PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

Analisis Keamanan Protokol Mutual Autentikasi Menggunakan *Hyperelliptic Curve Cryptosystem* (HECC)

I Made Mustika Kerta Astawa
Program Studi Teknik Informatika S-2, Universitas Pamulang
e-mail: made.mustika19@gmail.com

***Abstrak*— *Hyperelliptic Curve Cryptosystem* (HECC) sangat cocok digunakan untuk mengamankan komunikasi dalam jaringan sensor nirkabel yang memiliki sumber daya terbatas (seperti: penyimpanan, waktu atau daya) pada batasan titik sensor yang digunakan untuk teknik keamanan konvensional. Kita bisa membangun genus 2 HECC 80-bit pada *finite field* untuk mencapai tingkat keamanan yang sama seperti 160-bit *Elliptic Curve Cryptography* (ECC) atau 1024-bit RSA. Pada paper ini dijelaskan protokol mutual autentikasi yang didasarkan pada *Hyperelliptic Curve Digital Signature Algorithm* (HECDSA) untuk akses keamanan dalam perangkat yang dibatasi sehingga memungkinkan kedua entitas untuk memverifikasi keaslian masing-masing. Hasil penelitian menunjukkan bahwa protokol ini memiliki tingkat keamanan yang memadai karena tahan terhadap beberapa serangan (*attack*).**

***Kata Kunci*— *Hyperelliptic Curve Cryptosystem* (HECC), *Hyperelliptic Curve Digital Signature Algorithm* (HECDSA), Protokol Mutual Autentikasi**

I. PENDAHULUAN

Dengan perkembangan teknologi informasi yang sangat pesat, jaringan nirkabel sekarang banyak digunakan untuk mengirimkan informasi penting yang berkaitan dengan monitoring data *real time*. Mekanisme keamanan sangat penting untuk memastikan integritas, kerahasiaan dan keaslian data. Hal ini menyebabkan tantangan dalam penerapan *cryptosystem* yang cocok karena pada jaringan ini terdiri dari banyak perangkat kecil dan pintar yang dibatasi dalam hal memori, daya komputasi dan pasokan energi. Sementara, yang perlu dipertimbangkan adalah ancaman keamanan yang berbeda dalam jaringan sensor nirkabel, serta algoritma yang digunakan juga berbeda baik algoritma simetris/asimetris. Secara umum, pendekatan ini juga perlu persiapan pendistribusian Kunci sebagai upaya konfigurasi yang lebih tinggi sebelum dihasilkan dan dikembangkan pada lalu lintas yang lebih untuk mendapatkan hasil yang memerlukan konsumsi energi tinggi.

Pada kasus algoritma simetris, memori yang digunakan lebih kecil tetapi musuh dapat dengan mudah melakukan kemungkinan penyadapan proses komunikasi atau memantau titik komunikasinya. Untuk menghindari jenis serangan yang mungkin terjadi, dapat digunakan protokol mutual autentikasi berbasis ECC. Daya tarik utama dari ECC dibandingkan dengan RSA yang menawarkan keamanan yang sama yaitu penggunaan ukuran kunci yang jauh lebih kecil, sehingga mengurangi *overhead* pemrosesan. Protokol Mutual Autentikasi *Key Agreement* berbasis ECC sudah diterapkan untuk keamanan Wireless LAN. Sejauh ini, beberapa protokol telah diusulkan untuk memberikan keamanan pada proses otentikasi dan penggunaan kunci untuk Wireless LAN. Protokol ini menggunakan algoritma ECDSA untuk meningkatkan keamanan otentikasi pengguna dan proses pertukaran kunci. Namun, tingkat keamanan juga dapat ditingkatkan dengan menggunakan *Hyperelliptic Curve* (HECC) karena memiliki beberapa keuntungan daripada ECC. Untuk HECC pada *finite field* diperlukan panjang variabel 40-bit sampai 80-bit untuk perhitungan operasi grup pada kurva tersebut. Dalam kasus ECC, dibutuhkan panjang variabel sekitar 160-bit sedangkan dalam kasus RSA dibutuhkan panjang variabel sekitar 1024-bit untuk mencapai keamanan yang sama. Oleh karena itu, HECC lebih cocok untuk implementasi pada platform jaringan nirkabel.

