Jurnal Ilmiah Sinus (JIS) Vol : 20, No. 2, Juli 2022
ISSN (Print) : 1693-1173 , ISSN (Online): 2548-4028

Modifikasi Tanda Tangan Digital Pada Skema Esign Berbasis Kurva Eliptik

Sa'aadah Sajjana Carita[1*)], Evie Sri Wahyuni[2)]
[1)] Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara
[2)] CPNS pada Badan Siber dan Sandi Negara
[1)] sajjana.carita@bssn.go.id, [2)] eviesriwahyuni018@gmail.com

ABSTRACT

Digital signature has an important role in the digital era, where more and more people join the paperless life. Many cryptographic researchers support digital development by creating safe cryptographic schemes, and one of them is digital signature. The purpose of this paper is to propose a digital signature scheme based on an elliptic curve defined over $\mathbb{Z}_n$, $n = p^2q$, where p and q are private keys of prime numbers. This scheme utilizes the advantages of elliptic curve cryptography in terms of security by using points that satisfy the elliptic curve equation. Additionally, the shorter key size increases the speed, making this scheme faster in signature values generation and verification process. This research was conducted to determine the differences between the modified ESIGN scheme based on elliptic curve and the original ESIGN scheme. Through the experiment, it was found that the process of finding the point on the ring $\mathbb{Z}_n$, with a large n, resulted in a more complex key generation algorithm. However, the selection of two points in this key generation is precomputed. This means the actual signature value generation algorithm took significantly less time than the original. This is one of the advantages of the proposed scheme.

Keywords: *digital signature, elliptic curve cryptography, ESIGN scheme*

I. PENDAHULUAN

Perkembangan teknologi dan kecepatan penyampaian informasi mengakibatkan semakin banyak orang berinteraksi dengan dunia digital. Hal ini dapat dilihat, diantaranya, pada kesadaran keamana siber mahasiswa yang cukup baik yaitu mencapai level "medium"(Kusumaningrum et al., 2022). Pandemi Covid-19 juga mengharuskan banyak sektor, termasuk pendidikan, untuk beralih menjadi *online.* Pembuatan dan distribusi dokumen yang sebelumnya dilakukan dalam bentuk cetak semakin beralih menjadi salinan digital atau *softcopy.* Selain sisi positif seperti penghematan kertas dan kemudahan pengiriman dokumen digital, juga muncul kerentanan keamanan informasi pada dokumen digital, salah satunya mengenai keutuhan isi dokumen serta keabsahan tanda tangan pada dokumen tersebut. Hal ini dapat diatasi dengan penerapan skema tanda tangan digital.

Efficient digital SIGNature (ESIGN) merupakan skema tanda tangan digital perkembangan dari RSA. Skema RSA memiliki kelemahan yaitu kecepatannya yang relatif rendah, karena keamanan RSA berdasarkan pada pemilihan bilangan prima besar p dan q. Hal ini berdampak pada besarnya waktu perhitungan perpangkatan bilangan besar pada pesan dengan modulo kunci publik $n = pq$ yang ukurannya dua kali lipat dari input kunci privat p dan q. Oleh karenanya, skema ESIGN didesain agar memiliki kompleksitas komputasi yang lebih kecil namun tetap setara keamanannya dengan RSA (Kramer, 2017). Meski panjang kunci dan panjang tanda tangan sebanding dengan RSA, skema ESIGN dua puluh kali lebih cepat daripada RSA (Khalique et al., 2010).

Proses penandatanganan ESIGN menghasilkan tanda tangan s dari pesan m, sedangkan proses verifikasi dilakukan dengan memeriksa apakah $s^e \bmod n$, dengan $n = p^2q$, berada pada rentang rentang tertentu yang ditentukan oleh pesan. Kelemahan yang dimiliki skema ini ialah dapat ditemukannya pasangan pesan m dan m', sedemikian sehingga nilai hash $h(m)$ dan $h(m')$ berada pada *high-order* $(\log n)/3$ bit. Dengan

menggunakan *birthday paradox*, musuh dapat menemukan pasangan m dan m' hanya dalam $O(2^{logn/6})$ percobaan. Jika musuh memperoleh nilai tanda tangan yang valid untuk menandatangani pesan m, maka tanda tangan tersebut juga dapat dilakukan pada pesan m' yang berbeda (A. J. Menezes et al., 1997).

Tujuan keamanan dari setiap skema tanda tangan digital adalah agar secara eksistensial tahan terhadap serangan *adaptive-chosen-message-attack* dalam model *oracle* acak di bawah asumsi *approximate e-th root* (A. Menezes et al., 2001). Di dalam model *oracle* acak ini, fungsi *hash* dimodelkan sebagai fungsi acak. Fungsi *hash* yang digunakan beraneka ragam, diantaranya MD5 dan SHA1 seperti yang digunakan dalam system manajemen bukti digital (Pakarti et al., 2021). Fungsi *hash* menjadi bagian dari proses tanda tangan, sehingga musuh tidak dapat mengambil tanda tangan yang valid (Menezes, Oorschot, Paul, & Vanstone, 1997).

Tanda tangan digital terus dikembangkan untuk mengamankan informasi yang termasuk di dalamnya autentikasi, integritas data, dan nir-penyangkalan. Jika seseorang mampu memalsukan tanda tangan, maka perlu adanya mekanisme yang memberikan bukti terjadinya pemalsuan tersebut. Untuk itu, penting untuk terus dilakukan desain, modifikasi, dan analisis skema tanda tangan digital agar memiliki tingkat keamanan yang baik.

