INTEGRASI ALGORITMA EdDSA DENGAN MULTI-SIGNATURE PADA SISTEM TANDA TANGAN DIGITAL BERBASIS QR CODE UNTUK VERIFIKASI DOKUMEN AKADEMIK

AHMAD FAUZI SAIFUDDIN[1], Lukman[2], Muhyiddin AM Hayat[3]
[1,2,3]*Informatika, Universitas Muhamadiyah Makassar, Makassar, 90221, Indonesia*
e-mail koresponden:
*105841102021@student.unismuh.ac.id[*1],lukman@unismuh.ac.id[2],muhyiddin@student.unismuh.ac.id[3].*

Received: Februari 01,2026; Accepted: Maret 01, 2026; Published: Maret 31, 2026

Abstrak

Perkembangan dokumen akademik digital menuntut adanya sistem verifikasi yang mampu menjamin keaslian, integritas, dan keabsahan dokumen secara cepat dan aman. Penelitian ini bertujuan untuk mengimplementasikan sistem tanda tangan digital berbasis QR Code dengan mengintegrasikan algoritma Edwards-curve Digital Signature Algorithm (EdDSA) varian Ed25519 dan skema multi-signature untuk verifikasi dokumen akademik. Setiap dokumen ditandatangani secara digital oleh satu atau lebih penandatangan menggunakan pasangan kunci kriptografi Ed25519, kemudian hasil tanda tangan, nilai hash dokumen, serta identitas penandatangan disematkan ke dalam QR Code sebagai media verifikasi. Sistem diuji pada beberapa jenis dokumen akademik, yaitu KKP, KHS, dan Persetujuan Hasil, dengan jumlah penandatangan yang berbeda. Hasil pengujian menunjukkan bahwa seluruh tanda tangan digital berhasil diverifikasi dengan tingkat keberhasilan 100% dan waktu eksekusi rata-rata di bawah 0,3 detik, termasuk pada skenario multi-signature. Dengan demikian, integrasi EdDSA dan multi-signature berbasis QR Code terbukti efektif, efisien, dan layak diterapkan sebagai solusi verifikasi dokumen akademik yang aman dan andal.

***Kata kunci**: Tanda tangan digital, EdDSA, Ed25519, multi-signature, QR Code*

Abstract

The development of digital academic documents requires a verification system that can ensure document authenticity, integrity, and validity in a fast and secure manner. This study aims to implement a QR Code–based digital signature system by integrating the Edwards-curve Digital Signature Algorithm (EdDSA) using the Ed25519 variant and a multi-signature scheme for academic document verification. Each document is digitally signed by one or more authorized signatories using Ed25519 key pairs, and the generated digital signatures, document hash values, and signer identities are embedded into QR Codes as a verification medium. The system was tested on several types of academic documents, including internship reports (KKP), academic transcripts (KHS), and approval documents, with different numbers of signatories. The experimental results show that all digital signatures were successfully verified with a 100% success rate and an average execution time below 0.3 seconds, including in multi-signature scenarios. These results demonstrate that the integration of EdDSA and multi-signature mechanisms with QR Code technology is effective, efficient, and suitable for secure and reliable academic document verification.

***Keyword**: Digital signature, EdDSA, Ed25519, multi-signature, QR Code*

1. Pendahuluan

Perkembangan teknologi informasi mendorong perguruan tinggi untuk beralih dari dokumen akademik berbasis kertas ke dokumen digital, seperti Kartu Hasil Studi (KHS), laporan Kuliah Kerja Praktik (KKP), dan lembar persetujuan hasil. Transformasi ini menuntut sistem verifikasi yang mampu menjamin keaslian, integritas, dan keabsahan dokumen secara cepat dan aman. Metode konvensional yang masih mengandalkan tanda tangan basah dan pemeriksaan manual dinilai kurang efisien serta rentan terhadap pemalsuan dokumen akademik [1].

