 2009). Selain itu juga, prospek perkembangan *m-banking* akan semakin pesat. Hal ini bisa terlihat pada pesatnya penggunaan aplikasi *m-banking* di China (To & Lai, 2014). Bahaya keamanan layanan *m-banking* ini banyak berasal dari aspek non teknis. Misalnya, bahaya dari penggunaan *m-banking* bisa terjadi ketika ada pihak ketiga mengetahui nomor PIN dari seorang pengguna *m-*

banking. Sebuah autentikasi dengan beberapa teknik misalnya *neural network* juga diperlukan (Ku, 2005). Dalam perkembangannya, penggunaan autentikasi dengan *password* yang pendek akan menjadi sangat riskan (Ren, dkk., 2009). Teknik autentikasi untuk melakukan autentikasi pada *user* juga bisa dilakukan melalui metode pembangkitan kunci autentikasi. Untuk mengatasi kelemahan dengan teknik *password*, skema autentikasi misalnya dengan teknik *group authentication* telah dikembangkan (Ham, 2013).

Motivasi pengguna dalam menggunakan layanan *m-banking* bisa dikatakan baik. Apalagi dengan dukungan berbagai fitur dalam *m-banking* yang memberikan manfaat, kemudahan dalam penggunaan, dan kualitas layanan yang baik membuat layanan transaksi berbasis *mobile* ini semakin diminati oleh berbagai kalangan pengguna (Shih & Lin, 2015).

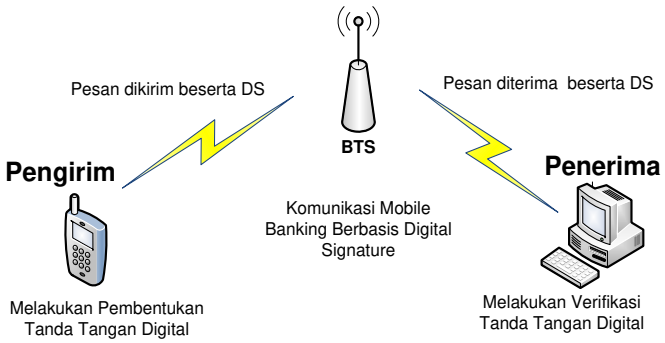
Kurva *hyper elliptic* adalah kelas khusus dari sebuah kurva aljabar dan dapat dinyatakan sebagai generalisasi dari sebuah kurva eliptik. Algoritma kurva *hyper elliptic* ini menggunakan genus dengan ukuran yang kecil pada proses komputasi sehingga menghasilkan ukuran kunci yang lebih pendek dibandingkan dengan algoritma sejenis seperti RSA (Menezes & Zuccherato, 1996: 35).

2. Tinjauan Pustaka

2.1. Penelitian Terdahulu

Di Indonesia, penelitian yang telah dilakukan dalam membangun sistem keamanan *m-banking* adalah dengan menerapkan tanda tangan digital (*Digital Signature*) berbasis SHA (*Secure Hash Algorithm*). *Digital Signature* (DS) akan digunakan untuk memeriksa validitas pesan yang dikirim melalui jaringan publik pada komunikasi SMS *banking*. Skema komunikasi *m-banking* dengan menggunakan teknik pengamanan tanda tangan digital dapat diilustrasikan pada Gambar 1.

Dari analisis yang didapatkan, penelitian ini menyimpulkan bahwa pemberian tanda tangan digital terhadap sebuah pesan dapat dilakukan terhadap pesan SMS melalui perangkat bergerak. Untuk itu, model ini memungkinkan untuk dapat diterapkan dalam proses transaksi SMS *banking* dimana sistem keamanan SMS *banking* saat ini masih mempunyai kekurangan dalam keamanan di level non teknis (Budiono, 2013).



Gambar 1. Model Komunikasi SMS *Banking* dengan SHA

Penelitian lain juga telah diajukan untuk meningkatkan keamanan transaksi *internet banking*. Penelitian ini mengajukan metode pengamanan *internet banking* berbasis multi biometrik. Metode multi biometrik yang diajukan berupa kombinasi pengamanan internet *banking* melalui penerapan *token* dan *fingerprint*. Proses kerja sistem ini adalah dengan melakukan pemeriksaan *token* dan *fingerprint* setiap kali pengguna ingin melakukan transaksi perbankan. Sistem ini bisa diilustrasikan pada Gambar 2.