Kriptografi kurva eliptik pertama kali diajukan oleh Victor Miller dan Neil Koblitz pada tahun 1985 (Khalique et al., 2010). Keamanan dari kriptografi ini terletak pada kesulitan menemukan nilai k pada persamaan $Q = kP$, dimana Q dan P adalah dua titik pada kurva eliptik. Hingga saat ini, belum ada kelemahan yang signifikan yang ditemukan pada ECC (Gómez Pardo, 2013). Implementasi pada skema tanda tangan digital mampu mengurangi penggunaan sumber daya, yaitu pemrosesan serta ruang penyimpanan yang dibutuhkan (Khalique et al., 2010).

Berdasarkan uraian di atas, penelitian ini akan mengaitkan skema ESIGN dengan kurva eliptik dengan tujuan meningkatkan keamanan serta menghemat sumber daya, supaya skema ini dapat diimplementasikan pada *software* maupun *hardware*. Berdasarkan perubahan yang telah dilakukan, akan dibandingkan performa dari skema ESIGN dengan skema yang telah dimodifikasi berbasis kurva eliptik.

II. TINJAUAN PUSTAKA

Pada bab ini akan diberikan penjelasan singkat mengenai dasar teori penelitian ini, yaitu skema ESIGN dan kurva eliptik berbasis ring $\mathbb{Z}_n$.

2.1. Skema ESIGN

Skema *Efficient digital SIGNature* disingkat dengan ESIGN merupakan skema tanda tangan digital yang keamanannya bergantung pada kesulitan pemfaktoran bilangan bulat (Menezes, Oorschot, Paul, & Vanstone, 1997). Skema ini pertama kali diajukan oleh Okamoto dan Shiraishi untuk menjawab skema tanda tangan digital OSS oleh Ong, Schnorr, dan Shamir yang dinyatakan tidak aman oleh Pollard (A. Menezes et al., 2001). Berdasarkan (Kramer, 2017), (A. Menezes et al., 2001), dan (Okamoto et al., 1993), skema ini lebih efisien dan dua puluh kali lebih cepat daripada skema RSA, dengan panjang kunci dan Panjang tanda tangannya sebanding dengan skema RSA. Skema ini juga memiliki banyak versi setelah ditemukannya kelemahan ketika menggunakan nilai $e \leq 4$ (Kramer, 2017).

Dapat disimpulkan bahwa ESIGN terbukti aman berdasarkan pada AERP atau *approximate e-th root problem* (Kramer, 2017), karena bilangan bulat n yang digunakan adalah $n = p^2q$ dengan p dan q merupakan bilangan prima yang memiliki ukutan panjang bit yang sama (A. Menezes et al., 2001). Selain itu skema ini juga disebut efisien jika

 DOI : https://doi.org/10.30646/sinus.v20i2.625

digunakan untuk tanda tangan digital dan aplikasi masa depan lainnya (A. Menezes et al., 2001).

Skema ini, mengacu pada (Okamoto et al., 1993) dan (Okamoto, Tatsuaki; Shiraishi, 1985), menggunakan pertidaksamaan kongruensi kuadratik serta *one-way hash function* $h: \{0,1\}^* \to \mathbb{Z}_n$. Pertidaksamaan pada skema ESIGN digunakan untuk memverifikasikan nilai tanda tangan digital yang diterima. Skema ini terdiri atas tiga algoritma, yaitu pembangkitan kunci, pembangkitan nilai tanda tangan, dan verifikasi.

a. Pembangkitan kunci

Algoritma ini dilakukan oleh setiap entitas A untuk membangkitkan kunci, sebagai berikut:

a) Entitas A akan memilih bilangan prima acak p dan q, sedemikian sehingga $p \geq q$ dan p, q memiliki panjang bit yang sama (r bit).
b) Hitung nilai $n = p^2 q$, jika panjang $n \neq 3r$, pilih p atau q yang berbeda.
c) Pilihlah bilangan bulat $e \geq 4$.
d) Entitas A akan memperoleh kunci publik (n, e) dan kunci privat (p, q).

b. Pembangkitan nilai tanda tangan

Algoritma ini masih dilakukan oleh entitas A untuk mendatangani pesan m, sebagai berikut.

a) Hitung $v = h(m)$.
b) Pilih bilangan acak $x, 0 \leq x < pq$.
c) Hitung $w = \left\lceil \frac{(v - x^e) mod\ n}{pq} \right\rceil$ dan $y = w \cdot (ex^{e-1})^{-1}\ mod\ p$.
d) Hitung $s = x + ypq\ mod\ n$.
e) Nilai tanda tangan digital A untuk pesan m adalah s.

c. Verifikasi

Algorirme ini dilakukan oleh entitas B untuk memverifikasikan nilai tanda tangan digital s pada m yang diterima dari entitas A.

a) Telah diperoleh kunci publik entitas A (n, e).
b) Hitung $u = s^e mod\ n$ dan $z = h(m)$. Jika $z \leq u \leq z + 2^{\left\lceil \frac{2}{3} \lg n \right\rceil}$ tanda tangan diterima, sedangkan lainnya ditolak.