Pemanfaatan QR Code mulai banyak diterapkan sebagai media verifikasi dokumen digital karena kemampuannya menyimpan informasi autentik yang dapat diakses dengan cepat melalui proses pemindaian [2]. Dalam konteks dokumen akademik, QR Code memungkinkan pihak ketiga melakukan verifikasi secara mandiri tanpa harus menghubungi institusi penerbit.

Tanda tangan digital berbasis kriptografi kunci publik telah digunakan secara luas untuk menjamin autentikasi, integritas data, dan prinsip non-repudiation pada dokumen elektronik. Penelitian oleh Wellem et al. menunjukkan bahwa integrasi QR Code dengan algoritma ECDSA mampu mendeteksi pemalsuan dokumen akademik secara efektif [3]. Namun, algoritma ECDSA masih bergantung pada bilangan acak dalam proses penandatanganan, yang berpotensi menimbulkan celah keamanan apabila generator bilangan acak tidak diimplementasikan dengan baik [4].

Sebagai alternatif, Edwards-curve Digital Signature Algorithm (EdDSA) diperkenalkan sebagai algoritma tanda tangan digital modern yang lebih aman dan efisien. EdDSA, khususnya varian Ed25519, memiliki sifat deterministik, ukuran kunci dan tanda tangan yang lebih kecil, serta performa komputasi yang lebih tinggi dibandingkan algoritma kriptografi klasik seperti RSA dan ECDSA [5], [6].

Selain aspek algoritma, dokumen akademik pada umumnya memerlukan pengesahan dari lebih dari satu pihak, seperti dosen pembimbing, ketua program studi, dan pimpinan fakultas. Sistem tanda tangan tunggal belum mampu merepresentasikan otorisasi kolektif tersebut secara optimal. Oleh karena itu, skema multi-signature menjadi pendekatan yang relevan untuk menjamin bahwa seluruh pihak yang berwenang telah terlibat dalam proses pengesahan dokumen secara kriptografis [7]–[9].

Integrasi QR Code dengan tanda tangan digital semakin banyak diterapkan pada sistem administrasi akademik karena mampu mempercepat proses verifikasi dan mengurangi ketergantungan pada pemeriksaan manual [10], [11]. Perbandingan algoritma kriptografi menunjukkan bahwa EdDSA (Ed25519) memiliki performa yang lebih unggul dibandingkan RSA dan ECDSA dari sisi kecepatan, efisiensi ukuran tanda tangan, dan keamanan [12]. Sifat deterministik EdDSA juga menjadikannya lebih tahan terhadap serangan side-channel [13]. Penelitian terbaru menunjukkan bahwa integrasi multi-signature dengan QR Code memungkinkan proses verifikasi dokumen dilakukan secara offline maupun online secara andal [14], [15].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan sistem tanda tangan digital berbasis QR Code yang mengintegrasikan algoritma EdDSA (Ed25519) dengan skema multi-signature untuk verifikasi dokumen akademik.

2. Metode Penelitian

2.1. Alat dan Bahan

Alat dan bahan yang digunakan terdiri dari perangkat keras dan perangkat lunak sebagai berikut.

a. Perangkat Keras
   - Laptop sebagai media pengembangan dan pengujian sistem
   - Prosesor Intel Core i3 generasi ke-11
   - Memori (RAM) sebesar 8 GB
   - Media penyimpanan SSD 512 GB
   - Sistem operasi Windows

Perangkat keras tersebut digunakan untuk menjalankan proses kriptografi Ed25519, pembuatan QR Code, serta pengujian performa sistem secara lokal.

b. Perangkat Lunak
   - Sistem operasi Windows
   - Visual Studio Code sebagai code editor
   - Bahasa pemrograman JavaScript
   - Library kriptografi Ed25519 untuk pembuatan dan verifikasi tanda tangan digital
   - Library QR Code untuk pembangkitan dan pemindaian QR Code