Hyperelliptic Curve Cryptosystem (HECC) diusulkan pertama kali oleh Koblitz pada tahun 1989 yang berbasis permasalahan logaritma diskret pada *Jacobian* dari *finite field hyperelliptic curve*. Perbedaan utama antara ECC dan HECC adalah grup operasi teutama pada urutan yang berbeda dari operasi yang digunakan. Tidak seperti pada *elliptic curve*, titik-titik pada *hyperelliptic curve* tidak membentuk sebuah grup. Grup aditif yang diimplementasikan pada kriptografi primitif adalah *divisor class group*. Setiap elemen dari grup ini adalah pengurangan dari *divisor*. Operasi *divisior group* pada HECC lebih kompleks dibandingkan dengan operasi titik pada ECC untuk implementasi pada kriptografi primitif. Oleh karena itu, terdapat tantangan untuk iplementasi HECC dalam lingkungan terbatas. Adapun kontribusi yang ingin dibahas pada makalah ini antara lain :

PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

a. Protokol Mutual Autentikasi yang didasarkan pada HECDSA untuk komunikasi yang aman dalam jaringan wireless untuk perangkat yang dibatasi. Protokol yang diusulkan adalah protokol autentikasi yang aman sehingga terhindar dari semua kemungkinan serangan baik dari pengguna internal maupun serangan eksternal (*hacker*).
b. Penerapan dari protokol autentikasi yang berbasis HECDSA serta dapat dilihat juga ketahanan terhadap serangan-serangan (*attack*) yang mungkin terjadi pada suatu protokol..

II. METODE PENELITIAN

Pada penelitian ini, penulis menggunakan metode penelitian kepustakaan. Metode tersebut berupa deskripsi penelitian yang dihasilkan atas kajian referensi pustaka yang didukung dengan analisis data. Sama seperti bentuk penelitian lainnya, penelitian kepustakaan dan analisis ini bertujuan untuk mengklarifikasi atau memperluas pemahaman dan pengetahuan dari konsep yang ada. Tahapan proses penelitian ini adalah sebagai berikut:

a. Pengumpulan data

Melakukan pengumpulan referensi dari beberapa buku atau referensi lain mengenai mekanisme mutual autentikasi dan *Hyperelliptic Curve Cryptosystem* (HECC)

b. Perancangan Skema

Melakukan perumusan dan perancangan skema terhadap mekanisme Mutual Autentikasi menggunakan konsep *Hyperelliptic Curve Cryptosystem* (HECC).

c. Analisis data

Analisis hasil pengumpulan data yang telah dilakukan, sehingga didapat analisis terkait keamanan dari mekanisme mutual autentikasi dan *Hyperelliptic Curve Cryptosystem* (HECC).

d. Pengambilan Kesimpulan

Pengambilan simpulan hasil penelitian..

III. PEMBAHASAN

A. Aritmatika Hyperelliptic Curve

Anggap F merupakan *finite field* dan $\bar{F}$ aljabar tertutup dari F . *Hyperelliptic curve* C pada genus $g \geq 1$ pada batasan F merupakan himpunan solusi $(u,v) \in F \times F$ untuk persamaan $C: v^2 + h(u)v = f(u)$. Polinimial $h(u) \in F[u]$ derajat yang lebih besar dari g dan $f(u) \in F[u]$ merupakan *polynomial monic* dengan derajat $2g+1$. Untuk karakteristik tersebut sudah cukup untuk menganggap bahwa $h(u) = 0$ dan $f(u)$ adalah derajat bebas. Jika tidak ada titik kurva pada batasan aljabar yang tertutup $\bar{F}$ dari F yang memenuhi kedua turunan parsial $2v + h(u) = 0$ dan $h'(u)v - f'(u) = 0$, kemudian kurva tersebut dinamakan non singular.