2.2. Kurva Eliptik atas Ring $\mathbb{Z}_n$

Elliptic Curve Cryptography (ECC) adalah algoritma kunci publik yang dikembangkan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985 (Ahlswede, 2016). Koblitz dan Miller mengklaim bahwa panjang kunci yang digunakan pada ECC lebih pendek daripada kunci yang digunakan pada RSA, namun dengan tingkat keamanan yang relatif sama. Kondisi ini memberikan keuntungan pada memori dan komputasi yang lebih sedikit, dengan perbandingan kunci ECC sepanjang 160-bit menyediakan keamanan yang sama dengan 1024-bit kunci RSA.

Penjelasan kurva eliptik ini diolah dari (Silverman, 2009) kecuali disebutkan lain.

Definisi 1

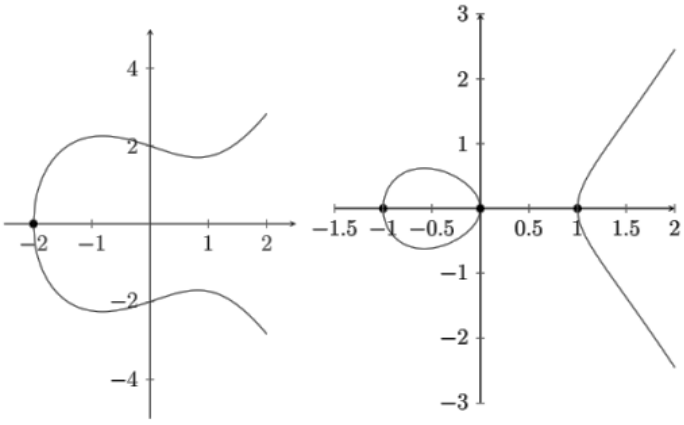
Untuk bilangan prima $p \neq 2,3$, kurva eliptik $E(\mathbb{Z}_p)$ adalah himpunan titik-titik $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ yang memenuhi

$$y^2 = x^3 + Ax + B, \qquad (1)$$

dengan $A, B \in \mathbb{Z}_p$ dan $4A^3 + 27B^2 \neq 0$, ditambahkan "titik di takhingga" $\mathcal{O}$ yang bersifat sebagai identitas terhadap penjumlahan titik.

Berikut dijelaskan penjumlahan titik pada kurva eliptik. Gambar pada bagian ini diperoleh dari (ISARA, 2019).

Pada persamaan (1), terdapat 1 atau 3 nilai real yang mungkin untuk x, sehingga terdapat dua kemungkinan sketsa grafik kurva eliptik, yang diberikan pada Gambar 1.



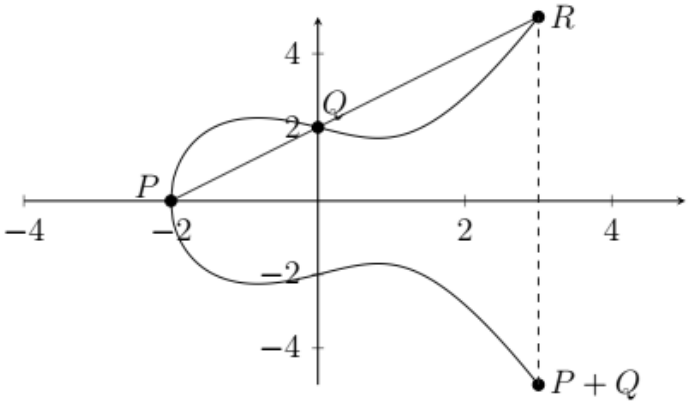
Gambar 1. Sketsa grafik kurva eliptik

Penjumlahan dua titik $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ menghasilkan titik $P + Q = (x_3, y_3)$ dengan perhitungan yang dapat dibagi dalam 4 kasus.

Kasus 1. $x_1 \neq x_2$ (diilustrasikan pada Gambar 2)

Tarik garis melalui P dan Q dan memotong kurva E kembali di titik R. Titik $P + Q$ adalah pencerminan dari R terhadap sumbu-x. Rumus eksplisitnya diberikan pada persamaan (2).

$$x_3 = m^2 - (x_1 + x_2),\ y_3 = m(x_3 - x_1) + y_1, \text{ dengan } m = \frac{y_2 - y_1}{x_2 - x_1} \qquad (2)$$



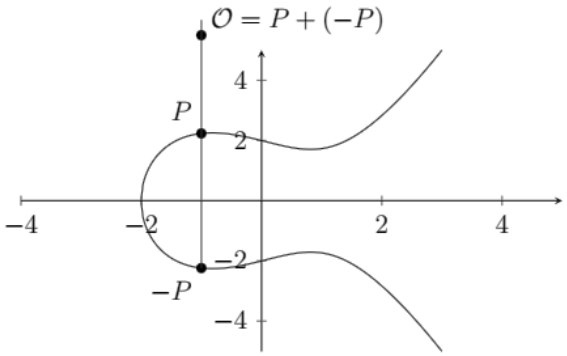
Gambar 2. Kasus 1 penjumlahan titik

Kasus 2. $x_1 = x_2, y_1 = -y_2$ (diilustrasikan pada Gambar 3)