Selain itu, metode lain yang diajukan untuk meningkatkan keamanan *m-banking* adalah dengan menerapkan *One Time Password* (OTP) yang digunakan dalam proses enkripsi dan dekripsi pesan pada proses transaksi pesan antara *client* dan *server*. Penerapan metode OTP ini digunakan untuk mencapai pengamanan berbasis *end-to-end authentication* (Singh & Jasmine, 2015). Pengembangan metode pengamanan komunikasi *m-banking* juga sudah dilakukan

menggunakan kombinasi OTP dan *personal biometric*. Metode pengamanan transaksi *m-banking* juga telah dikembangkan dengan menggunakan penerapan skema layer pada protokol *mobile banking* (Li, dkk., 2009).

Gambar 2. Ilustrasi Pengamanan *Internet Banking* dengan Multi Biometrik

2.2. Kriptografi Kurva *Hyper Elliptic*

Perkembangan algoritma ECC (*Elliptic Curve Cryptosytem*) mengalami perubahan menuju skema kurva *hyper elliptic* dimulai ketika Miller and Koblitz untuk pertama kali mengajukan konsep HECC (*Hyper Elliptic Curve Cryptosytem*) pada tahun 1989 untuk melengkapi kekurangan algoritma kurva eliptik. Kurva eliptik masih memiliki *overhead* komputasi yang cukup tinggi pada beberapa parameter (genus) yang digunakan, sehingga kurang efektif jika diterapkan pada perangkat bergerak seperti *smartphone*. Tingkat keamanan menggunakan konsep kurva *hyper elliptic* ini terletak pada penggunaan masalah logaritma diskrit pada kurva Jacobian. Persamaan kurva Jacobian standar bisa dilihat pada persamaan (1), dimana h(x) adalah polinomial dari perpangkatan g dan h(x) ϵ F(x). f(x) adalah polinomial bersifat *monic* dari hasil perpangkatan 2g+1 dan h(x) ϵ F(x).

$$E : y^2 + h(x)y = f(x) \quad (1)$$

Penentuan genus yang digunakan pada komputasi akan mempengaruhi performa komputasi pada HECC (Vijayakumar, dkk., 2014). Salah satu bidang yang menerapkan algoritma kurva eliptik ini adalah di bidang *e-shopping* yang banyak dilakukan melalui aplikasi berbasis *mobile* (Ham, 2013). Algoritma kriptografi kurva eliptik ini juga cocok digunakan pada perangkat keras berbasis *mobile* seperti pada *processor* ARM yang banyak digunakan pada perangkat *smartphone* (Bartolini, dkk., 2008). Hal ini menjadi sangat bermanfaat pada jaringan *wireless* yang digunakan sebagian luas oleh pengguna *smartphone* saat ini (Lauter, 2004).

3. Metode Pengamanan yang Diusulkan

Skema kriptografi yang terdiri dari tanda tangan digital dan proses pengacakan pesan melalui enkripsi dan dekripsi akan digunakan untuk mengamankan sebuah pesan *m-banking*, kriptografi berfungsi untuk mengubah sebuah teks asli *(plaintext)* menjadi teks berkode *(ciphertext)* dan sebaliknya.

Tanda tangan digital berbasis kurva *hyper elliptic* akan digunakan untuk membangun sebuah proses autentikasi yang cepat dan memiliki tingkat keamanan yang baik. Selain itu juga, proses enkripsi akan digunakan untuk mengubah *plaintext* menjadi *ciphertext* dan dekripsi digunakan untuk mengubah *ciphertext* menjadi *plaintext*. Proses ini akan dilakukan pada setiap pesan yang akan ditransaksikan melalui *m-banking*.

3.1. Model Pengamanan

Pendekatan komunikasi yang digunakan pada penelitian ini adalah dengan dengan model arsitektur berbasis *client server*. Pada saat ingin melakukan transaksi perbankan melalui *m-banking*, seorang *client* harus terlebih dahulu meminta kepada *server* sebuah kunci yang akan digunakan untuk melakukan komunikasi. Konsep pengamanan berbasis kunci pada penelitian ini akan menggunakan kunci *public* dan *private*. Kedua kunci tersebut akan berfungsi untuk: (a) Kunci privat. Kunci ini akan digunakan untuk memberikan tanda tangan digital pada pesan pada sisi pengirim dan akan digunakan untuk melakukan dekripsi pesan pada sisi penerima. (b) Kunci Publik. Kunci ini akan digunakan untuk melakukan verifikasi tanda tangan digital pada pesan pada sisi penerima dan akan digunakan untuk melakukan enkripsi pesan pada sisi pengirim.