Titik pada kurva C dibangkitkan oleh himpunan yang disebut *Jacobian. Jacobian* dari kurna C merupakan *quotient group* $J = D^0 / P$, dimana D^0 merupakan himpunan pembagi pada derajat nol, dan P merupakan himpunan pembagi pada fungsi rasional. Elemen Jacobian pada batasan F dinotasikan sebagai $J_C(F)$ dapat dipresentasikan secara unik oleh pembagi $D = \sum m_i P_i, m_i \in Z$, penjumlahan secara formal dari titik $\bar{F}$. Derajat merupakan penjumlahan dari koefesien $\sum m_i$. Himpunan dari seluruh pembagi pada grup Abelian dinotasikan oleh $D(C)$. Himpunan pada pembagi derajat nol D^0 pada subgrup $D(C)$ ..

B. Keamanan dari Hyperelliptic Curve

Pada *Hyperelliptic Curve Cryptography*, menemukan sebuah kurva *hyperelliptic* yang sesuai merupakan suatu permasalahan yang sangat penting. Keamanan dari HECC yang berbasiskan sulitnya dalam memecahkan permasalahan logaritma diskrit pada *Jacobian* (*Hyperelliptic Curve Discrete Logarithm Problem* (HCDLP)). HCDLP pada $J\left(C; F_q^n\right)$ yaitu : diberikan dua bilangan pembagi D_1, D_2 yang didefinisikan pada $J\left(C; F_q^n\right)$ dalam batas F_q^n , untuk mendapatkan nilai integer m sehingga $D_2 = mD_1$.

PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

Untuk menyediakan sebuah aspek keamanan *hyperelliptic curve, Jacobian* harus memenuhi kondisi berikut ini :

a. Adleman dan kawan-kawan telah menemukan algoritma waktu subeksponential untuk memecahkan logaritma diskrit di *Jacobian* dari HEC yang memiliki genus besar dalam batasan *finite field*. Kurva dengan genera yang lebih tinggi ($g \le 4$) tidak sesuai digunakan untuk kriptografi $\left(2g+1 < \log q^n\right)$.
b. Jika orde dari grup tersebut besar tetapi habis dibagi dengan prima kecil, maka DLP akan bisa dirusak dengan serangan Pohlig-Hellman. Sehingga bisa dinyatakan bahwa panjang dari faktor prima terbesar harus paling sedikit 16-bit.
c. Untuk mencegah serangan Frey yang menggunakan pembangkitan *tate pairing* pada serangan MOV, faktor prima besar pada $J\left(C; F_q^n\right)$ harus tidak membagi $\left(q^n\right)^k - 1$, dimana $k < (\log q^n)^2$.
d. Untuk mencegah serangan yang dihasilkan oleh Ruck, *Jacobian* pada *hyperelliptic curve* atas field prima besar harus tidak memiliki *p*-order subgroup.

Untuk menguatkan kriptografi primitif dari serangan *side-channel* yang sederhana, harus dibuat informasi yang independent dari skalar rahasia. Hal ini dapat diimplementasikan melalui *Montgomery* untuk perkalian skalar.

C. Protokol Mutual Autentikasi

Protokol mutual autentikasi diperlukan untuk mencegah serangan ketika pengguna yang berbahaya berpura-pura sebagai pihak yang berwenang dan melakukan duplikat, perubahan,, penambahan dan penghapusan data pada saat proses pengiriman. Maka dari itu, pada paper ini diusulkan protokol mutual autentikasi yang berbasis HECDSA pada jaringan wireless yang akan memberikan aspek autentikasi dan anti penyangkalan. Beberapa hal-hal baru dari protokol ini adalah sebagai berikut :

a. Protokol mutual autentikasi ini berbasis HECDSA pada jaringan wireless yang sangat cocok untuk peralatan yang dibatasi dengan menggunakan genus 2 HEC pada 80-bit *finite field* dimana memiliki tingkat keamanan yang sama dengan ECC 160-bit.
b. Setiap pengguna jarak jauh dapat memperoleh layanan dari pengguna lain tanpa melakukan pendafatarn dengan KDC setiap kali melakukan komunikasi. Mereka dapat mentransfer data setelah melakukan otentikasi bersama.
c. *Session key* yang baru disediakan untuk setiap sesi tertentu dengan tujuan melindungi data dari *replay attack* pada jaringan wireless.
d. Enkripsi terhadap pesan yang dikirim menggunakan asimetrik dengan tujuan menghemat energy dan penyimpanan pada proses enkripsi, yang merupakan suatu hal terpenting pada perangkat yang dibatasi.

