Analisis Stabilitas dan Konvergensi Benchmark Kriptografi pada Skema CBAS Menggunakan MIRACL Core

Asroni✉
Universitas Muhammadiyah Yogyakarta,

✉Corresponding Author: asroni@umy.ac.id

ABSTRAK

Perkembangan skema kriptografi modern, khususnya *Certificate-Based Aggregate Signature* (CBAS), menuntut evaluasi kinerja yang akurat terhadap operasi dasar kriptografi yang digunakan, seperti *bilinear pairing*, eksponensiasi modular, dan operasi kurva eliptik. Dalam praktiknya, banyak penelitian melakukan pengukuran waktu komputasi dengan jumlah iterasi tertentu tanpa mengevaluasi stabilitas dan konvergensi hasil benchmarking tersebut. Hal ini berpotensi menghasilkan estimasi biaya komputasi yang kurang akurat, terutama dalam analisis keamanan dan efisiensi skema kriptografi berbasis pairing. Permasalahan utama dalam penelitian ini adalah bagaimana menentukan apakah jumlah iterasi benchmarking (N) yang digunakan sudah cukup untuk menghasilkan nilai waktu eksekusi yang stabil dan representatif. Secara khusus, penelitian ini bertujuan untuk menganalisis stabilitas dan konvergensi hasil pengukuran waktu operasi kriptografi pada skema CBAS dengan membandingkan variasi jumlah iterasi yang berbeda.Metode yang digunakan dalam penelitian ini adalah pendekatan eksperimental berbasis implementasi menggunakan *MIRACL Core library*. Operasi kriptografi yang diuji meliputi operasi berbasis pairing pada kurva BLS12381, seperti *bilinear pairing* (T_bpo), eksponensiasi pada grup target (T_pbsm), dan multiplikasi pada grup target (T_pbpa), serta operasi aritmetika medan hingga seperti invers modular (T_rc) dan eksponensiasi modular (T_meo dan T_meo*). Selain itu, dilakukan juga pengujian pada kurva eliptik konvensional NIST256 untuk operasi perkalian skalar (T_smec) dan penjumlahan titik (T_paec). Pengukuran waktu dilakukan menggunakan fungsi *high-resolution timer* dengan dua variasi jumlah iterasi, yaitu N=1000 dan N=5000, serta dilengkapi dengan fase *warm-up* untuk mengurangi efek *cold start*. Hasil eksperimen menunjukkan bahwa seluruh operasi kriptografi yang diuji memiliki tingkat stabilitas yang sangat tinggi terhadap variasi jumlah iterasi. Nilai waktu eksekusi rata-rata untuk operasi pairing (T_bpo) pada BLS12381 sebesar 1.2527 ms untuk N=1000 dan 1.2539 ms untuk N=5000, menunjukkan perbedaan yang sangat kecil. Hal serupa juga terlihat pada operasi lainnya, seperti T_pbsm (0.8420 ms vs 0.8435 ms), T_meo* (3.9391 ms vs 3.9304 ms), dan T_smec (0.1816 ms vs 0.1818 ms). Perbedaan yang sangat kecil ini mengindikasikan bahwa hasil benchmarking telah mencapai kondisi konvergen bahkan pada jumlah iterasi yang relatif kecil (N=1000). Dari hasil tersebut, dapat disimpulkan bahwa peningkatan jumlah iterasi dari 1000 menjadi 5000 tidak memberikan perubahan signifikan terhadap nilai rata-rata waktu eksekusi. Dengan demikian, jumlah iterasi yang lebih kecil sudah cukup untuk menghasilkan estimasi kinerja yang stabil dan akurat. Temuan ini memberikan kontribusi penting dalam metodologi benchmarking kriptografi, khususnya dalam konteks evaluasi skema CBAS, karena dapat mengurangi waktu eksperimen tanpa mengorbankan akurasi hasil.

