Jurnal Elektronik Ilmu Komputer Udayana
Volume 15, No 1. August 2026
p-ISSN: 2301-5373
e-ISSN: 2654-5101

Keamanan Seed Phrase dalam *Wallet Cryptocurrency* Menggunakan Algoritma *Elliptic Curve Cryptography* (ECC)

I Kadek Adi Sentana[a1], I Gusti Ngurah Anom Cahyadi Putra[a2], Luh Arida Ayu Rahning Putri[a3], I Gede Surya Rahayuda[a4]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Jimbaran, Kuta Selatan, Badung, Bali, Indonesia

[1]sentana.2208561138@student.unud.ac.id
[2]anom.cp@unud.ac.id
[3]rahningputri@unud.ac.id
[4]igedesuryarahayuda@unud.ac.id

ABSTRAK

Penyimpanan *seed phrase* pada *wallet* mata uang kripto seringkali menjadi titik lemah keamanan utama karena umumnya disimpan dalam format teks terang (*plain text*) yang rentan terhadap akses tidak sah. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem pengamanan *seed phrase* menggunakan algoritma *Elliptic Curve Cryptography* (ECC) dengan standar kurva SECP256k1. Untuk memperkuat lapisan perlindungan, sistem ini juga mengintegrasikan metode *Key Wrapping* berbasis PBKDF2 dengan penambahan *salt* guna melindungi kunci privat dari upaya peretasan. Metodologi pengujian yang digunakan mencakup analisis performa komputasi serta simulasi serangan *brute force* pada lapisan autentikasi sistem. Hasil penelitian menunjukkan bahwa implementasi algoritma ECC sangat efisien dengan waktu eksekusi rata-rata untuk proses enkripsi dan dekripsi di bawah 0,1 milidetik, sehingga tidak membebani performa perangkat. Selain itu, hasil pengujian ketahanan terhadap serangan *brute force* dengan 220000 data uji menunjukkan status gagal atau sistem aman. Hal ini dikarenakan penggunaan kata sandi kompleks menghasilkan nilai entropi sebesar 4,75 x 10^{23} kombinasi, yang secara matematis mustahil untuk ditembus dalam rentang waktu yang rasional menggunakan teknologi komputasi saat ini. Simpulan dari penelitian ini adalah penggabungan algoritma ECC dan kebijakan kata sandi yang kuat terbukti efektif dalam memberikan perlindungan tingkat tinggi bagi aset digital pengguna dari berbagai skenario serangan siber.

Kata Kunci : Cryptocurrency, Seed Phrase, Elliptic Curve Cryptography (ECC), Brute Force, Keamanan Data.

1. PENDAHULUAN

Pertumbuhan pesat dalam adopsi aset digital dan *cryptocurrency* menuntut standar keamanan tingkat tinggi di sisi pengguna, terutama dalam pengelolaan dompet digital (*wallet*) [1]. Setiap wallet cryptocurrency umumnya dilengkapi dengan seed phrase yang berfungsi sebagai mekanisme pemulihan private key ketika pengguna kehilangan akses terhadap wallet. Kerahasiaan seed phrase menjadi aspek yang sangat penting karena siapa pun yang mengetahui seed phrase dapat memperoleh kendali penuh terhadap aset digital yang tersimpan di dalam wallet. Menjaga kerahasiaan *seed phrase* sangat krusial untuk mencegah akses tidak sah dan melindungi aset pengguna dari pencurian [2]. Sayangnya, kelalaian dalam mengamankan *seed phrase* masih menjadi celah keamanan utama. Pengguna sering kali menyimpannya dalam format teks terang (*plain text*) di perangkat yang rentan terhadap retasan jaringan. Apabila pihak ketiga berhasil membobol gerbang akses utama pengguna melalui serangan *brute force*, seluruh isi *wallet* dapat terkuras [3].

Oleh karena itu, penelitian ini mengusulkan implementasi algoritma *Elliptic Curve Cryptography* (ECC)[4]. Algoritma ECC dipilih karena memiliki ukuran kunci yang lebih kecil dibandingkan algoritma RSA, namun tetap mampu memberikan tingkat keamanan yang setara dengan performa komputasi yang lebih efisien [5]**,** [6]. Karakteristik tersebut menjadikan ECC banyak digunakan pada sistem dengan keterbatasan sumber daya, termasuk aplikasi blockchain dan cryptocurrency [7]. Implementasi kriptografi juga telah banyak diterapkan pada berbagai arsitektur jaringan dan media komunikasi untuk menjamin aspek kerahasiaan data[8], [9]. Dengan mengombinasikan ECC dan mekanisme pelindungan Kunci Privat berbasis *hashing* dan *salting*, sistem ini diharapkan mampu menghasilkan brankas *seed phrase* yang kebal terhadap upaya pembobolan tanpa membebani performa perangkat keras [10], [11].