Pada kasus P_1 dan P_2 saling bernegasi. Garis lurus yang menghubungkan kedua titik tersebut vertikal, sehingga

$$P_1 + P_2 = \mathcal{O} \qquad (3)$$

 DOI : https://doi.org/10.30646/sinus.v20i2.625

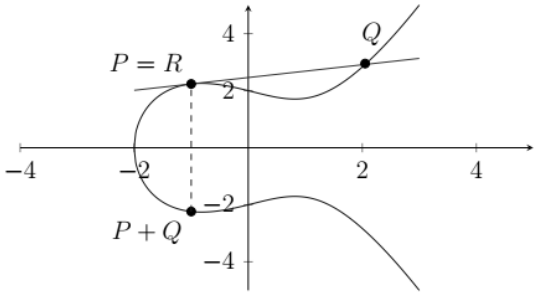


Gambar 3. Kasus 2 penjumlahan titik

Kasus 3. $x_1 = x_2, y_1 = y_2$ dengan $y_1 \neq 0$ (diilustrasikan pada Gambar 4)

Pada kasus ini, titik $P_1 = P_2$. Garis yang ditarik berupa garis singgung di titik P_1 dan $P_1 + P_2 = 2P_1 = (x_3, y_3)$ dapat diperoleh dengan persamaan (4).

$$x_3 = m^2 - 2x_1, y_3 = -m(x_3 - x_1) - y_1, \text{ dengan } m = \frac{3x_1^2 + A}{2y_1} \qquad (4)$$

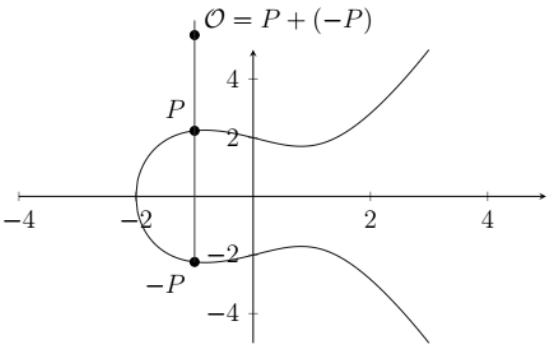


Gambar 4. Kasus 3 penjumlahan titik

Kasus 4. $x_1 = x_2, y_1 = y_2 = 0$ (diilustrasikan pada Gambar 5)

Pada kasus ini, garis yang ditarik berupa garis singgung di titik P_1 dan merupakan garis vertikal, sehingga seperti pada kasus 2,

$$P_1 + P_2 = 2P_1 = \mathcal{O} \qquad (5)$$



Gambar 5. Kasus 4 penjumlahan titik

Dari kasus 1 hingga 4, dapat ditunjukkan bahwa titik-titik pada kurva eliptik membentuk suatu grup komutatif terhadap penjumlahan. Bukti pernyataan ini terdapat pada (Silverman, 2009). Berikut didefinisikan perkalian bilangan bulat taknegatif dengan titik di kurva eliptik.

Definisi 2

Misalkan P titik pada kurva eliptik E, maka untuk setiap bilangan bulat k, titik kP didefinisikan pada persamaan (6)

$$\underbrace{P + P + \cdots P}_{k} \quad (6)$$

Jika diberikan sebarang titik P dan titik $Q = kP$, sangat sulit untuk menemukan nilai k (Hoffstein et al., 2014), (Blumenfeld, 2011). Masalah matematik ini disebut *Elliptic Curve Discrete Logarithm Problem* (ECDLP) dan digunakan untuk menjamin kesulitan memecahkan kriptografi kurva eliptik.

Definisi-definisi di atas juga berlaku untuk kurva eliptik $\boldsymbol{E}$ atas ring $\mathbb{Z}_{\boldsymbol{n}}$. Untuk ring $\mathbb{Z}_n$, perlu diperhatikan dari Persamaan (2) dan (4), penjumlahan titik hanya berlaku saat nilai $x_2 - x_1$ dan y_1 saling prima dengan $n = p^2q$.

III. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini yaitu telaah kepustakaan dan metode eksperimen, dengan tahapan sebagai berikut.

1. Telaah kepustakaan
   Telaah kepustakaan dilakukan dengan cara mempelajari teori-teori terkait penelitian dengan melalui sumber berupa buku, *paper*, disertasi, tesis, skripsi, sumber dari internet maupun sumber pendukung lainnya. Teori-teori yang dipelajari antara lain skema ESIGN, kriptografi kurva eliptik, dan kompleksitas waktu algoritma.
2. Perancangan modifikasi algoritma
   Pada tahap ini dilakukan penelitian modifikasi ESIGN berdasarkan studi literatur yang telah dilakukan sebelumnya dan melakukan pemodelan skema modifikasi ke dalam program untuk dieksekusi. Tahap ini meliputi pembuktian matematis dari formula yang digunakan.
3. Pengujian
   Pada tahap pengujian, akan dilakukan simulasi algoritma ESIGN dan modifikasi yang telah dirancang sebelumnya. Simulasi dilakukan pada perangkat *All-in-One Desktop* Dell OptiPlex 7480 Intel Core i7-10700. Data yang diperoleh adalah data kuantitatif berupa waktu eksekusi dari tiap input yang telah ditentukan.
4. Analisis
   Analisis yang dilakukan ialah analisis teoritis modifikasi algoritma serta perbandingan durasi eksekusi dan kompleksitas waktu skema ESIGN milik Okamoto *et al*. dengan skema modifikasi ESIGN berbasis kurva eliptik.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas mengenai modifikasi skema ESIGN berbasis kurva eliptik, pembuktian matematis skema modfikasi, implementasi skema modifikasi, serta perbandingan durasi eksekusi dan kompleksitas waktu antara ESIGN dan modifikasi ESIGN berbasis kurva eliptik yang dirancang.