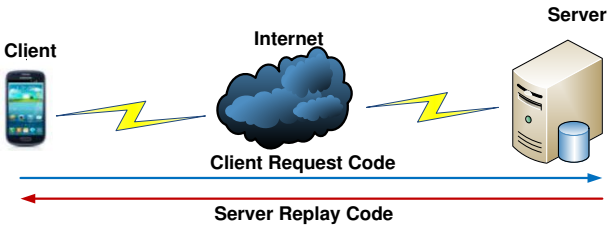
Kedua kunci tersebut akan dibangkitkan menggunakan konsep kurva *hyper elliptic*. Pada sisi *client*, setiap pengguna yang hendak mengirim pesan melalui jaringan publik (internet) terlebih dahulu harus melakukan enkripsi pada pesan tersebut.

3.2. Tahap Pengamanan

Pada penelitian ini penerapan algoritma kurva *hyper elliptic* digunakan selama sesi komunikasi antara *client* dan *server* bank. Di dalam proses pengamanan pesan *m-banking* yang menggunakan konsep autentikasi dan kerahasiaan pesan ini, ada beberapa tahap yang harus dilalui pada sisi *client* maupun *server*, tahap-tahap pengamanan yang dilalui antara lain dikemukakan pada sub bab 3.2.1. sampai sub bab 3.2.4.

3.2.1. Tahap Memulai Komunikasi

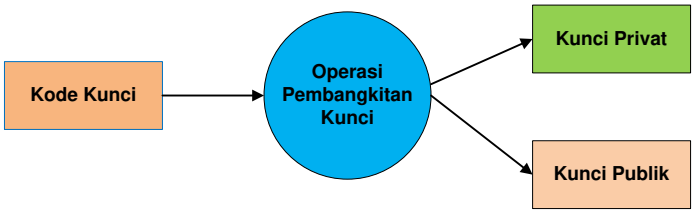
Pada tahap ini, *client* akan melakukan *request* kepada *server* untuk meminta kode pembangkitan kunci yang akan digunakan untuk melakukan komunikasi dalam sebuah sesi. Pada tahap ini, *server* akan mengirimkan sebuah kode acak kepada setiap *user* dan merekam identitas pengguna yang melakukan permintaan kode. Setelah kode diterima oleh *client*, kode akan digunakan untuk membangkitkan kunci yang akan digunakan untuk mengamankan komunikasi yang terjadi selama sesi berlangsung. Tahap permintaan kode oleh *client* yang digunakan untuk pembangkitan kunci bisa diilustrasikan pada Gambar 3. Setiap kali *client* ingin melakukan transaksi perbankan melalui jaringan publik, maka *client* harus melakukan aksi *request code* (permintaan kode tertentu kepada *server*).



Gambar 3. Transaksi Kode pada *m-banking*

3.2.2. Tahap Pembangkitan Kunci

Pada tahap ini, setiap *client* yang telah menerima *random code* dari *server* akan mulai membangkitkan kunci masing-masing dengan skema algoritma kurva *hyper elliptic*. Hasil dari pembangkitan kunci tersebut kemudian akan digunakan untuk melakukan komunikasi pesan. Proses pembangkitan kunci bisa diilustrasikan pada Gambar 4. Kunci yang telah dibangkitkan tadi hanya bisa digunakan dalam sebuah sesi komunikasi, jika sesi transaksi data berakhir maka *server* akan menghapus kunci sehingga tidak bisa digunakan untuk melakukan transaksi yang berikutnya. Hal ini untuk menghindari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

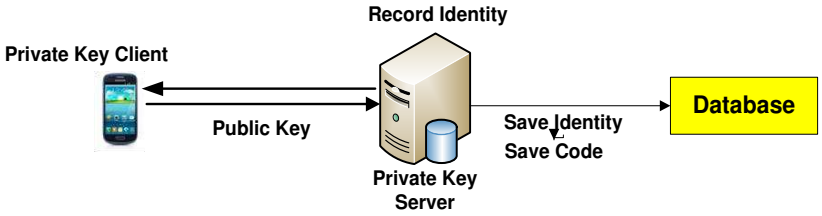


Gambar 4. Pembangkitan Kunci

3.2.3. Tahap Otentikasi Awal dan Pertukaran Kunci Publik

Setelah kode pembangkitan kunci publik dan privat telah dilakukan pada sisi *client* dan sisi *server*, setelah itu keduanya akan bertukar kunci publik yang bisa dikirimkan melalui jalur internet. Pada tahap ini juga, akan dilakukan proses autentikasi awal pada sisi *server* dengan

cara menyimpan kode dan identitas perangkat yang memiliki kode tersebut. Tahap ini digunakan sebagai proses otentikasi awal pengguna *m-banking* selama sesi komunikasi berlangsung. Skema pertukaran kunci dan autentikasi awal terhadap *user* bisa diilustrasikan pada Gambar 5.