Beberapa notasi-notasi yang digunakan pada protokol ini antara lain :

C : *Hyperelliptic curve* pada genus *g* yang didefinisikan pada batasan F_p

p : Bilangan prima besar

q : Pembagi bilangan prima besar pada $p-1$

P : Basis titik pada hyperelliptic curve

D : Semi *reduced divisor* pada HEC

D' : Unik *reduced divisor* pada HEC

PR_A, PU_A : Masing-masing kunci privat dan publik dari A

PR_B, PU_B : Masing-masing kunci privat dan publik dari B

ID_A : Identitas dari A

ID_B : Identitas dari B

M : Input Pesan

(r, s) : Pasangan Signature

M' : Pesan yang diterima

(r', s') : Pasangan Signature yang diterima

$H(.)$: Fungsi hash satu arah dengan panjang output yang tetap

K : Kunci Rahasia yang Umum

K_s : *Session Key*

K_a : Premaster key yang dibagi antara pengguna dan KDC

T_s : *Session Time*

PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

$\oplus$: Penambahan gurp diantara elemen Jacobi

Penjelasan umum dari protokol ini adalah sebagai berikut :

Selama fase inisialisasi, *Key Distribution Center* (KDC) membangkitkan *hyperelliptic curve* C acak yang didefinisikan pada batasan F_p. Kemudian KDC menghitung *semi reduce divisor* D dan *unik reduced divisor* D' dari kurva yang dipilih menggunakan algoritma Cantor. Protokol ini menggunakan D' dan D yang jelas.

KDC juga menghitung sebuah titik $P=\left(x_1,y_1\right)\in C\left(F_p\right)$ dimana merupakan basis titik pada kurva, bilangan prima besar p dan pembagi prima q dengan ketentuan q membagi $p-1$. F_p berisi representasi dari seluruh elemen *field* pada order *n.* Akhirnya parameter-parameter yang dibangkitkan oleh KDC yaitu $\left(F_p,C,D',p,q,D,n\right)$.

Selama fase pembentukan sebuah jaringan, seluruh pengguna mengirimkan permintaan pesan ke KDC untuk didaftarkan pada jaringan. Setelah pendaftaran, KDC memberikan ID yang unik untuk setiap pengguna dan mengirimkan ID dengan parameter K_a untuk setiap pengguna. KDC juga membuat daftar seluruh pengguna beserta ID masing-masing.

Setelah fase pembentukan jaringan, KDC mengumumkan daftar pengguna yang dienkripsi dengan parameter kunci K_a untuk seluruh pengguna dari jaringan dengan parameter sistem $\left(F_p,C,D',p,q,D,n\right)$. Diasumsikan juga setelah dilakukan pembentukan pada pengguna (titik), setiap penguna kan bersifat tetap.

Misalnya, pengguna A ingin melakukan komunikasi dengan pengguna B. Pengguna A mengrimkan permintaan pesan ke pengguna B yang mengandung ID_A dan *nonce* N_1. Setelah pesan diterima, jika pengguna B ingin melakukan komunikasi dengan pengguna A, pertama kali akan dilakukan verifikasi ID dari daftar pengguna. Jika ID cocok, maka pengguna B akan mengirimkan pesan persetujuan ke pengguna A yang mengandung ID_B dan *nonce* N_1.

Selanjutnya, pengguna A dan pengguna B akan berkomunikasi setelah melakukan mutual autentikasi. Pada skema mutual autentikasi, *session key* dibangkitkan dari tahapan-tahaapan secara umum sebagai berikut :

a. Tahapan Pertama

Pengguna B memilih bilangan acak d_B, dimana $1\le d_B\le n-1$, kemudian menghitung $Q_B=d_B\times D'=\left[u_B,v_B\right]$ menggunakan perkalian scalar pada genus 2 HECC. Kemudian pengguna B membangkitkan kunci privat $PR_B\in N$ (pilih bilangan prima positif dalam N) dan kunci public $PU_B=\left[PR_B\right]D$. PU_B diwakili dengan representasi Mumford yaitu dalam bentuk $\left[u_B,v_B\right]$. Akhirnya, pengguna B mengirimkan $\left(Q_B,PU_B\right)$ ke pengguna A.