2. METODE PENELITIAN

Pengembangan perangkat lunak dalam penelitian ini diadaptasi dari model *System Development Life Cycle* (SDLC) *Waterfall* secara ringkas, yang mencakup analisis kebutuhan, perancangan, implementasi, dan pengujian. Alih-alih berfokus pada tahapan rekayasa perangkat lunak konvensional, penelitian ini menitikberatkan pada perancangan arsitektur keamanan kriptografi berlapis. Arsitektur matematis dan operasional sistem ini dibagi ke dalam tiga mekanisme utama:

1. Desain Algoritma dan Pembangkitan Kunci (*Key Generation*) ECC

Sistem menggunakan algoritma *Elliptic Curve Cryptography* (ECC) dengan standar kurva SECP256k1 yang secara luas diakui keandalannya dalam ekosistem *cryptocurrency Kurva* SECP256k1 dipilih karena telah digunakan secara luas dalam implementasi Bitcoin dan berbagai cryptocurrency sehingga memiliki tingkat interoperabilitas dan keamanan yang tinggi[7]. Pada tahap pembangkitan kunci, sistem menggunakan *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG) untuk membangkitkan bilangan bulat acak sebagai Kunci Privat (d) Selanjutnya, Kunci Publik (Q) dihitung menggunakan operasi perkalian skalar terhadap titik dasar kurva (G) melalui persamaan $Q = d \times G$ Penggunaan kurva SECP256k1 memastikan komputasi berjalan ringan namun memberikan tingkat keamanan ekuivalen dengan algoritma konvensional berukuran kunci jauh lebih besar

2. Mekanisme *Key Wrapping* Berbasis PBKDF2

Untuk melindungi private key dari serangan pembacaan data maupun brute force terhadap password, penelitian ini menerapkan mekanisme Password-Based Key Derivation Function 2 (PBKDF2). PBKDF2 bekerja dengan mengombinasikan password pengguna, nilai salt acak, serta proses iterasi sehingga menghasilkan kunci turunan yang lebih sulit ditebak melalui serangan exhaustive search [12]

3. Skema Enkripsi dan Dekripsi *Seed Phrase*

Objek utama yang diamankan adalah *seed phrase*, yang dibentuk dari *wordlist* standar BIP 39 berisi 2048 kata. Skema enkripsi pada lapisan ketiga ini tidak menggunakan block cipher yang berat, melainkan menggunakan operasi logika *bitwise Exclusive-OR* (XOR). *Seed phrase* di-XOR-kan dengan kunci turunan berbasis *hash* (SHA-256) yang diekstrak dari Kunci Publik ECC. Skema matematisnya adalah sebagai berikut:

$$Enkripsi: Ciphertext = Seedphrase \oplus SHA256(Q)$$

$$Dekripsi: Seedphrase = Ciphertext \oplus SHA256(Q)$$

Pendekatan operasi logika ini dipilih secara spesifik karena terbukti tidak menghasilkan pembengkakan ukuran data (*overhead*), sehingga efisiensi penyimpanan memori tetap terjaga.

Sistem ini dikembangkan menggunakan metode System Development Life Cycle (SDLC) dengan model Waterfall. Data yang digunakan dalam sistem merupakan kata-kata yang bersumber dari wordlist standar BIP 39 yang berjumlah 2048 kata. Alur matematis algoritma ECC dibagi menjadi beberapa tahapan operasional, yaitu pembangkitan kunci (key generation), skema enkripsi, dan skema dekripsi. Pada tahap pembangkitan kunci, sistem membangkitkan bilangan bulat acak aman sebagai Kunci Privat (d) dan menghitung Kunci Publik (Q) menggunakan operasi perkalian skalar titik dasar kurva (G) melalui rumus Q = d x G. Kurva standar yang digunakan adalah SECP256k1 seperti ditunjukkan pada persamaan (1)

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Kriptografi ECC

Pemilihan operasi logika antara teks asli dengan kunci turunan berbasis *hash* (SHA-256) dari Kunci Publik ECC yang kami kembangkan dilakukan dengan mempertimbangkan efisiensi sumber daya. Operasi pada sistem ini tidak menghasilkan pembengkakan ukuran data (*overhead*). Mengingat *seed phrase* umumnya berupa 12 kata (berdasarkan standar BIP 39), sistem berhasil memperoleh keunggulan perlindungan matematis ECC sembari mempertahankan efisiensi penyimpanan memori.