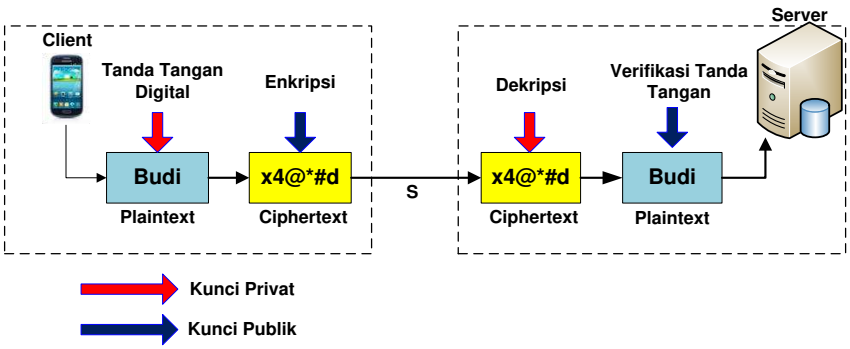


Gambar 5. Skema Pertukaran Kunci pada *m-banking*

3.2.4. Tahap Transaksi Data

Pada tahap ini *client* yang hendak melakukan komunikasi dengan *server* harus memiliki kunci (*session key*) yaitu sebuah kunci yang hanya bisa digunakan pada saat sesi tersebut berlangsung. *Session key* ini terdiri dari sepasang kunci yaitu kunci privat dan kunci publik. *Client* yang telah memiliki *session key* akan melakukan pemberian tanda tangan digital dan proses enkripsi pada pesan menggunakan kunci privat yang dimiliki.

Pesan yang dikirim melalui jaringan publik (internet) berupa pesan *ciphertext* yang sudah diberikan tanda tangan digital. Model pengamanan *m-banking* dengan skema komunikasi *client server* ini bisa terlihat seperti Gambar 6. Transaksi pesan dalam sistem keamanan *m-banking* ini menggunakan format *ciphertext* yang sudah dibubuhi dengan tanda tangan digital sehingga dapat menjaga keaslian pesan yang dikirim melalui jalur internet. Pada saat sebuah pesan ingin dikirimkan, maka pesan tersebut akan melalui sebuah proses pemberian tanda tangan digital menggunakan algoritma kurva *hyper elliptic*. Pemberian tanda tangan digital akan menggunakan kunci privat yang dimiliki oleh setiap pengirim baik *server* maupun *client.* Ketika pesan *ciphertext* tersebut sampai ke *server*, maka pesan akan didekripsikan menjadi sebuah *plaintext* menggunakan kunci *session key* yang dimiliki oleh *server*. Sebuah pesan *ciphertext* hanya bisa didekripsikan jika kunci enkripsi dan dekripsinya sama. Setelah itu, pesan *plaintext* akan diverifikasi menggunakan kunci publik yang sudah dikirim pada awal sesi komunikasi untuk melakukan validasi keaslian pesan. Proses dekripsi akan menggunakan konsep permasalahan Logaritma Diskrit (Smart, 1999).



Gambar 6. Proses Transaksi Pesan *m-banking*

3.3. Algoritma Pengamanan

Untuk proses pengamanan pesan dalam transaksi *m-banking*, skema algoritma kurva *hyper elliptic* yang digunakan dikemukakan pada subbab 3.3.1 sampai dengan subbab 3.3.3.