Kata kunci : benchmark kriptografi, CBAS, MIRACL Core, BLS12381, konvergensi

A. Pendahuluan

Perkembangan teknologi kriptografi modern mendorong penggunaan skema tanda tangan digital yang tidak hanya aman, tetapi juga efisien dalam hal komputasi. Salah satu skema yang banyak dikembangkan adalah *Certificate-Based Aggregate Signature* (CBAS), yang memungkinkan penggabungan beberapa tanda tangan menjadi satu representasi yang

ringkas tanpa mengorbankan aspek keamanan. Skema ini banyak memanfaatkan operasi kriptografi berbasis pairing, khususnya pada kurva *BLS12381*, yang dikenal memiliki tingkat keamanan tinggi namun dengan biaya komputasi yang relatif besar [1].

Dalam implementasi praktis, evaluasi kinerja dari operasi kriptografi menjadi aspek yang sangat penting, terutama untuk memastikan bahwa skema yang diusulkan dapat diterapkan pada sistem nyata, seperti Internet of Things (IoT) dan sistem terdistribusi. Evaluasi ini umumnya dilakukan melalui proses benchmarking dengan mengukur waktu eksekusi dari operasi dasar seperti *bilinear pairing*, eksponensiasi modular, serta operasi pada kurva eliptik. Penelitian sebelumnya menunjukkan bahwa operasi pairing memiliki kompleksitas yang jauh lebih tinggi dibandingkan operasi kurva eliptik konvensional, sehingga menjadi bottleneck utama dalam sistem berbasis pairing [2].

Namun demikian, sebagian besar penelitian hanya menggunakan jumlah iterasi tertentu tanpa mempertimbangkan apakah hasil pengukuran tersebut telah mencapai kondisi stabil atau belum. Padahal, akurasi hasil benchmarking sangat bergantung pada jumlah iterasi yang digunakan. Studi terbaru dalam bidang evaluasi performa kriptografi menunjukkan bahwa stabilitas hasil pengukuran sangat dipengaruhi oleh faktor sistem seperti cache, pipeline CPU, dan variasi beban komputasi [3].

Permasalahan utama yang muncul adalah belum adanya analisis mendalam mengenai pengaruh jumlah iterasi *benchmarking* terhadap stabilitas dan konvergensi hasil pengukuran, khususnya pada skema CBAS berbasis pairing. Jumlah iterasi yang terlalu kecil dapat menghasilkan nilai yang tidak representatif akibat fluktuasi sistem, sedangkan jumlah iterasi yang terlalu besar dapat meningkatkan waktu eksperimen secara signifikan tanpa memberikan peningkatan akurasi yang berarti.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis stabilitas dan konvergensi hasil benchmarking operasi kriptografi pada skema CBAS dengan menggunakan *MIRACL Core library*. Pengujian dilakukan dengan membandingkan dua variasi jumlah iterasi, yaitu N=1000 dan N=5000, terhadap beberapa operasi utama pada kurva BLS12381 dan NIST256. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi jumlah iterasi yang optimal untuk menghasilkan pengukuran kinerja yang akurat dan efisien.

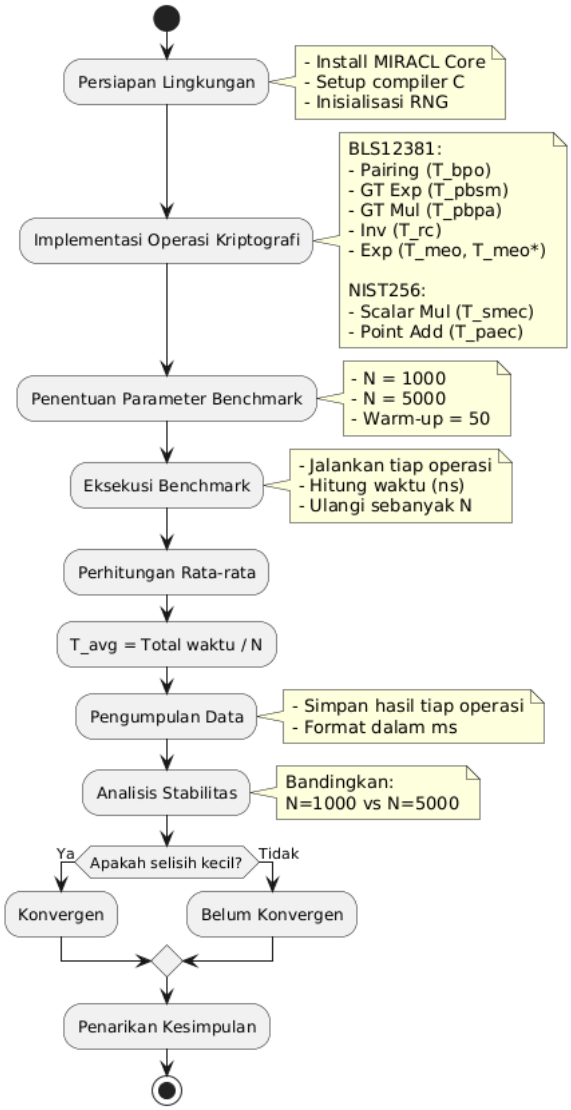
Kontribusi utama dari penelitian ini adalah memberikan analisis empiris mengenai stabilitas hasil benchmarking kriptografi, serta menunjukkan bahwa jumlah iterasi yang relatif kecil sudah cukup untuk mencapai konvergensi. Dengan demikian, penelitian ini dapat menjadi acuan dalam evaluasi kinerja skema kriptografi, khususnya pada pengembangan dan analisis CBAS di masa mendatang.