b. Tahapan Kedua

Pengguna A memilih bilangan acak d_A, dimana $1\le d_A\le n-1$, kemudian menghitung $Q_A=d_A\times D'=\left[u_A,v_A\right]$ menggunakan perkalian scalar pada genus 2 HECC. Selanjutnya pengguna A menghitung $z=Q_A\oplus Q_B$ untuk mutual autentikasi (dengan melakukan penambahan pembagi pada koordinat *affine*). Kemudian pengguna A membangkitkan kunci privat $PR_A\in N$ (pilih bilangan prima positif dalam N) dan kunci public $PU_A=\left[PR_A\right]D$. Setelah itu, pengguna A menghitung nilai kunci rahasia $K=d_A\times Q_B=\left[u_1,v_1\right]$. Sebagai tambahan, pengguna A menghitung $r=\left(\sum_{i=0}^{e-1}L(u_i)q^i\right)\bmod p$ dimana e merupakan integer dengan $e\le g$ dan diasumsikan elemen *finite field* merupakan order seperti $0\le L\left(u_i\right)<q$ [untuk pemetaan diantara Jacobian $J\left(F_p\right)$dan *finite field* $GF\left(p\right)$]. Pengguna A juga menghitung $s=\left[r^{-1}\left(H\left(M\right)-\left[PR_A\right]r\right)\right]\bmod p$. Akhirnya, $\left(r,s\right)$ menjadi pasangan signature dan pengguna A mengirimkan pasangan signature dengan $\left(Q_A,PU_A\right)$ ke pengguna B.

c. Tahapan Ketiga

Pengguna B menghitung $\beta=Q_A\oplus Q_B$ dengan *divisor addition* pada koordinat *affine*. Pengguna B juga menghitung *secret key* $K=d_B\times Q_A=\left[u_i,v_i\right]$. Jika protokol bekerja secara benar, kedua pengguna akan menghasilkan nilai K yang sama. Hal ini dapat dibuktikan dengan perhitungan matematika sederhana yang ditunjukkan dibawah ini :

PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

$$K = d_B \times Q_A = d_B \times d_A \times D^{'} = d_A \times d_B \times D^{'} = d_A \times Q_B = \left[u_i, v_i\right]$$

Pengguna B juga menghitung $w = \left(s^{'}\right)^{-1} \bmod p$ dimana $\left(r^{'}, s^{'}\right)$ merupakan signature yang diterima. Kemudian pengguna B menghitung $U_1 = \left(H\left(M^{'}\right)w\right) \bmod p$ dan $U_2 = \left(r^{'}w\right) \bmod p$. Sebagai tambahan, B menghitung $V = \left[U_1\right]D \oplus \left[U_2\right]PU_A = \left[u_f, v_f\right]$. Jika $V = \left[1,0\right]$, hal itu berarti signaturenya tidak benar, dan pengguna B menolak pesan dengan signature tersebut. Pengguna B menghitung $V^{'} = \left(\sum_{i=0}^{e-1} L\left(u_{f,i}\right)q^i\right) \bmod p$ [untuk mapping diantara Jacobian $J\left(F_p\right)$ dan *finite field* $GF\left(p\right)$]. Jika $\left(V^{'} == r\right)$, berarti signaturenya benar, sehingga pengguna B mengotentikasi pengguna A dan pengguna B dapat mengkonfirmasi bahwa pengguna A telah benar-benar menyediakan *secret key* yang sama. Kemudian pengguna B menghitung $Y_B = H\left(\beta\right) + u_i$ dan mengirim enkripsi Y_B (proses enkripsi dilakukan dengan menggunakan *secret key* K) untuk pengguna A. Pengguna A mendekripsi paket tersebut dan mendapatkan nilai Y_B .