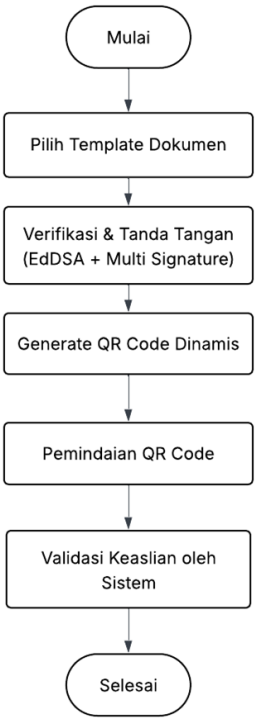
Seluruh perangkat lunak tersebut digunakan untuk mengimplementasikan algoritma EdDSA, membangun sistem tanda tangan digital berbasis web, serta melakukan pengujian fungsional dan performa sistem.

2.2. Perancangan Sistem

Perancangan sistem dilakukan untuk membangun mekanisme tanda tangan digital yang aman dan efisien dalam memverifikasi dokumen akademik. Sistem dirancang untuk mendukung beberapa jenis dokumen akademik, yaitu Kuliah Kerja Praktik (KKP), Kartu Hasil Studi (KHS), dan Persetujuan Hasil, yang masing-masing memiliki kebutuhan jumlah penandatangan yang berbeda. Perbedaan jumlah penandatangan ini menjadi dasar penerapan skema multi-signature dalam sistem.

Alur kerja sistem dimulai dari proses pemilihan jenis dokumen dan input data penandatangan. Selanjutnya, sistem melakukan pembangkitan pasangan kunci kriptografi Ed25519 untuk setiap penandatangan, kemudian menghitung nilai hash dari dokumen yang akan ditandatangani. Nilai hash tersebut digunakan sebagai input dalam proses pembuatan tanda tangan digital menggunakan algoritma EdDSA. Setelah proses penandatanganan selesai, hasil tanda tangan digital disematkan ke dalam QR Code yang ditempatkan pada dokumen akademik.

Alur keseluruhan proses sistem ini digambarkan secara ringkas pada Gambar 1. Flowchart Pelaksanaan Sistem. Gambar tersebut menunjukkan hubungan antar tahapan mulai dari pembuatan dokumen, proses penandatanganan digital, hingga verifikasi dokumen menggunakan QR Code.



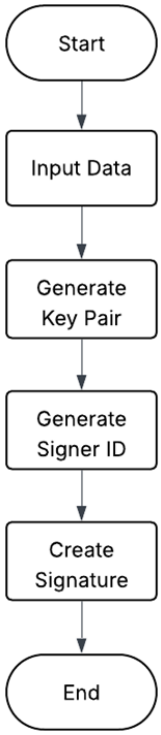
Gambar 1. Flowcart Pelaksanaan Sistem

2.3. Implementasi Algoritma EdDSA (Ed25519)

Implementasi algoritma EdDSA pada penelitian ini menggunakan varian Ed25519 yang berbasis kurva Edwards. Algoritma ini terdiri dari tiga tahap utama, yaitu pembangkitan kunci (key generation), pembuatan tanda tangan (signature generation), dan verifikasi tanda tangan (signature verification).

Pada tahap pembangkitan kunci, sistem menghasilkan pasangan kunci privat dan kunci publik untuk setiap penandatangan. Kunci privat digunakan untuk menghasilkan tanda tangan digital, sedangkan kunci publik digunakan dalam proses verifikasi. Tahap pembuatan tanda tangan dilakukan dengan menghitung nilai hash dokumen, kemudian menghasilkan tanda tangan digital secara deterministik menggunakan kunci privat. Pendekatan deterministik ini bertujuan untuk menghindari kelemahan bilangan acak yang sering menjadi celah keamanan pada algoritma tanda tangan digital lainnya.

Tahapan algoritma EdDSA yang digunakan dalam penelitian ini divisualisasikan pada Gambar 2. Flowchart EdDSA, yang menjelaskan alur proses penandatanganan dan verifikasi tanda tangan digital secara sistematis.