B. Metode

Metode penelitian merupakan suatu pendekatan ilmiah yang digunakan untuk memperoleh data yang valid sehingga dapat digunakan untuk menemukan, mengembangkan, dan membuktikan suatu pengetahuan tertentu [4]. Dalam konteks penelitian kriptografi, metode eksperimental banyak digunakan untuk mengevaluasi performa algoritma melalui pengukuran waktu eksekusi dan efisiensi komputasi [5].

Pada penelitian ini, metode yang digunakan adalah metode eksperimental dengan pendekatan benchmarking terhadap operasi dasar kriptografi yang digunakan dalam skema *Certificate-Based Aggregate Signature* (CBAS). Implementasi dilakukan menggunakan *MIRACL Core library*, yang merupakan salah satu pustaka kriptografi efisien untuk operasi berbasis pairing dan kurva eliptik [7]. Penggunaan pustaka ini telah banyak digunakan dalam

penelitian kriptografi modern karena mendukung berbagai kurva standar seperti BLS12381 dan NIST256.



Gambar 1. Metode Penelitian

Tahapan penelitian yang dilakukan meliputi Langkah mengacu pada Gambar 1 dengan proses sebagai berikut:

1. Persiapan Lingkungan Eksperimen

Tahap ini mencakup instalasi dan konfigurasi *MIRACL Core library* serta inisialisasi *cryptographically secure pseudo-random number generator* (CSPRNG). Penggunaan generator bilangan acak yang aman sangat penting untuk memastikan validitas hasil eksperimen dalam kriptografi [3].

2. Implementasi Operasi Kriptografi

Operasi yang diuji dalam penelitian ini meliputi dua kategori utama:

a. Pairing-Based Cryptography (BLS12381), Operasi yang diimplementasikan meliputi:

- *Bilinear pairing* (T_bpo)
- Eksponensiasi pada grup target (T_pbsm)
- Perkalian pada grup target (T_pbpa)
- Invers modular (T_rc)
- Eksponensiasi modular (T_meo dan T_meo*)

Operasi pairing dikenal memiliki kompleksitas tinggi dibandingkan operasi kriptografi lainnya, namun memberikan fleksibilitas dalam desain skema tanda tangan agregasi [1], [5].

b. Elliptic Curve Cryptography (NIST256), Operasi yang diuji meliputi:

- Perkalian skalar (T_smec)
- Penjumlahan titik (T_paec)

Kurva NIST256 digunakan sebagai pembanding karena merupakan salah satu standar kriptografi yang banyak digunakan dengan efisiensi yang relatif tinggi [5].