4.1 Modifikasi Skema ESIGN Berbasis Kurva Eliptik

Pada penelitian ini dilakukan skema modifikasi ESIGN milik Okamoto dan Shiraishi (1985) yaitu dengan berbasis kurva eliptik atas ring $\mathbb{Z}_n$. Pada dasarnya modifikasi ini merupakan perluasan skema yang dilakukan Okamoto dengan menggunakan fungsi rasional (Okamoto, Fujioka, & Fujisaki, 1993). Penelitian ini menggunakan perluasan fungsi rasional ini sebagai dasar untuk pengimplementasian kriptografi kurva eliptik ke dalam skema ESIGN pertama kali. Skema ini menggunakan pemilihan acak dua titik P dan Q yang telah memenuhi persamaan kurva eliptik. Kedua titik ini dijadikan bagian dari

 DOI : https://doi.org/10.30646/sinus.v20i2.625

fungsi rasional bersamaan parameter k dan t yang juga diiput acak dalam fungsi rasional $f(t) = \frac{(kt^2+at+b)}{(x_2-x_1)(y_2-y_1)}$. Dapat diturunkan fungsi tersebut menjadi $f'(t) = \frac{2kt+a}{(x_2-x_1)(y_2-y_1)}$. Karena skema ini menggunakan modulo n, dengan $n = p^2q$, maka $f(t)$ dan $f'(t)$ haruslah tidak membagi habis modulo p dan q sehingga $f(t)$ dan $f'(t)$ tidak akan membagi habis n. Skema ini tersusun atas tiga algoritma yang terdiri dari pembangkitan kunci, pembangkitan nilai tanda tangan dan verifikasi.

4.1.1 Pembangkitan Kunci

Proses pembangkitan kunci ini dilakukan oleh setiap entitas A. Hasil akhir dari proses ini ialah parameter umum yang akan digunakan dalam skema tanda tangan digital berupa kunci publik dan kunci privat, yang masing-masing digunakan dalam proses tanda tangan dan verifikasi. Pembangkitan kunci ditunjukkan pada Algoritma 1.

Algoritma 1 Pembangkitan Kunci
Input: Bilangan prima p dan q dengan $p > q$, serta persamaan kurva $a, b \in \mathbb{Z}_n$ sedemikian sehingga $\gcd(4a^3 + 27b^2, n) = 1$
***Output*:** Kunci publik (n, k, a, b, P, Q) dan kunci privat (p, q)
a. Hitung $n = p^2q$. b. Pilih sebarang titik $P(x_1, y_1), Q(x_2, y_2) \in E_{a,b}(\mathbb{Z}_n)$. c. Pilih $k \in \mathbb{Z}_p^*$

Parameter yang dibutuhkan untuk membangkitkan nilai kunci adalah bilangan n yang diperoleh dari dua bilangan prima sesuai operasi pada Algoritma 1. Bilangan n akan digunakan sebagai modulus dalam operasi penjumlahan dan perkalian bilangan serta syarat penentuan nilai a dan b sedemikian sehingga $\gcd(4a^3 + 27b^2, n) = 1$. Kedua titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$ dipilih acak setelah persamaan kurva eliptik terpenuhi. Kedua titik tersebut akan digunakan dalam fungsi $f(t)$ pada algoritma selanjutnya, dimana $f(t) = \frac{(kt^2+at+b)}{(x_2-x_1)(y_2-y_1)}$, sehingga $x_2 \neq x_1, y_2 \neq y_1, P \neq \pm Q$.

4.1.2 Pembangkitan Nilai Tanda Tangan

Pada algoritma ini pesan yang akan ditandatangani perlu di-*hash* terlebih dahulu oleh entitas A. Fungsi *hash* di dalam skema tanda tangan digital digunakan untuk integritas data. Pesan *hash* dan nilai t sebagai nilai input untuk memperoleh nilai tanda tangan berupa $(s, h(m))$. Proses pembangkitan tanda tangan ditunjukkan pada Algoritma 2 sebagai berikut.

Algoritma 2 Pembangkitan Nilai Tanda Tangan
Input: Pesan *hash* $h(m)$, Nilai $t \in \mathbb{Z}_{pq}^*$.
***Output*:** Nilai tanda tangan $(s, h(m))$
a. Hitung pesan $m = h(m) \in \mathbb{Z}_n$. b. Hitung $w = \left\lceil \frac{h(m) - (f(t) \bmod n)}{pq} \right\rceil = \left\lceil \frac{h(m) - (\frac{(kt^2+at+b)}{(x_2-x_1)(y_2-y_1)} \bmod n)}{pq} \right\rceil$. c. Hitung $u = \frac{w}{f'(t)} mod\ p = w\ \frac{(x_2-x_1)(y_2-y_1)}{(2kt+a)}\ mod\ p$. d. Hitung $s = t + upq\ mod\ n$.