Gambar 2. Flowvart EdDSA

2.4. Skema Multi-Signature

Skema multi-signature diterapkan untuk menjamin bahwa dokumen akademik hanya dapat dinyatakan sah apabila seluruh pihak yang berwenang telah memberikan tanda tangan digital. Setiap penandatangan menghasilkan tanda tangan digital secara independen menggunakan pasangan kunci Ed25519 masing-masing, namun seluruh tanda tangan tersebut mengacu pada nilai hash dokumen yang sama.

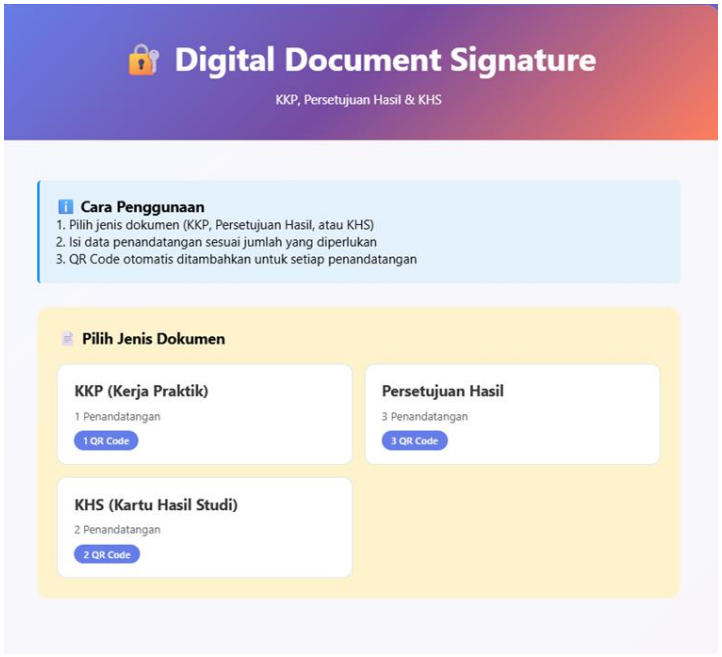
Pendekatan ini memungkinkan sistem untuk menerapkan otorisasi kolektif, di mana tidak ada satu pihak pun yang dapat mengesahkan dokumen secara sepihak. Dokumen hanya dinyatakan valid apabila seluruh tanda tangan digital berhasil diverifikasi menggunakan kunci publik penandatangan terkait.

2.5. Proses Pembuatan dan Verifikasi QR Code

QR Code digunakan sebagai media penyimpanan informasi tanda tangan digital karena mudah dipindai dan dapat digunakan sebagai sarana verifikasi mandiri. Setiap QR Code memuat nilai hash dokumen, tanda tangan digital, identitas penandatangan, serta timestamp penandatanganan.

Proses verifikasi dilakukan dengan memindai QR Code pada dokumen akademik. Sistem kemudian mengekstrak data dari QR Code, menghitung ulang nilai hash dokumen, dan mencocokkannya dengan tanda tangan digital yang tersimpan. Apabila seluruh tanda tangan dinyatakan valid, dokumen dianggap sah.

Implementasi antarmuka sistem ditunjukkan pada Gambar 3. Tampilan Awal Sistem Digital Document Signature, yang memperlihatkan halaman utama system.



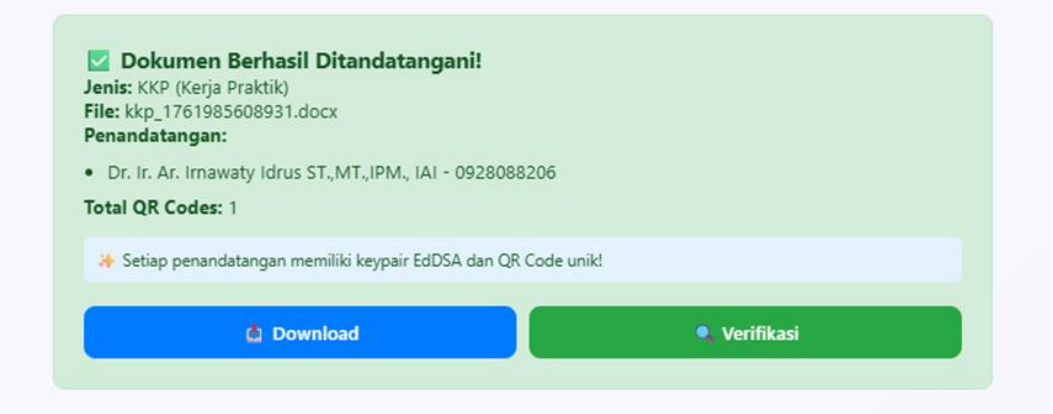
Gambar 3. Tampilan Awal Sistem Digital Document Signature