3.3.1. Algoritma Pembangkitan Kunci *(Generating)*

Algoritma *Generating* digunakan untuk membangkitkan sepasang kunci yang akan

digunakan untuk proses komunikasi antara *client* dan *server*. Kunci yang dibangkitkan berasal dari *random code* yang diberikan oleh *server*. Algoritma pembangkitan kunci bisa dideskripsikan pada persamaan (2), dengan masukan sebuah parameter umum dari kurva *hyper elliptic* C, bilangan prima p dan pembagi D *(Divisor)*, keluarannya adalah Kunci Publik P_A dan Kunci Privat a. Dengan proses: Untuk menghitung Kunci Privat $k_A \in RN$ diperoleh dari hasil perhitungan nilai prima acak dari k_A Hingga N. Sedangkan nilai Kunci Publik diperoleh melalui perhitungan persamaan (2), dimana P_A merupakan pasangan Polinomial *[u(x), v(x)]* . Pasangan kunci privat dan kunci publik merupakan titik pada kurva yaitu P_A, k_A.

$$P_A \leftarrow k_A \tag{2}$$

3.3.2. Algoritma Enkripsi

Algoritma enkripsi digunakan sebagai bentuk pengamanan akan diterapkan dalam pengubahan bentuk *plaintext* menjadi *ciphertext*. Proses ini menggunakan kunci publik yang diperoleh dari pasangan komunikasi. Pada proses ini, pesan *plaintext* akan diubah ke dalam bentuk kode ASCII dan direpresentasikan sebagai rangkaian titik (u_x, v_y). Algoritma enkripsi yang akan digunakan pada penelitian ini dideskripsikan berdasarkan persamaan (3).

Pada awal proses enkripsi, *user* harus memiliki sebuah pasangan kunci yang terdiri dari Kunci Privat dimana k_A adalah bilangan prima acak pada rentang N (bilangan *Real*) dan sebuah Kunci Publik (P_A): $P_A \leftarrow k_A$ merupakan pasangan dari polinomial [*U(x), V(x)*]. Setelah itu, sebuah kunci pernyataan dihitung dengan persamaan $Q_A \leftarrow k_A . P_B$, dimana P_B adalah representasi dari kunci publik penerima. Untuk menciptakan sebuah *ciphertext* maka persamaan yang digunakan adalah persamaan (3), dimana Cm direpresentasikan sebagai titik [*U(x), V(x)*].

$$C_m \leftarrow \{Q_A . E_m + P_A\} \tag{3}$$

3.3.3. Algoritma Dekripsi

Algoritma dekripsi ini digunakan untuk membuka pesan *ciphertext* yang sudah melalui proses enkripsi. Proses ini akan menggunakan kunci privat yang dimiliki oleh masing-masing penerima baik *server* maupun *client*. Algoritma enkripsi ini memiliki masukan berupa pesan *ciphertext* Cm, keluaran berupa pesan *plaintexti* Em. Pada proses dekripsi pesan *ciphertext* Cm, penerima akan melakukan ekstraksi koordinat 'Q_A' dari *ciphertext* yang diterima, kemudian koordinat kedua dari Q_A akan dioperasikan dengan kunci privat. Operasi dekripsi untuk mengembalikan format pesan menjadi *plaintext* dioperasikan dengan persamaan (4). Proses ini menggunakan konsep *Hyperelliptic Curve Discrete Logarithmic Problem* (HECDLP). Untuk meningkatkan aspek keamanan pesan yang dikirim melalui jaringan publik, pemilihan genus untuk algoritma dekripsi menjadi sangat penting.

$$\begin{aligned} &E_m + kP_B - Q_B(Q_A) = E \\ &= E_m + kP_B - k(Q_B D) \\ &= m + kP_B - Q_B(kD) \\ &E_m + kP_B - kP_B = E_m \end{aligned} \tag{4}$$

4. Analisis Keamanan

4.1. Keamanan *End-to-End*

Pada penelitian ini, metode pengamanan yang digunakan untuk pengamanan pesan *m-banking* adalah tanda tangan digital dan enkripsi/dekripsi. Algoritma yang digunakan untuk pengamanan adalah kurva *hyper elliptic* dengan panjang genus (g) adalah 2 dan 3. Penerapan kurva *hyper elliptic* dengan genus 2 dan 3 akan memberikan aspek keamanan yang tinggi dan waktu komputasi yang cepat dibandingkan dengan menggunakan nilai genus yang lain.