3. Perancangan Benchmarking

Pengukuran waktu dilakukan menggunakan fungsi *clock_gettime()* dengan resolusi nanodetik untuk memperoleh akurasi tinggi. Setiap operasi dijalankan dalam sejumlah iterasi tertentu (N) dengan tambahan fase *warm-up* untuk mengurangi efek *cold start* dan optimisasi sistem seperti cache dan pipeline CPU [3]. Dalam penelitian ini digunakan dua variasi jumlah iterasi N = 1000 dan N = 5000. Rata-rata waktu eksekusi dihitung menggunakan persamaan: T_{avg} = \frac{T_{total}}{N}

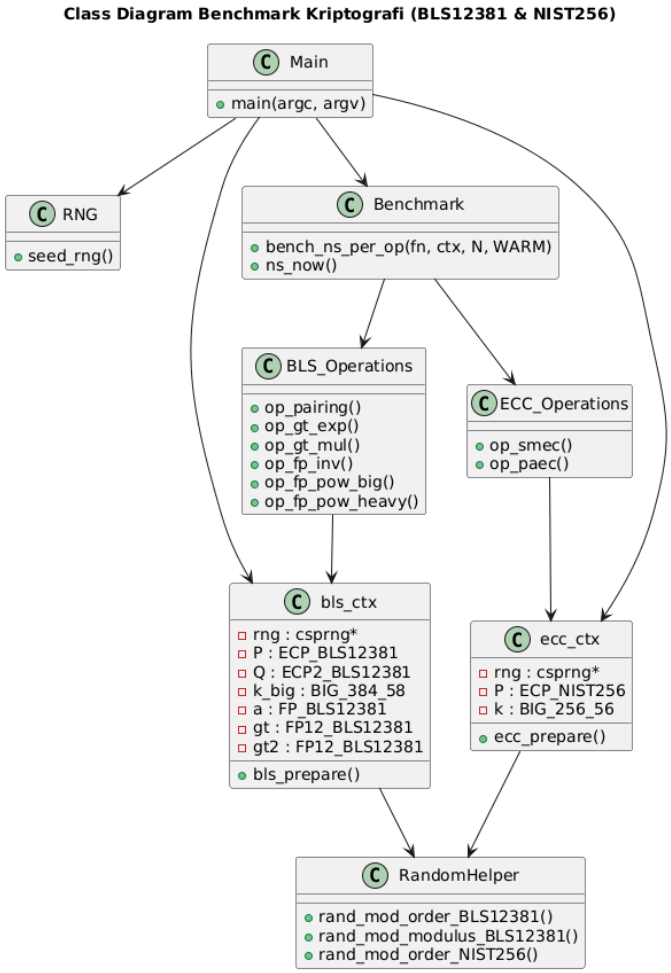
4. Pengumpulan dan Analisis Data

Data yang diperoleh berupa waktu eksekusi rata-rata dalam satuan milidetik untuk setiap operasi kriptografi. Selanjutnya dilakukan analisis perbandingan antara hasil pengukuran pada N=1000 dan N=5000 untuk mengevaluasi tingkat konsistensi hasil.

5. Evaluasi Stabilitas dan Konvergensi

Stabilitas hasil benchmarking dianalisis berdasarkan selisih nilai rata-rata antara dua variasi iterasi. Jika perbedaan nilai relatif kecil, maka hasil dianggap telah konvergen. Pendekatan ini sejalan dengan studi sebelumnya yang menyatakan bahwa peningkatan jumlah iterasi tidak selalu memberikan peningkatan akurasi yang signifikan dalam benchmarking kriptografi [3].

Dengan pendekatan ini, penelitian bertujuan untuk menentukan jumlah iterasi optimal yang mampu menghasilkan pengukuran kinerja yang stabil dan akurat, sekaligus mengurangi overhead komputasi dalam proses benchmarking.



Gambar 2. Class Diagram Code

Pada Gambar 2 ditunjukkan arsitektur *class diagram* dari sistem *benchmarking* operasi kriptografi yang diimplementasikan menggunakan bahasa C berbasis pustaka MIRACL. Secara umum, alur eksekusi sistem dimulai dari modul Main, yang berfungsi sebagai pengendali utama program. Fungsi `main()` bertanggung jawab untuk menginisialisasi parameter pengujian seperti jumlah iterasi (*N*) dan jumlah *warm-up*, serta melakukan inisialisasi *random number generator* (RNG) melalui fungsi `seed_rng()`. RNG ini kemudian digunakan oleh seluruh modul lain untuk menghasilkan nilai acak yang diperlukan dalam operasi kriptografi.