3. Hasil dan Pembahasan

3.1. Implementasi Sistem Tanda Tangan Digital

Hasil implementasi menunjukkan bahwa sistem tanda tangan digital berhasil dikembangkan sesuai dengan perancangan yang diusulkan. Sistem mampu menghasilkan dokumen akademik yang telah ditandatangani secara digital dan dilengkapi dengan QR Code sebagai media verifikasi.

Setelah proses penandatanganan selesai, sistem memberikan notifikasi bahwa dokumen telah berhasil ditandatangani secara digital. Kondisi ini ditunjukkan pada Gambar 4. Tampilan Hasil "Dokumen Berhasil Ditandatangani", yang menandakan bahwa seluruh tahapan penandatanganan telah dijalankan dengan sukses.

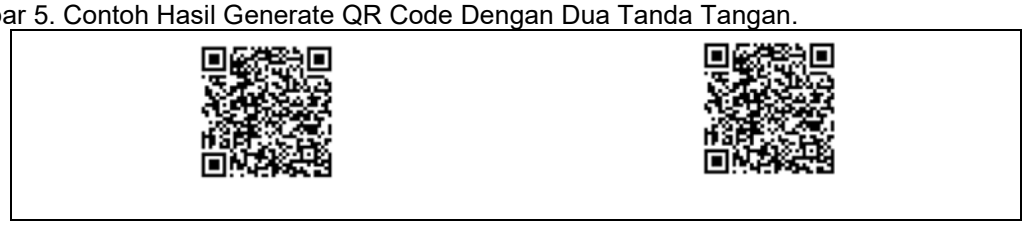


Gambar 4. Tampilan Hasil "Dokumen Berhasil Ditandatangani"

3.2 Hasil Implementasi QR Code

Hasil implementasi menunjukkan bahwa sistem berhasil menghasilkan QR Code sebagai media penyimpanan informasi tanda tangan digital pada dokumen akademik. QR Code yang dihasilkan memuat nilai hash dokumen, tanda tangan digital berbasis Ed25519, identitas penandatangan, serta informasi waktu penandatanganan. QR Code disematkan langsung pada dokumen akademik yang telah ditandatangani secara digital dan bersifat unik untuk setiap dokumen, karena proses pembangkitannya bergantung pada nilai hash dan tanda tangan digital masing-masing

penandatangan. Contoh hasil pembangkitan QR Code pada dokumen akademik ditunjukkan pada Gambar 5. Contoh Hasil Generate QR Code Dengan Dua Tanda Tangan.



Gambar 5. Contoh Hasil Generate QR Code Dengan Dua Tanda Tangan

3.2. Hasil Pengujian Performa Algoritma Ed25519

Pengujian performa dilakukan untuk mengukur efisiensi algoritma Ed25519 dalam proses pembangkitan kunci, pembuatan tanda tangan, dan verifikasi tanda tangan digital. Pengujian dilakukan pada beberapa jenis dokumen akademik dengan jumlah penandatangan yang berbeda.

Hasil pengujian performa ditunjukkan pada Tabel 1. Hasil Pengujian Performa Algoritma Ed25519. Berdasarkan tabel tersebut, rata-rata waktu eksekusi sistem berada di bawah 0,3 detik, bahkan pada skenario multi-signature. Hal ini menunjukkan bahwa algoritma Ed25519 memiliki kinerja yang sangat efisien dan cocok untuk sistem verifikasi dokumen akademik yang membutuhkan respon cepat.