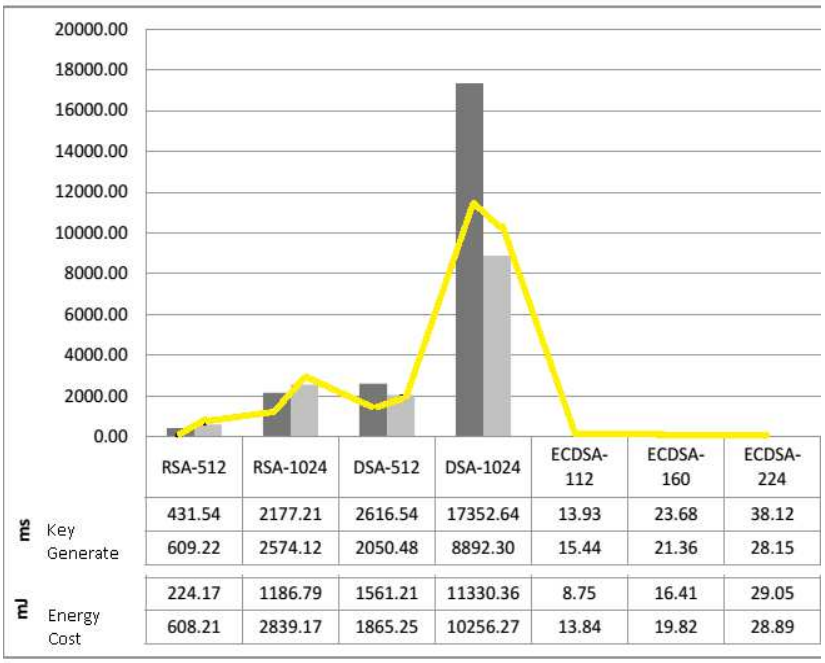
Penggunaan algoritma ini akan dimulai sejak proses pembangkitan pasangan kunci privat dan kunci publik yang akan digunakan selama sesi komunikasi *m-banking*. Pasangan

kunci yang telah dibangkitkan hanya dapat digunakan untuk satu sesi komunikasi sehingga tidak bisa digunakan oleh pihak yang tidak bertanggung jawab. Ketika *client* sudah berada pada status non-aktif maka *server* akan menghapus *public key* pada *server* sehingga transaksi *m-banking* tidak bisa dilakukan setelahnya.

Metode pengamanan dengan kombinasi *session key*, *digital signature* dan kriptografi di atas akan menciptakan aspek keamanan yang bersifat *end-to-end* dimana hanya pihak pengirim dan penerima yang bisa membaca dan memeriksa keaslian pesan yang dikirimkan melalui jalur internet publik.

4.2. Analisis *Overhead* Proses Komputasi

Penggunaan algoritma kurva *hyper elliptic* pada komunikasi *m-banking* akan memiliki keunggulan yakni pada proses pembangkitan kunci, serta proses enkripsi dan dekripsi yang cepat serta konsumsi *power* yang lebih rendah dibandingkan dengan algoritma kunci publik seperti RSA *(Rivest-Shamir-Adlemen)* atau DSA *(Digital Signature Algorithm).* Hal ini sangat cocok bagi perangkat bergerak yang memiliki *resource* dengan jumlah terbatas saat ini. Perbandingan waktu pembangkitan kunci dan *energy cost* pada beberapa algoritma asimetrik bisa dilihat pada Gambar 7.



		RSA-512	RSA-1024	DSA-512	DSA-1024	ECDSA-112	ECDSA-160	ECDSA-224
ms	Key Generate	431.54	2177.21	2616.54	17352.64	13.93	23.68	38.12
		609.22	2574.12	2050.48	8892.30	15.44	21.36	28.15
mJ	Energy Cost	224.17	1186.79	1561.21	11330.36	8.75	16.41	29.05
		608.21	2839.17	1865.25	10256.27	13.84	19.82	28.89

Gambar 7. Perbandingan Penggunaan Waktu dan Energi Algoritma Asimetri

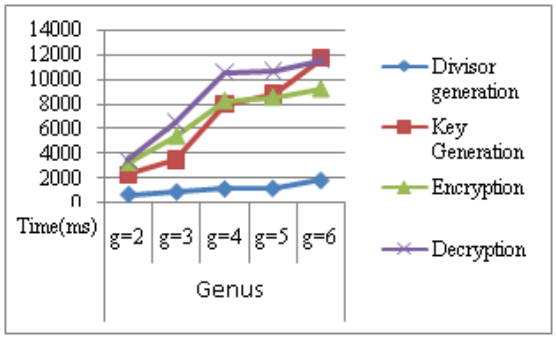
Keunggulan ini akan mempermudah implementasi baik pada level *software* maupun *hardware*. Oleh karena itu, algoritma kurva eliptik ini banyak digunakan untuk menyelesaikan permasalahan keamanan dengan perangkat keras yang memiliki *resource* terbatas. Pada sebuah pengujian dengan menggunakan perangkat PDA dan *smartphone* dengan CPU 400 MHz, terlihat kecepatan komputasi antara algoritma kurva Eliptik, RSA, DSA memiliki perbedaan yang signifikan (Rifà-Pous & Herrera-Joancomarti, 2011).