Untuk mengotentikasi pengguna B, pengguna A akan menghitung $Y_A = H\left(z\right) + u_i$ (dicek $Y_A = Y_B$) dan pengguna A akan memverifikasi nilai Y_A tersebut. Jika keduanya cocok, kemudian pengguna A mengotentikasi pengguna B dan pengguna A dapat mengkonfirmasi bahwa pengguna B benar-benar menyediakan *secret key* yang sama dengan dirinya. Pengguna A kemudian mengirim pengakuannya dengan *session time* T untuk pengguna B. Akhirnya, pengguna A dan pengguna B setuju dengan *session key* K_s, dimana $K_s = H\left(ID_A \| ID_B \| K\right)$. Jika semua langkah tersebut dijalankan dengan benar, kedua belah pihak akan setuju dengan *session key* K_s. Setelah seluruh protokol dijalankan dengan benar, kedua belah pihak diperbolehkan menggunakan K_s untuk mengenkripsi pesan (menggunakan metode ElGamal) dengan *timestamp* untuk setiap sesi komunikasi dalam rangka menciptakan saluran komunikasi yang rahasia. Setelah setiap sesi valid, mala *session key* yang baru akan dibangkitkan.

IV. ANALISIS KEAMANAN

Pada bagian ini, akan dijelaskan aspek keamanan dari protokol mutual autentikasi berbasis HECDSA. Suatu protokol akan dapat dikatakan sebagai protokol autentikasi yang aman apabila memenuhi sifat-sifat berikut :

1) *Man in the middle attack*
   Serangan ini dapat dikatakan sebagai serangan aktif. Pada protokol ini, tidak ada informasi yang beguna untuk mengungkap sebuah kunci rahasia K selama proses berlangsung. Jika penyerang E menyadapat paket pesan yang berisi $\left(Q_B, PU_B\right)$, E menerima PU_B dan Q_B dari B. Namun, hal ini berarti E harus menghitung nilai K. Akan tetapi E tidak dapat menghitung nilai K karena E tidak mengetahui nilai dari d_A atau nilai dari d_B. Permasalahan ini sering disebut dengan *Computational Diffie-Hellman Problem*(CDHP). Sehingga, E tidak akan dapat menghitung nilai K. Artinya, protokol ini tahan terhadap *Man in the Middle attack*.
2) *Small subgroup attack*
   Jika *hyperelliptic curve* C memiliki faktor utama, penyerangan dapat menentukan scalar rahasai modulo dari seluruh prima tersebut dan memulihkan sebagian besar dari rahasia menggunakan *Chinese Remainder Theorem*. Untuk menghindari serangan ini, kita mengecek D yang mempunyai order l dimana l adalah prima. Untuk melakukan pengecekan tersebut, pertama kita mengecek bahwa $\left[l\right]D = 0$ dan menghitung $\left[h\right]D$ untuk $h = c/p_i$, untuk seluruh pembagi bilangan prima p_i dari c dan mengecek hasilnya tidak sama dengan 0.
3) *Known-key attack*
   Dalam protokol ini, diantara pengguna membangkitkan PU_A dan PU_B baru pada setiap sesi baru, dan penambahan kunci rahasia K yang dibangkitkan setiap sesi baru juga. Aspek penting lainnya dari protokol ini adalah *session key* yang dihitung secara independen pada kedua sisi dan dilindungi oleh fungsi hash yang aman. Jadi protokol ini dapat dikatakan aman untuk *known key attack* karena asumsinya *hyperelliptic curve discrete logarithm problem* merupakan sesuatu yang sangat sulit.
4) *Perfect forward secrecy*

PROKASDADIK: Prosiding Kecerdasan Artifisial, Sains Data, dan Pendidikan Masa Depan
Vol. 3, No. 2, (2025) E-ISSN: 3063-5845

Pada *perfect forward secrecy*, bahkan jika ID pengguna mengalami kebocoran, tidak akan pernah seorang penyerang dapat menentukan *session key* untuk sesi terakhir dan melakukan dekripsi. Pada protokol ini, didasarkan pada asumsi bahwa permasalahan logaritma diskrit sangat rumit dan pada nilai kunci rahasia K. Bahkan jika penherang mengetahui nilai Q_B yang benar, penyerang tetap tidak akan bisa menghitung *session key* yang sebelumnya karena K_s merupakan turunan dari K yang dibangkitkan dari nilai d_A dan d_B. Jadi protokol ini memenuhi sifat *perfect forward secrecy*.