Tabel 1. Hasil Pengujian Performa Algoritma Ed25519

Operasi	**Rata-rata Waktu (*ms*)**	**Minimum (*ms*)**	**Maksimum (*ms*)**	**Keterangan**
Pembangkitan Kunci (*Key Generation*)	8.3	7	12	Cepat karena menggunakan operasi aritmetika kurva *eliptik* yang efisien.
Pembuatan Tanda Tangan (*Signature Creation*)	12.1	10	18	*Deterministik*, tidak memerlukan *random number* generator.
Verifikasi Tanda Tangan	8.2	6	11	Akurat dan konsisten terhadap *hash* dokumen.
Pemrosesan Dokumen (1 penandatangan)	156	142	189	Termasuk proses *hashing* dan embed tanda tangan.
Pemrosesan Dokumen (3 penandatangan)	298	276	341	Meningkat proporsional sesuai jumlah penandatangan.

3.3. Analisis Pengujian Multi-Signature

Pengujian multi-signature dilakukan untuk memastikan bahwa sistem hanya mengesahkan dokumen apabila seluruh tanda tangan digital berhasil diverifikasi. Pengujian dilakukan pada

dokumen KKP dengan satu penandatangan, KHS dengan dua penandatangan, serta Persetujuan Hasil dengan tiga penandatangan.

Rekapitulasi hasil pengujian multi-signature ditunjukkan pada Tabel 2. Hasil Pengujian Multi-Signature pada Dokumen Akademik. Hasil pengujian menunjukkan tingkat keberhasilan verifikasi sebesar 100% pada seluruh skenario, yang membuktikan bahwa sistem mampu menjamin otorisasi kolektif secara kriptografis.

Tabel 2. Hasil Pengujian Multi-Signature pada Dokumen Akademik

Jenis Dokumen	Jumlah Penandatangan	Jumlah Tanda Tangan Diuji	Tanda Tangan Valid	Tanda Tangan Tidak Valid	Tingkat Keberhasilan
KKP	1	1	1	0	100%
KHS	2	2	2	0	100%
Persetujuan Hasil	3	3	3	0	100%

3.4. Pembahasan

Berdasarkan hasil pengujian, integrasi algoritma EdDSA (Ed25519) dengan skema multi-signature dan QR Code memberikan peningkatan signifikan terhadap keamanan dan efisiensi sistem verifikasi dokumen akademik. Dibandingkan dengan pendekatan konvensional, sistem ini mampu mengurangi risiko pemalsuan dokumen, mempercepat proses verifikasi, serta memungkinkan verifikasi dilakukan secara mandiri.

Hasil penelitian ini memperkuat temuan penelitian sebelumnya yang menyatakan bahwa EdDSA memiliki performa lebih baik dibandingkan algoritma kriptografi klasik, dengan kontribusi tambahan berupa penerapan skema multi-signature pada lingkungan akademik.

4. Kesimpulan

Penelitian ini berhasil mengimplementasikan sistem tanda tangan digital berbasis QR Code dengan mengintegrasikan algoritma EdDSA varian Ed25519 dan skema multi-signature untuk verifikasi dokumen akademik. Sistem mampu menjamin keaslian, integritas, dan otorisasi kolektif dokumen akademik dengan tingkat keberhasilan verifikasi 100% dan waktu eksekusi di bawah 0,3 detik. Dengan demikian, sistem yang diusulkan layak diterapkan sebagai solusi verifikasi dokumen akademik digital yang aman, efisien, dan andal.