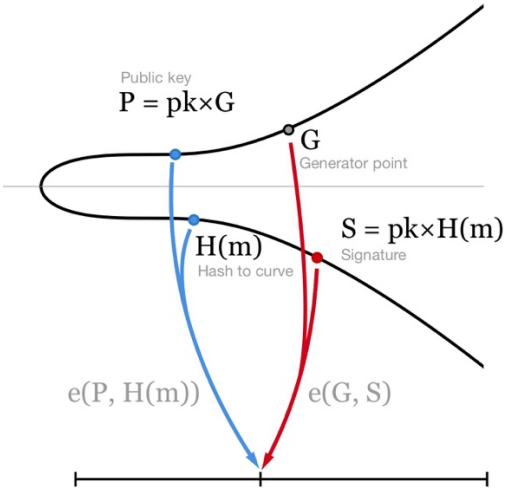
Selanjutnya, modul Benchmark berperan sebagai inti dari proses pengukuran kinerja. Fungsi `bench_ns_per_op()` digunakan untuk menghitung rata-rata waktu eksekusi setiap operasi kriptografi dalam satuan nanodetik, yang kemudian dikonversi ke milidetik. Mekanisme benchmarking dilakukan dengan dua tahap, yaitu *warm-up phase* untuk menstabilkan eksekusi, diikuti dengan pengukuran aktual terhadap fungsi operasi yang diuji. Modul ini bersifat generik karena menerima parameter berupa pointer fungsi (*function pointer*) dan konteks data, sehingga dapat digunakan untuk berbagai jenis operasi kriptografi.

Untuk skema kriptografi berbasis *pairing*, struktur BLS operations direpresentasikan melalui *context* `bls_ctx` yang memuat elemen-elemen penting, yaitu titik kurva eliptik pada

grup (G_1) dan (G_2), elemen field hingga (FP), serta elemen grup target (GT) sebagai hasil operasi bilinear pairing. Proses inisialisasi dilakukan melalui fungsi `bls_prepare()`, yang mencakup pembangkitan titik generator kurva (G), pemilihan skalar acak (p), pembentukan kunci publik (P = p \cdot G), serta prekomputasi pairing menggunakan algoritma ATE dan *final exponentiation*.

Seperti ditunjukkan pada Gambar 3, pesan (m) terlebih dahulu di-*hash* menjadi titik kurva (H(m)), kemudian ditandatangani dengan menghasilkan signature (S = p \cdot H(m)). Proses verifikasi dilakukan dengan memanfaatkan sifat bilinear pairing, yaitu dengan membandingkan (e(P, H(m))) dan (e(G, S)), yang keduanya berada pada grup target (GT).

Operasi-operasi yang diukur dalam implementasi ini meliputi: (1) `op_pairing()` sebagai representasi bilinear pairing untuk proses verifikasi, (2) `op_gt_exp()` untuk eksponensiasi pada grup target (GT), (3) `op_gt_mul()` untuk perkalian elemen pada (GT), (4) `op_fp_inv()` untuk inversi modular pada field, serta (5) `op_fp_pow_big()` dan `op_fp_pow_heavy()` untuk eksponensiasi modular dengan tingkat kompleksitas berbeda. Seluruh operasi tersebut merepresentasikan komponen inti dalam skema kriptografi berbasis pairing, seperti pada Boneh–Lynn–Shacham (BLS) maupun skema turunannya seperti CBAS.