Pesan $\boldsymbol{h(m)}$ tidak bergantung pada parameter lainnya, sehingga pada tahap awal proses pembangkitan nilai tanda tangan bisa dilakukan terlebih dahulu tanpa pesan *hash* (*pre-computed*). Hal ini yang membuat proses pembangkitan nilai tanda tangan lebih cepat. Dalam memilih parameter $\boldsymbol{t}$ terdapat beberapa perhatian, yaitu jika menemui kondisi sebagai berikut, pilih acak nilai $\boldsymbol{t}$ lain dengan $\boldsymbol{t} \in \mathbb{Z}_{\boldsymbol{pq}}^{*}$: (1) $\boldsymbol{f(t)\ mod\ p} = \infty$, (2) $\boldsymbol{f(t)\ mod\ q} = \infty$, (3) $\boldsymbol{f(t)\ mod\ p} = \boldsymbol{0}$, (4) $\boldsymbol{f(t)\ mod\ q} = \boldsymbol{0}$, (5) $\boldsymbol{f'(t)\ mod\ p} = \infty$, (6) $\boldsymbol{f'(t)\ mod\ q} = \infty$, (7) $\boldsymbol{f'(t)\ mod\ p} = \boldsymbol{0}$, (8) $\boldsymbol{f'(t)\ mod\ q} = \boldsymbol{0}$. Kondisi diatas ditentukan karena algoritma ini menggunakan modulus $\boldsymbol{n}$, dengan $\boldsymbol{n} = \boldsymbol{p^2 q}$. Informasi dalam algoritma ini hanya diketahui oleh pihak penandatangan untuk mencegah adanya pemalsuan maupun penyangkalan pada tanda tangan.

3.1.3 Verifikasi Nilai Tanda Tangan

Pada bagian ini akan dijelaskan mengenai proses verifikasi nilai tanda tangan yang valid. Hasil akhir dari proses verifkasi adalah memastikan jika nilai tanda tangan (s) disubstitusikan ke dalam fungsi $f(s)$ berada dalam rentang yang telah ditentukan. Proses ini dilakukan oleh entitas B yang telah mendapatkan kunci publik serta nilai tanda tangan. Proses verifikasi nilai tanda tangan ditunjukkan pada Algoritma 3 sebagai berikut.

Algoritma 3 Verifikasi Nilai Tanda Tangan

Input: Kunci publik (n, k, a, b, P, Q), dan nilai tanda tangan (s, m)

***Output*:** validasi tanda tangan

a. Hitung $h(m) \leq f(s)\ mod\ n < h(m) + 2^{\left\lceil \frac{2}{3} \lg n \right\rceil}$, maka, $h(m) \leq \frac{(ks^2+as+b)}{(x_2-x_1)(y_2-y_1)}\ mod\ n < h(m) + 2^{\left\lceil \frac{2}{3} \lg n \right\rceil}$.
b. Jika $f(s)$ atas $\mathbb{Z}_n$ berada dalam rentang tersebut, tanda tangan digital diterima, jika tidak maka ditolak.

4.2 Pembuktian Matematis Modifikasi Skema ESIGN Berbasis Kurva Eliptik

Pembuktian matematis ini dilakukan untuk memastikan bahwa skema modifikasi yang telah dirancang dapat berjalan dengan baik. Berikut dilakukan penurunan fungsi dari persamaan algoritma verifikasi. Penurunan fungsi ini akan menunjukkan bahwa nilai yang dibangkitkan pada proses pembangkitan nilai tanda tangan bernilai valid. Selain pembuktian matematis, skema modifikasi ini juga telah memenuhi sifat-sifat skema tanda tangan digital pada (Stallings, 2017).

Dipilih, $f(s) = \frac{(kt^2+at+b)}{(x_2-x_1)(y_2-y_1)}$, yang merupakan fungsi analitik dan tidak memiliki titik singular di $[0, n)$. Diketahui, untuk sebarang $t \in \mathbb{Z}_{pq}^{*} \subseteq [0, n)$ dan $t + upq \in [0, n)$. Berdasarkan [6], Ekspansi Taylor dari $f(t + upq)$ adalah :

$$f(t + upq)\ mod\ n = f(t) + f^{(1)}(t)upq + \left(\frac{f^{(2)}(t)}{2}\right)(upq)^2 + \cdots\ \ mod\ n$$

$$= f(t) + f^{(1)}(t)upq + (upq)^2\left(\frac{f^{(2)}(t)}{2} + \cdots\right) mod\ n$$

$$= f(t) + f^{(1)}(t)upq\ mod\ n.$$

Karena $w = f^{(1)}(t)\ u\ mod\ p$, diperoleh $f(t + upq)\ mod\ n = f(t) + wpq\ mod\ n$. Diketahui juga $w = \left\lceil \frac{h(m) - (f(t)\ atas\ \mathbb{Z}_n)}{pq} \right\rceil$, maka $wpq = h(m) - (f(t)\ mod\ n) + \gamma$ dengan $0 \leq \gamma < pq$. Jadi

 DOI : https://doi.org/10.30646/sinus.v20i2.625

$$f(t+upq)\ mod\ n = f(t) + h(m) - (f(t)\ mod\ n) + \gamma\ mod\ n = h(m) + \gamma\ mod\ n.$$

Untuk $0 \le h(m) < n - pq$,

$$h(m) \le h(m) + \gamma\ mod\ n = h(m) + \gamma < h(m) + pq$$
$$h(m) \le f(t+upq) < h(m) + pq$$
$$h(m) \le f(s) < h(m) + pq < h(m) + 2^{\left\lceil \frac{2}{3}\lg n \right\rceil}, \quad (7)$$

maka $f(s)$ berada dalam rentang yang ditentukan, dan tanda tangan bernilai valid.