5. Saran

Penelitian selanjutnya disarankan untuk mengembangkan sistem tanda tangan digital ini dengan menambahkan mekanisme manajemen kunci yang lebih terpusat dan aman, seperti integrasi dengan hardware security module (HSM) atau layanan manajemen kunci berbasis cloud. Selain itu, sistem dapat diperluas dengan menerapkan skema multi-signature yang lebih kompleks, seperti threshold signature, sehingga fleksibilitas otorisasi dokumen dapat ditingkatkan. Pengujian lebih lanjut juga disarankan pada skala pengguna yang lebih besar dan berbagai jenis dokumen akademik lainnya, serta evaluasi terhadap ketahanan sistem pada kondisi lingkungan yang berbeda, seperti kualitas cetak QR Code dan variasi perangkat pemindai, guna memastikan keandalan sistem dalam penerapan nyata di lingkungan perguruan tinggi.

Referensi:

[1] A. Andriati dan M. Batubara, “Keabsahan Tanda Tangan Digital Berbasis QR Code dalam Perspektif Undang-Undang Informasi dan Transaksi Elektronik,” Jurnal Hukum dan Teknologi Informasi, vol. 5, no. 2, pp. 112–121, 2024.
[2] R. Wahyudi dan A. Ristian, “Implementasi QR Code pada Sistem Verifikasi Dokumen Digital,” Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 11, no. 1, pp. 45–54, 2024.
[3] M. Wellem, Y. Nataliani, dan D. Iriani, “Academic Document Authentication Using ECDSA and QR Code,” Journal of Information Security, vol. 13, no. 4, pp. 233–242, 2022.
[4] G. Shukla dan R. Prasad, “Security Analysis of Random Number Generation in ECDSA,” International Journal of Cryptography Research, vol. 9, no. 1, pp. 1–10, 2021.
[5] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, dan B.-Y. Yang, “High-Speed High-Security Signatures,” Journal of Cryptographic Engineering, vol. 2, no. 2, pp. 77–89, 2012.
[6] S. Carita dan D. Wahyuni, “Analisis Performa Algoritma Ed25519 pada Sistem Tanda Tangan Digital,” Jurnal Informatika dan Keamanan Informasi, vol. 7, no. 3, pp. 201–210, 2022.
[7] S. Yuliana dan R. Walidaniy, “Integrasi EdDSA dan Multi-Signature Berbasis QR Code untuk Otentikasi Dokumen Digital,” Jurnal Sistem Informasi dan Keamanan, vol. 6, no. 2, pp. 98–107, 2024.
[8] M. Noor, “Threshold and Multi-Signature Scheme for Secure Document Authorization,” International Journal of Computer Security, vol. 15, no. 1, pp. 34–43, 2021.
[9] S. Yuniati dan A. Sidiq, “Penerapan Multi-Signature untuk Otorisasi Dokumen Digital,” Jurnal Teknologi dan Sistem Komputer, vol. 8, no. 4, pp. 289–297, 2020.
[10] A. Halim, R. Siregar, dan M. Lubis, “Penerapan QR Code sebagai Tanda Tangan Digital pada Sistem Surat Menyurat,” Jurnal Informatika STMIK, vol. 12, no. 2, pp. 55–63, 2024.
[11] E. Gunawan, F. Nugroho, dan D. Saputra, “Digital Signature Berbasis QR Code untuk Verifikasi Dokumen Elektronik,” Jurnal Ilmu Komputer dan Aplikasi, vol. 10, no. 1, pp. 1–9, 2024.
[12] P. Serengil dan A. Ozpinar, “Performance Comparison of RSA, ECDSA, and EdDSA in Digital Signature Systems,” Applied Cryptography Journal, vol. 14, no. 3, pp. 155–166, 2025.
[13] S. Guruprakash dan S. Koppu, “Deterministic Signature Schemes and Their Resistance to Side-Channel Attacks,” IEEE Access, vol. 10, pp. 112345–112356, 2022.
[14] R. Mainzaghi, L. Conti, dan F. Martinelli, “QR Code-Based Digital Signature Verification for Offline Documents,” Future Internet, vol. 17, no. 2, pp. 1–15, 2025.
[15] A. Eka Sintyaningrum dan A. Ashar, “Verifikasi Sertifikat Digital Menggunakan QR Code dan Tanda Tangan Elektronik,” Jurnal Teknologi Informasi, vol. 9, no. 3, pp. 180–189, 2022.