4.3. Level Keamanan Algoritma

Untuk mencapai level autentikasi maupun proses enkripsi dan dekripsi yang baik, beberapa nilai genus g dapat dipilih pada kasus *m-banking*. Nilai g akan mempengaruhi setiap proses komputasi pengamanan pesan mulai dari proses pembangkitan kunci, pemberian tanda tangan hingga verifikasi tanda tangan digital pada pesan. Kinerja setiap genus g pada komputasi perangkat bergerak (*mobile)* bisa diilustrasikan pada Gambar 8. Pada Gambar 8, *key generation*

menggambarkan waktu pembangkitan pasangan kunci dengan memanfaatkan algoritma kurva *hyper elliptic* pada lingkungan perangkat bergerak (*smartphone*). Sedanglan *divisor generation* merupakan nilai yang diperoleh dari perhitungan titik pada *Jacobian Curve* melalui operasi penambahan dan perkalian titik pada kurva *hyper elliptic*.

Penggunaan algoritma kurva *hyper elliptic* menghasilkan komputasi yang efisien dengan penggunaan yang *resource* yang kecil. Berdasarkan grafik pada Gambar 8 bisa terlihat bahwa penggunaan nilai genus g=2 menghasilkan nilai yang paling kecil. Hal ini menandakan penggunaan nilai genus g=2 pada kurva *hyper elliptic* menjadi pilihan yang paling memungkinkan jika diterapkan pada komputasi *mobile*. Selain itu juga, penggunaan kurva *hyper elliptic* dengan nilai genus=2 akan memberikan level keamanan yang lebih tinggi dari pada pada RSA 256/512 dan DSA 256/512 (Rifà-Pous & Herrera-Joancomarti, 2011). Jika komputasi dilakukan dengan nilai genus yang lebih tinggi misalnya dengan nilai genus=6, maka akan memberikan keamanan yang lebih baik tetapi menggunakan waktu yang lebih besar dan mengkonsumsi energi yang lebih tinggi (Ganesan & Vivekanandan, 2011).



Gambar 8. Kinerja Genus g pada Komputasi *Mobile*

Pada skema pengamanan yang diusulkan penelitian ini, penggunaan konsep tanda tangan digital dengan fungsi *hash* pada algoritma kurva eliptik dilakukan untuk memvalidasi pesan yang diterima oleh *receiver*. Ukuran blok yang dihasilkan sesuai dengan pilihan fungsi *hash* dengan memperhatikan aspek keamanan yaitu dengan menggunakan SHA 2 atau SHA 3. Hal ini akan memberikan aspek keaslian pesan yang memastikan bahwa pesan tidak berubah selama proses pengiriman melalui jaringan internet publik. Selain itu juga penggunaan kurva *hyper elliptic* sebagai algoritma keamanan memiliki tingkat keamanan yang baik dibandingkan dengan algoritma RSA dan DSA yang sudah terlebih dahulu diterapkan pada berbagai macam aplikasi dan perangkat keras (Vijayakumar, dkk. 2014). Pada penelitian ini, perangkat simulasi yang digunakan pada pengujian komputasi algoritma kurva *hyper elliptic* bisa dilihat pada Tabel 1.

Tabel 1. Spesifikasi Perangkat (*Simulator*) Pengujian

Spesifikasi	Jenis Processor	RAM	Internal Memory
Simulator 1	ARM**v7** 800Mhz	128 MB	100 MB
Simulator 2	ARM**v7** 800Mhz	266 MB	150

5. Kesimpulan

Penelitian ini mengajukan sebuah metode pengamanan yang efisien dengan konsep keamanan *end-to-end* yang akan diterapkan pada *m-banking*. Metode pengamanan yang digunakan adalah kombinasi tanda tangan digital dan kriptografi. Tanda tangan digital akan digunakan untuk melakukan validasi terhadap keaslian sebuah pesan, sedangkan enkripsi/dekripsi akan digunakan untuk menjaga kerahasiaan pesan yang dikirim pada proses transaksi *m-banking* sehingga dua aspek keamanan pesan bisa tercapai sekaligus.