3.2 Performa Enkripsi dan Dekripsi

Hasil pengujian waktu eksekusi menunjukkan bahwa algoritma ECC beroperasi dengan sangat optimal. Berdasarkan benchmarking, waktu eksekusi rata-rata untuk proses enkripsi maupun dekripsi seed phrase berada di bawah 0,1 milidetik. Tingkat kecepatan ini menunjukkan bahwa metode yang diusulkan sangat layak untuk diimplementasikan pada perangkat dengan spesifikasi rendah sekalipun tanpa menimbulkan latensi. Temuan ini sejalan dengan penelitian Adrian dkk. [13] yang menunjukkan bahwa algoritma ECC memiliki performa komputasi yang lebih efisien dibandingkan RSA karena menggunakan ukuran kunci yang lebih kecil. Selain itu, karakteristik matematis ECC yang diperkenalkan oleh Koblitz [5] dan Miller [6] menjadikan algoritma ini mampu memberikan tingkat keamanan tinggi tanpa meningkatkan kompleksitas komputasi secara signifikan.

Tabel 3.1 Hasil Pengujian Konsistensi Waktu Eksekusi (12 Kata)

No. Sampel	Panjang data	Waktu Enkripsi	Waktu Dekripsi
Sampel 1	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 2	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 3	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 4	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 5	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 6	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 7	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 8	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 9	12 Kata	< 0,1 ms	**< 0,1 ms**
Sampel 10	12 Kata	< 0,1 ms	**< 0,1 ms**

3.3 Pengujian Keamanan Terhadap Brute Force

Pengujian Keamanan Terhadap Brute Force Pengujian dilakukan dengan mengasumsikan penyerang telah mengetahui *username* target dan menjalankan pencarian ekstensif (*exhaustive search*) untuk menebak kata sandi. Pada pengujian yang menargetkan kata sandi kompleks,

serangan yang mengeksekusi 220.000 data uji kombinasi kata sandi berstatus gagal atau sistem terbukti aman. Secara matematis, dengan panjang sandi 12 karakter dan variasi simbol, total kombinasi mencapai 4.75 x 10^{23} kemungkinan. Berdasarkan hasil dari 220.000 percobaan kegagalan tersebut, terbukti bahwa dibutuhkan waktu dan komputasi yang tidak rasional (*computationally infeasible*) untuk menebak sandi yang benar

Pengujian juga menunjukkan bahwa seluruh percobaan brute force terhadap kata sandi gagal memperoleh password yang benar. Hasil tersebut mendukung penggunaan PBKDF2 sebagai mekanisme key derivation karena proses iterasi dan penggunaan salt meningkatkan biaya komputasi yang harus dikeluarkan penyerang untuk melakukan pencarian password secara exhaustive. Mekanisme tersebut telah direkomendasikan dalam standar PKCS #5 sebagai salah satu metode perlindungan password yang efektif [12].

Tabel 3.2 *Benchmark* Percobaan *ECC*

No	Waktu uji	Jumlah percobaan	Durasi (detik)	Kecepatan (*key/sec)*
1	2026-05-08 08:33:07	100000	0.3055	**327382**
2	2026-05-08 08:33:11	200000	0.3023	**661611**
3	2026-05-08 08:33:14	300000	0.3058	**980914**
4	2026-05-08 08:33:22	500000	0.3054	**1637464**
5	2026-05-08 08:33:29	800000	0.3118	**2565845**
6	2026-05-08 08:33:33	1000000	0.3127	**3197521**
7	2026-05-08 08:33:43	2000000	0.4397	**4548882**
8	2026-05-08 08:33:57	2500000	0.5036	**4964249**
9	2026-05-08 08:34:04	3000000	0.5529	**5426096**
10	2026-05-08 08:34:07	4000000	0.6106	**6551033**
11	2026-05-08 08:34:14	5000000	0.5867	**8522728**

Tabel 3.3 Tabel Pengujian *Form Login*

Parameter Pengujian	Keterangan
Target Username	**Adis**
Kategori Kata Sandi	**Kompleks**
Panjang Karakter	**12 Karakter**
Kombinasi Karakter	**Huruf Besar, Huruf Kecil, Angka, dan Simbol Khusus**
Batas Waktu Pengujian	**220.000 data uji**
Hasil Akhir	**Gagal (sistem aman)**