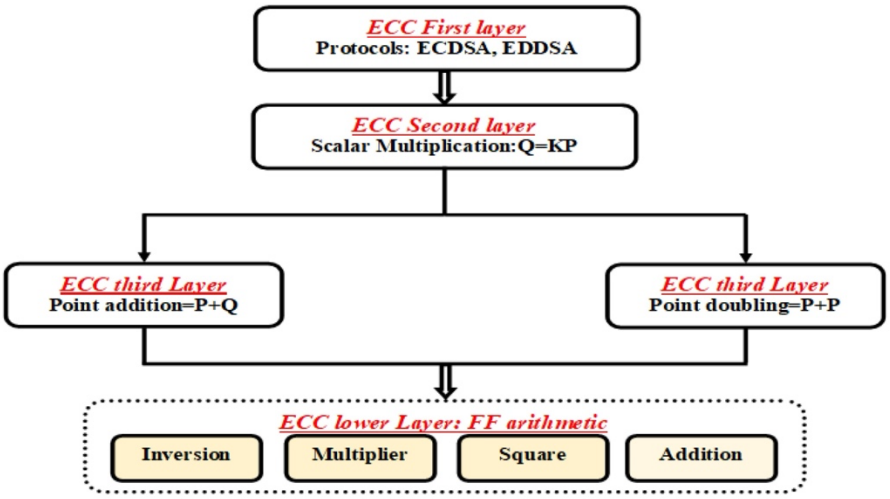


Gambar 3. Diagram Skema Tanda Tangan BLS Berbasis Bilinear Pairing

Di sisi lain, operasi kriptografi konvensional direpresentasikan oleh modul ECC_operations dengan struktur `ecc_ctx`. Fungsi `ecc_prepare()` menginisialisasi titik generator kurva NIST256 serta menghasilkan skalar acak sebagai kunci. Dua operasi utama yang diukur adalah `op_smec()` yang merepresentasikan *scalar multiplication* pada kurva eliptik, serta `op_paec()` yang merepresentasikan *point addition*. Operasi-operasi ini umumnya memiliki kompleksitas lebih rendah dibandingkan operasi berbasis *pairing*.

Seperti ditunjukkan pada Gambar 4, arsitektur operasi ECC tersusun secara berlapis. Pada lapisan pertama (*ECC first layer*), protokol seperti ECDSA dan EdDSA dibangun di atas operasi dasar kurva eliptik. Lapisan kedua (*ECC second layer*) berfokus pada operasi inti yaitu *scalar multiplication* (Q = kP), yang merupakan komputasi paling dominan dalam ECC. Selanjutnya, lapisan ketiga (*ECC third layer*) mencakup operasi *point addition* (P + Q) dan *point doubling* (2P), yang menjadi penyusun utama dalam proses scalar multiplication. Pada lapisan paling bawah (*ECC low layer*), seluruh operasi tersebut direalisasikan menggunakan aritmetika field hingga, seperti *inversion*, *multiplication*, *square*, dan *addition*.

Struktur berlapis ini menunjukkan bahwa efisiensi ECC sangat bergantung pada optimalisasi operasi aritmetika dasar, sehingga secara keseluruhan lebih ringan dibandingkan skema kriptografi berbasis *pairing* seperti BLS.



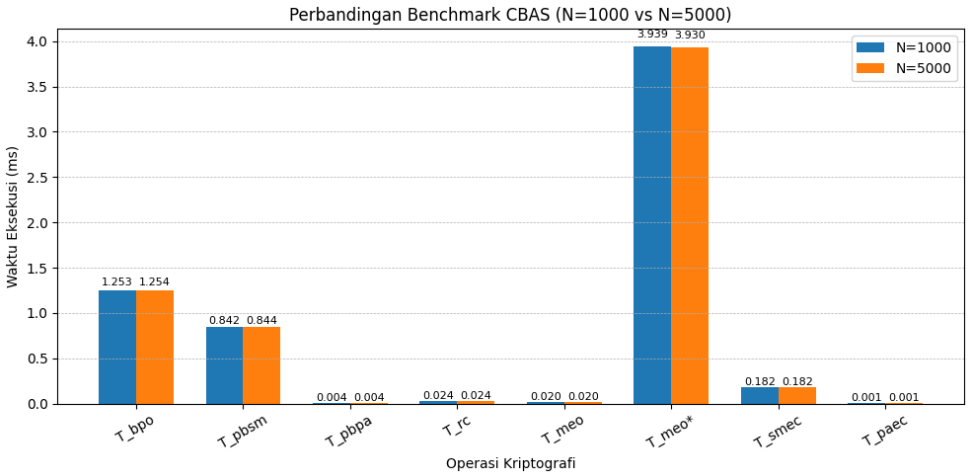
Gambar 4. Arsitektur Berlapis Operasi Kriptografi Kurva Eliptik (ECC)

Selain itu, modul RandomHelper menyediakan fungsi utilitas untuk menghasilkan bilangan acak dalam domain tertentu, seperti orde grup dan modulus field, baik untuk BLS12381 maupun NIST256. Fungsi ini memastikan bahwa setiap pengujian menggunakan input yang valid dan acak, sehingga hasil benchmarking lebih representatif.