Peneilitian menerapkan *session key* yaitu sepasang kunci (kunci privat dan kunci publik) yang hanya bisa digunakan pada sebuah sesi komunikasi *m-banking*. *Session key* dibangkitkan

melalui sebuah kode yang dibangkitkan sebelumnya oleh *server* dan dikirimkan kepada *client* untuk proses autentikasi dan enkripsi/dekripsi pada proses komunikasi.

Untuk mencapai level keamanan yang baik, *overhead* yang kecil dan waktu komputasi yang rendah, penelitian mengusulkan penggunaan genus g=2 pada perhitungan kurva *hyper elliptic.* Analisis yang telah dilakukan menunjukkan waktu komputasi dengan genus g=2 menghasilkan waktu yang paling rendah. Selain itu juga, pengguaan kurva *hyper elliptic* menghasilkan *overhead* yang lebih kecil dibandingkan dengan penggunaan algoritma asimetri yang sejenis seperti RSA dan DSA.

Referensi

Bartolini, S., Branovic, I., Giorgi, R., & Martinelli, E. (2008). Effects of Instruction-Set Extensions on an Embedded Processor: A Case Study on Elliptic Curve Cryptography over GF (2 m). *Computers, IEEE Transactions on,57(5),* 672-685.

Budiono. (2013). "*Penerapan Tanda Tangan Digital Untuk Keamanan Transaksi Sms – Banking,*" ITB Bandung.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: a survey of issues, malware penetration, and defenses. *Communications Surveys & Tutorials, IEEE, 17(2),* pp. 998-1022.

Ganesan, R, & Vivekanandan, K, (2011). Comparative Analysis Of Higher Genus Hyperelliptic Curve Cryptosystems Over Finite Field F_P, *ICTACT Journal On Communication Technology.* 2(1). pp. 238-240.

Ham, L. (2013). "Group Authentication". *IEEE Trans. Vehicular Technology*, 62(9).

Ku, W. C. (2005). Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture. *IEEE transactions on neural networks/a publication of the IEEE Neural Networks Council, 16(4),* 1002-1005.

Kumar, N., Mathur, A., & Lal, S. (2013). Banking 101: Mobile-izing Financial Inclusion in an Emerging India. *Bell Labs Technical Journal, 17(4),* 37-41.

Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications, 11(1),* 62-67.

Li, D., Lin, D., Zhao, G., & Huang, B. (2009). Design and correctness proof of a security protocol for mobile banking. *Bell Labs Technical Journal, 14(1),* 259-265.

Menezes, A., Wu, Y. & Zuccherato, R. (1996). An elementary introduction tohyperelliptic curves. Department of C&O, University of Waterloo, Ontario, Canada.

Ren, K., Yu, S., Lou, W., & Zhang, Y. (2009). Multi-user broadcast authentication in wireless sensor networks. *Vehicular Technology, IEEE Transactions on, 58(8),* 4554-4564.

Rifà-Pous, H., & Herrera-Joancomarti, J. (2011). Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices, *Future Internet, 3 (1):* 31-48.

Rivest, R.L., Shamir, A., Adleman, L. (1994). "*AMethod for Obtaining DigitalSignatures and Public-KeyCryptosystems"*, Massachusetts Institute of Technology, Cambridge.

Shih, K. H., & Lin, C. Y. (2015). *Is mobile banking a competitive weapon?. International Journal of Electronic Finance,* 8(2-4), pp. 189-201.

Singh, B., & Jasmine, K. S. (2015). Secure End-To-End Authentication for Mobile Banking. *In Software Engineering in Intelligent Systems* (pp. 223-232). Springer International Publishing.

Smart, N. P. (1999). On the performance of hyperelliptic cryptosystems. In *Advances in Cryptology—EUROCRYPT'99* (pp. 165-175). Springer Berlin Heidelberg.

To, W. M., & Lai, L. S. (2014). Mobile banking and payment in China. *IT Professional, 16(3),* 22-27.

Vasco. (2009). Security: a major concern for the adoption of m-banking. (Online, http://www.banking-business-review.com/suppliers/vasco_strong_authentication_and_e_signature_specialising_in_online_accounts_identities_and_transactions/whitepapers/security_a_major_concern_for_the_adoption_of_m_banking)

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(1),* 137-146.