Berikut pembuktian untuk $h(m) + pq < h(m) + 2^{\left\lceil \frac{2}{3}\lg n \right\rceil}$. Diketahui jika $q < p$, maka

$$q^{\frac{1}{3}} < p^{\frac{1}{3}} \Leftrightarrow \frac{q}{q^{\frac{2}{3}}} < \frac{p^{\frac{4}{3}}}{p}$$
$$pq < p^{\frac{4}{3}}q^{\frac{2}{3}} = (p^2q)^{\frac{2}{3}} = n^{\frac{2}{3}} = 2^{\log n^{\frac{2}{3}}} = 2^{\frac{2}{3}\log n} < 2^{\left\lceil \frac{2}{3}\lg n \right\rceil},$$

diperoleh $pq < 2^{\left\lceil \frac{2}{3}\lg n \right\rceil}$. Oleh karena itu, dapat dibuktikan bahwa $h(m)pq < h(m) + 2^{\left\lceil \frac{2}{3}\lg n \right\rceil}$, sehingga pertidaksamaan (7) terbukti.

4.3 Implementasi Modifikasi ESIGN Berbasis Kurva Eliptik

Implementasi yang dilakukan pada algoritma tanda tangan digital dengan perubahan berbasis kurva eliptik ini ditunjukkan dengan proses penghitungan menggunakan contoh bilangan sederhana.

1. Pembangkitan Kunci
   a. Dipilih bilangan prima $p = 43$ dan $q = 31$.
   b. Menghitung $n = p^2q = 57319$.
   c. Dipilih persaman kurva eliptik $: y^2 : x^3 + 6x + 8\ (mod\ 57319)$, $\gcd(4a^3 + 27b^2, n) = 1$.
   d. Dipilih titik $(48226\ ,47159)$, $Q(31862\ ,35218) \in E_{12,9}(mod\ 57319)$.
   e. Dipilih $k = 219$.
   f. Kunci publik yang dihasilkan adalah $n = 57319, a = 6, b = 8$, $P(48226\ ,47159)$, dan $Q(31862\ ,35218)$. Kunci privat $p = 43$ dan q= 31.
2. Pembangkitan Nilai Tanda Tangan
   a. Hitung pesan ke dalam fungsi *hash*, $m = h(m) = 8249\ (mod\ 57319)$.
   b. Dipilih $t = 1273 \in \mathbb{Z}_{1333}$, dengan t sudah memenuhi syarat yang ditentukan.
   c. Menghitung $w = \lceil (m\ -(\ f(t)\ atas\ \mathbb{Z}\_n)\ )/pq \rceil = \lceil -28.720 \rceil = -28$
   d. Menghitung $u = \frac{w}{f'(t)} = 24\ (mod\ 43)$
   e. Menghitung $s = t + upq\ (mod\ n) = 33265\ (mod\ 57319)$. Diperoleh nilai tanda tangan adalah $(s, m) = (33265\ ,\ 8247)$.
3. Proses verifikasi
   a. Menghitung $f(s)$, dengan menggunakan nilai tanda tangan s yang diterima;

$$f(s) = \frac{(ks^2 + as + b)}{(x_2 - x_1)(y_2 - y_1)} = \frac{219 \times (33265)^2 + 6 \times 33265 + 8}{(31862 - 48226) \times (35218 - 47159)}$$
$$= 7663\ (mod\ 57319)$$

$h(m) = 8247$, dan $h(m) + 2^{\left\lceil \frac{2}{3}\lg n \right\rceil} = 8247 + 4096 = 10528$.

   b. Diketahui $8247 \le 7663 \le 10528$, sehingga tanda tangan diterima.

4.4 Perbandingan Kompleksitas dan Durasi Eksekusi Algoritma

Perhitungan kompleksitas mengacu pada (Munir, 2015). Fungsi yang dimanfaatkan dalam algoritma serta kompleksitas waktu asimtotiknya diberikan pada Tabel 1:

Tabel 1. Algoritma dan Kompleksitas Asimptotiknya

Algoritma	**Kompleksitas waktu asimptotik**
Extended Euclidean	$O(n)$
Greatest Common Divisor	$O(n)$
Pencarian titik	$O(n)$

Perbandingan kompleksitas algoritma ESIGN dan modifikasinya berbasis kurva eliptik seperti pada Tabel 2.

Tabel 2. Perbandingan Kompleksitas Algoritma ESIGN dan Modifikasinya

Algoritma	**ESIGN**	**Modifikasi Skema ESIGN Berbasis Kurva Eliptik**
Pembangkitan Kunci	$O(n)$	$O(n^2)$
Pembangkitan Nilai Tanda Tangan	$O(n)$	$O(n)$
Verifikasi	$O(n)$	$O(n)$

Berdasarkan Tabel 2, algortime modifikasi memiliki kompleksitas yang lebih besar, yaitu $O(n^2)$, pada proses pembangkitan kunci, tetapi tidak mengubah kompleksitas pada proses lain. Kompleksitas yang besar pada pembangkitan kunci ini disebabkan oleh bagian pemilihan titik pada kurva eliptik, yang dilakukan untuk menambah keamanan skema ESIGN terhadap pemalsuan tanda tangan.

Pada Tabel 3. diberikan perbandingan durasi eksekusi algoritma ESIGN dan modifikasinya. Eksekusi dilakukan pada 5 (lima) ukuran input n, yairu 8-bit, 12-bit, 16-bit, 20-bit, dan 24-bit.