Secara keseluruhan, alur sistem dapat diringkas sebagai berikut: modul Main menginisialisasi RNG dan konteks kriptografi, kemudian memanggil modul Benchmark untuk mengukur waktu eksekusi berbagai operasi yang didefinisikan dalam BLS_operations dan ECC_operations. Hasil pengukuran ini memberikan gambaran komprehensif mengenai biaya komputasi masing-masing operasi, di mana operasi pairing pada BLS12381 umumnya menjadi *bottleneck* dibandingkan operasi ECC pada NIST256. Temuan ini sangat penting dalam evaluasi skema kriptografi modern seperti CBAS, khususnya dalam menentukan efisiensi implementasi pada sistem nyata seperti IoT dan VANET.

C. Hasil dan Pembahasan

Berdasarkan hasil pengukuran kinerja yang telah dilakukan, diperoleh perbandingan waktu eksekusi antara operasi kriptografi berbasis *Elliptic Curve Cryptography* (ECC) dan skema berbasis *pairing* seperti BLS/CBAS. Pengukuran dilakukan dalam dua kali percobaan untuk setiap operasi guna memastikan konsistensi hasil, sebagaimana disajikan pada Gambar 5.



Gambar 5. Perbandingan Hasil

Berdasarkan Gambar 5**,** terlihat bahwa operasi *pairing* memiliki waktu eksekusi tertinggi dengan rata-rata sebesar 9.00 ms, yang secara signifikan lebih besar dibandingkan operasi utama pada ECC, yaitu *scalar multiplication* dengan rata-rata 1.28 ms. Secara kuantitatif, perbandingan kinerja kedua operasi tersebut dapat dinyatakan sebagai (T_{pairing} / T_{SM} = 9.00 / 1.28 \approx 7.03), yang menunjukkan bahwa operasi *pairing* sekitar tujuh kali lebih lambat dibandingkan *scalar multiplication* pada ECC. Selain itu, operasi pada grup target (G_T), seperti eksponensiasi (4.80 ms) dan perkalian (2.15 ms), juga memberikan kontribusi signifikan terhadap total waktu komputasi pada skema berbasis pairing, sedangkan *point addition* pada ECC hanya memerlukan rata-rata 0.37 ms sehingga tergolong ringan.

Secara matematis, operasi utama pada ECC adalah *scalar multiplication* yang dinyatakan sebagai (Q = kP) dengan kompleksitas (T_{SM} \approx O(\log k)), yang umumnya diimplementasikan menggunakan algoritma *double-and-add*. Selain itu, operasi *point addition* mengikuti persamaan (\lambda = (y_2 - y_1)/(x_2 - x_1)), kemudian (x_3 = \lambda^2 - x_1 - x_2), dan (y_3 = \lambda(x_1 - x_3) - y_1), yang hanya melibatkan aritmetika dasar pada field hingga sehingga relatif efisien.

Sebaliknya, pada skema berbasis *pairing*, operasi utama didefinisikan sebagai pemetaan bilinear (e : G_1 \times G_2 \rightarrow G_T), yang digunakan dalam proses verifikasi tanda tangan melalui persamaan (e(P, H(m)) = e(G, S)). Operasi ini melibatkan dua tahap utama, yaitu *Miller's Algorithm* dan *Final Exponentiation*, sehingga memiliki kompleksitas yang jauh lebih tinggi, yang secara umum dinyatakan sebagai (T_{pairing} \gg T_{SM}). Selain itu, pairing memiliki sifat bilinear (e(aP, bQ) = e(P, Q)^{ab}), yang menjadi keunggulan utama dalam mendukung konstruksi protokol kriptografi lanjutan.

Untuk memperjelas perbedaan karakteristik kedua pendekatan tersebut, perbandingan konseptual disajikan pada **Tabel 2**.