5) Replay attack

Replay attack melibatkan penangkapan data secara pasif dan rangkaian sebelum transmisi untuk menunjukkan efek yang tidak sah. Setiap pengguna berbahaya yang tidak sah dapat mengirimkan data duplikat secara berulang kali ke seluruh penerima yang sudah dikirim. Perlindungan terhadap *replay attack* pada protokol ini bergantung nilai-nilai timestamp. Pada protokol ini, setelah setiap kali melakukan *session time* T yang valid dan tidak diketahui oleh pengguna berbahaya, *session key* yang baru akan dibangkitkan untuk proses enkripsi, sehingga *replay attack* tidak mungkin untuk dilakukan..

V. KESIMPULAN

HECC ini juga cocok untuk komunikasi yang aman pada jaringan wireless untuk perangkat dibatasi. HEC ukuran variabelnya hanya merupakan jumlah pecahan dari ukuran variabel EC dan hampir semua protokol standar yang berbasis logaritma diskrit seperti Diffie-Hellman dan EIGamal dapat diterapkan HEC. Protokol Mutual Autentikasi yang berbasis HECDSA dapat digunakan untuk akses yang aman pada perangkat dibatasi yang memungkinkan kedua entitas untuk memverifikasi keaslian masing-masing. Pada protookol ini dapat dilihat bahwa HECC sangat efisien sebagai timing pada perbandingan pembangkitan signature/ proses verifikasinya dengan timing pada ECC yang sudah disediakan. HECC (genus 2) dengan panjang variabel 80-bit memberikan tingkat keamanan yang sama dengan ECC 160-bit. Selain itu, HECC lebih cocok diterapkan pada platform jaringan wireless.

DAFTAR PUSTAKA

[1] R. M. Avanzi, "*Aspects of hyper-elliptic curves over large prime fields in software implementations*",Cryptographic Hardware and Embedded Systems, LNCS vol. 3156, pp. 148-162, 2004.

[2] M. A. Azim and A. Jamalipour. "*An efficient elliptic curve cryptography based authenticated key agreement protocol for wireless LAN security*", International Workshop on High Performance Switching and Routing (HPSR'05), pp. 376-380, 2005.

[3] P. E. Abi-char, A. Mhamed, and B. E. Hassan, "*A secure authenticated key agreement protocol based on elliptic curve cryptography*", IEEE International Symposium on Information Assurance and Security, vol.57, pp. 89-94, 2007.

[4] L. Adleman, J. DeMarrais, and M. Huang, "*A subexponential algorithm for discrete. logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*", Algorithmic Number Theory (ANTS-1), LNCS 877, pp. 28-40, 1994.

[5] M. Aydos, T. Yanık, and C. K. Koc, "*High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor*", IEE Proceedings: Communications, vol.148, no. 5, pp.273–279, 2001.

[6] H. Chan, A. Perrig, and D. Song, "*Random key predistribution schemes for sensor networks*", Proceedings of the IEEE Security and Privacy Symposium, pp. 197-213 , 2003.

[7] D. G. Cantor, "*Computing in the Jacobian of a hyperelliptic curve*", Mathematics of Computation, vol.48, pp. 95-101, 1987.

[8] H. Cohen and G. Frey, "*Handbook of Elliptic and Hyperelliptic Curve Cryptography*", Chapman & Hall/CRC Press, 2006.

[9] K. Chatterjee and D. Gupta, "*Evolution of Hyperelliptic Curve Cryptosystems*", in proceedings of ICDCIT 2010, LNCS 5966, pp.206-211, Springer -Verlag Berlin Heidelberg 2010.

[10] L. Eschenauer and V. Gligor. "*A key management scheme for distributed sensor networks*", Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), pp. 41-47, 2002.

[11] G. Frey and H. Ruck, "*A remark concerning mdivisibility and the discrete logarithm in the divisor class group of curves*", Mathematics of Computation, vol. 62, pp. 865-874, 1994.