Tabel 3. Durasi Eksekusi Algoritma ESIGN dan Modifikasinya

Ukuran Modulus n (bit)	**Durasi Eksekusi (detik)**					
	ESIGN			MODIFIKASI SKEMA ESIGN		
	Pembangkitan Kunci	Pembangkitan Nilai Tanda Tangan	Verifikasi	Pembangkitan Kunci	Pembangkitan Nilai Tanda Tangan	Verifikasi
8	0.016000	0.0	0.014999	0.030999	0.0	0.0
12	0.016000	0.0	0.016000	0.062000	0.0	0.0
16	0.014999	0.031000	0.015999	0.125000	0.0	0.015000
20	0.015000	1.921000	1.391000	3.701999	0.0	0.015000
24	0.014999	60.486000	93.72799	135.1570	0.0	0.0

Dari Tabel 3, terlihat bahwa modifikasi yang dilakukan memperlambat proses pembangkitan kunci. Namun, bagian pemilihan dua titik pada kurva eliptik pada proses ini dapat dilakukan sebelum input pesan (*precomputated*), sehingga dapat secara signifikan mempersingkat waktu pembangkitan kunci. Juga, dapat dilihat bahwa proses pembangkitan dan verifikasi tanda tangan pada skema modifikasi jauh lebih singkat daripada skema ESIGN asli.

 DOI : https://doi.org/10.30646/sinus.v20i2.625

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan pertama adalah, kriptografi kurva eliptik dapat diterapkan pada skema ESIGN. Terdapat beberapa perhatian dalam pemilihan persamaan kurva eliptik serta parameter pemilihan titik yang digunakan agar dapat dijalankan pada fungsi $f(t)$ di dalam skema yang diajukan dalam penulisan ini. Kedua, dari perbandingan durasi eksekusi dan kompleksitas, dapat disimpulkan bahwa algoritma pembangkitan kunci skema ESIGN lebih unggul. Namun, pada algoritma pembangkitan nilai tanda tangan dan verifikasinya, modifikasi skema ESIGN menunjukkan hasil yang lebih baik.

5.2 Saran

Saran yang dapat diberikan untuk penelitian selanjutnya adalah pertama, perlu dilakukan kajian keamanan serta serangan terhadap skema modifikasi, khususnya serangan yang sama dengan skema ESIGN, yaitu menemukan dua pesan berbeda yang memiliki tanda tanggan yang sama. Kedua, dapat dilakukan optimalisasi pada skema modifikasi terutama bagian pemilihan dua titik kurva eliptik pada pembangkitan kunci, agar algoritma tersebut menjadi semakin efisien.

DAFTAR PUSTAKA

Ahlswede, R. (2016). Hiding data - selected topics : Rudolf Ahlswede's lectures on information theory 3. In A. Ahlswede, I. Althöfer, C. Deppe, & U. Tamm (Eds.), *Foundations in Signal Processing, Communications and Networking*. Springer. https://doi.org/10.1007/978-3-319-31515-7

Blumenfeld, A. (2011). Discrete Logarithms on Elliptic Curves. *Journal Rose-Hulman Undergraduate Mathematics Journal*, *12*(1), 30–57.

Gómez Pardo, J. L. (2013). *Introduction to Cryptography with Maple*. Springer-Verlag GmbH. https://doi.org/10.1007/978-3-642-32166-5_11

Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). *Introduction to Mathematical Cryptography* (2nd ed.). Springer. https://doi.org/10.1007/978-81-322-1599-8_12

ISARA. (2019). *Isogeny-Based Cryptography Tutorial*. https://www.isara.com/resource-center/isogeny-based-cryptography-tutorial.html

Khalique, A., Singh, K., & Sood, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal of Computer Applications*, *2*(2), 21–27. https://doi.org/http://dx.doi.org/10.5120/631-876

Kramer, R. A. (2017). *A Survey of ESIGN: State of the Art and Proof of Security* (Issue Winter Term).

Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, *20*(1), 69. https://doi.org/10.30646/sinus.v20i1.586

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. Taylor & Francis.

Menezes, A., Qu, M., Stinson, D., & Wang, Y. (2001). Evaluation of Security Level of Cryptography : ESIGN Signature Scheme. In *CRYPTREC Project*.

Munir, R. (2015). *Kompleksitas Algoritma*. Institut Teknologi Bandung.

Okamoto, Tatsuaki; Shiraishi, A. (1985). A Fast Signature Scheme Based on Quadratic Inequalities. *1985 IEEE Symposium on Security and Privacy*, 123–132.

Okamoto, T., Fujioka, A., & Fujisaki, E. (1993). An Efficient Digital Signature Scheme Based on an Elliptic Curve over the Ring Zn. In E. F. Brickell (Ed.), *Advances in Cryptography-CRYPTO'92* (pp. 54–65). Springer. https://doi.org/https://doi.org/10.1007/3-540-48071-4_4

Pakarti, M. B., Fudholi, D. H., & Prayudi, Y. (2021). Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Pada Masa Pandemi Covid-19. *Jurnal Ilmiah SINUS*, *19*(1), 27. https://doi.org/10.30646/sinus.v19i1.502

Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Springer. https://doi.org/10.1007/978-0-387-09494-6

Stallings, W. (2017). *Cryptography and Network Security Principles and Practice 7th Edition*. Pearson Education Limited.