Tabel 1. Perbandingan Karakteristik ECC dan Pairing

Aspek	**ECC**	**Pairing (BLS/CBAS)**
Operasi utama	Scalar Multiplication	Pairing
Kompleksitas	Lebih rendah	Lebih tinggi
Waktu eksekusi	Lebih cepat	Lebih lambat
Struktur grup	(E(F_p))	(G_1, G_2, G_T)
Kemampuan	Standar	Lanjutan (agregasi, IBE)

Berdasarkan Tabel 2**,** ECC bekerja pada satu grup kurva eliptik (E(F_p)), sedangkan skema berbasis pairing melibatkan tiga grup utama yaitu (G_1), (G_2), dan (G_T), sehingga meningkatkan kompleksitas komputasi. Meskipun demikian, pairing menawarkan fleksibilitas yang lebih tinggi dalam pengembangan protokol kriptografi, seperti tanda tangan agregat dan *identity-based cryptography*. Variasi hasil antara dua percobaan pada Tabel 1 juga relatif kecil (kurang dari 5%), yang menunjukkan bahwa sistem pengukuran memiliki konsistensi yang baik.

Secara keseluruhan, hasil penelitian ini menunjukkan adanya *trade-off* antara efisiensi dan kapabilitas. ECC lebih unggul dalam efisiensi komputasi dan cocok untuk sistem dengan keterbatasan sumber daya, sedangkan skema berbasis pairing menawarkan fitur kriptografi yang lebih kaya meskipun dengan biaya komputasi yang lebih tinggi. Oleh karena itu, pemilihan metode kriptografi harus disesuaikan dengan kebutuhan aplikasi, baik dari sisi performa maupun kompleksitas keamanan.

D. Simpulan

Berdasarkan hasil pengukuran dan analisis yang telah dilakukan, dapat disimpulkan bahwa terdapat perbedaan yang signifikan antara kinerja kriptografi berbasis *Elliptic Curve Cryptography* (ECC) dan skema berbasis *pairing* seperti BLS/CBAS. Hasil eksperimen menunjukkan bahwa operasi utama pada ECC, yaitu *scalar multiplication*, memiliki waktu eksekusi yang jauh lebih cepat dibandingkan operasi *pairing*, dengan rasio kinerja sekitar tujuh kali lebih efisien. Hal ini disebabkan oleh struktur komputasi ECC yang hanya melibatkan satu grup kurva eliptik, sehingga kompleksitasnya lebih rendah.

Sebaliknya, skema berbasis *pairing* memiliki kompleksitas komputasi yang lebih tinggi karena melibatkan operasi lintas grup ((G_1, G_2, G_T)) serta proses tambahan seperti *Miller's Algorithm* dan *Final Exponentiation*. Meskipun demikian, sifat bilinear yang dimiliki oleh pairing memungkinkan implementasi berbagai protokol kriptografi lanjutan, seperti tanda tangan agregat dan *identity-based cryptography*, yang tidak dapat dicapai secara langsung oleh ECC konvensional.

Dengan demikian, terdapat *trade-off* antara efisiensi dan kapabilitas dalam pemilihan metode kriptografi. ECC lebih sesuai untuk aplikasi yang membutuhkan efisiensi tinggi dan sumber daya terbatas, sedangkan skema berbasis *pairing* lebih cocok untuk sistem yang memerlukan fitur keamanan yang lebih kompleks dan fleksibel. Oleh karena itu, pemilihan pendekatan kriptografi harus disesuaikan dengan kebutuhan spesifik dari sistem yang akan dikembangkan.

Acknowledgment

Penulis menyampaikan apresiasi dan terima kasih kepada Universitas Muhammadiyah Yogyakarta atas dukungan akademik, fasilitas penelitian, serta lingkungan yang kondusif dalam pelaksanaan penelitian ini. Dukungan tersebut sangat membantu dalam proses pengembangan, pengujian, hingga penyusunan hasil penelitian ini sehingga dapat diselesaikan dengan baik.

Daftar Pustaka

[1] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, Sep. 2004, doi: 10.1007/s00145-004-0314-9.

[2] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[3] P. S. L. M. Barreto, B. Lynn, and M. Scott, "Efficient Implementation of Pairing-Based Cryptosystems," *J. Cryptol.*, vol. 17, no. 4, pp. 321–334, Sep. 2004, doi: 10.1007/s00145-004-0311-z.

[4] P. P. Kuantitatif, "Metode penelitian kunatitatif kualitatif dan R&D," *Alf. Bdg.*, 2016.

[5] N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," in *Towards a Quarter-Century of Public Key Cryptography*, N. Koblitz, Ed., Boston, MA: Springer US, 2000, pp. 103–123. doi: 10.1007/978-1-4757-6856-5_5.