Secara keseluruhan, hasil penelitian menunjukkan bahwa integrasi algoritma ECC dengan mekanisme PBKDF2 mampu menghasilkan sistem pengamanan seed phrase yang efisien sekaligus memiliki ketahanan terhadap serangan brute force. Berbeda dengan beberapa penelitian sebelumnya yang hanya mengevaluasi performa ECC atau implementasi PBKDF2 secara terpisah, penelitian ini mengombinasikan kedua mekanisme tersebut dalam satu sistem keamanan wallet cryptocurrency sehingga mampu memberikan perlindungan terhadap seed phrase dan private key secara berlapis [5], [6], [7], [12], [13].

4. KESIMPULAN

Berdasarkan hasil analisis, implementasi, dan pengujian pada sistem, dapat ditarik kesimpulan: implementasi algoritma ECC kurva secp256k1 terbukti sangat efisien dengan waktu eksekusi enkripsi dan dekripsi kurang dari 0,1 milidetik, memberikan keamanan tanpa membebani perangkat. Pemanfaatan *key wrapping* berbasis pbkdf2 dengan *salt* mampu menutupi celah keamanan pada penyimpanan kunci privat. Hasil uji ketahanan terhadap serangan *brute force* menggunakan 220.000 data uji menunjukkan bahwa dengan entropi sandi sebesar 4.75 x 10^{23} kombinasi, upaya penebakan paksa menjadi tidak rasional secara komputasi (*computationally*

infeasible), sehingga implementasi yang diusulkan mampu memberikan tingkat perlindungan yang tinggi terhadap seed phrase berdasarkan skenario pengujian yang dilakukan**.**

DAFTAR PUSTAKA

[1] Y. Diasca et al., "Tinjauan Teknologi Blockchain Dalam Audit Cryptocurrency," in *Prosiding The 12th Industrial Research Workshop and National Seminar Bandung*, 2021.

[2] A. Ega, "Analisis Transaksi Jual Beli Bitcoin Dalam Cryptocurrency Ditinjau Dari Perspektif Ekonomi Islam," Doctoral dissertation, UIN Raden Intan Lampung, 2026.

[3] R. K. Dinata, S. Safwandi, N. Hasdyna, and R. Mahendra, "Kombinasi Algoritma Brute Force dan Stemming pada Sistem Pencarian Mashdar," *CESS (Journal of Computer Engineering, System and Science)*, vol. 5, no. 2, pp. 273-278, 2020.

[4] T. Indriyani, "Enkripsi Data Dengan Mengunakan Metode ECC (Elliptic Curve Cryptography)," in *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, Nov. 2023.

[5] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[6] V. S. Miller, "Use of Elliptic Curves in Cryptography," in Advances in Cryptology—CRYPTO '85 Proceedings, Lecture Notes in Computer Science, vol. 218, Springer, 1986, pp. 417–426.

[7] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, Fourthquarter 2018.

[8] M. Reza and N. Fauzi, "Implementasi Elliptic Curve Cryptography (ECC) Dalam Jalur Komunikasi Aplikasi Chatting," Makalah II4031 Kriptografi dan Koding, Semester II Tahun 2021/2022.

[9] D. H. Sulaksono, C. N. Prabiantissa, G. E. Yuliastuti, and A. R. Taqwa, "Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android," in *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, vol. 9, no. 1, pp. 570-576, Oct. 2021.

[10] Y. R. Hutasoit, V. Simangunsong, and D. Siallagan, "Analisis terhadap keamanan password menggunakan hash SHA256," *JURNAL QUANCOM: QUANTUM COMPUTER JURNAL*, vol. 3, no. 1, pp. 13-17, 2025.

[11] R. Rahman, S. Citra, and H. J. Andini, "Evaluasi Keamanan Sistem Login Menggunakan Hashing dan Salting Password," *INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer*, vol. 1, no. 03, 2026.

[12] B. Kaliski, "PKCS #5: Password-Based Cryptography Specification Version 2.0," RFC 2898, Internet Engineering Task Force (IETF), Sep. 2000.

[13] N. Adianson, Y. Yupianti, and A. Kurniawan, "Analisa Perbandingan Performansi Rsa (Rivest Shamir Adleman) Dan Ecc (Elliptic Curve) Pada Protokol Secure Socket Layer (Ssl)," *Jurnal Media Infotama*, vol. 11, no. 1, 2015.