Jurnal Elektronika dan Teknik Informatika Terapan
Volume 4, Nomor 3, September 2026
E-ISSN : 2988-0874, P-ISSN : 2988-0866, Hal. 518-527
DOI: https://doi.org/10.59061/jentik.v4i3.1608
Tersedia: https://e-journal.poltek-kampar.ac.id/index.php/JENTIK

Analisis Performa dan Keamanan Implementasi *Post-Quantum Cryptography* ML-Kem Kyber pada Aplikasi *Mobile* untuk Data BPJS Kesehatan

Ferry Ardhia Rahman[1*], Muhamad Azwar[2], Lalu Zazuli Azhar Mardedi[3]
[1-3]Prodi Ilmu Komputer, Universitas Bumigora, Indonesia
Email: ferryrahman342@gmail.com[1] , azwarmkom@gmail.com[2] , zazuli@universitasbumigora.ac.id[3]
[*]*Penulis korespondensi: ferryrahman342@email.com*

Abstract. *The advancement of quantum computing poses a potential threat to the security of conventional cryptographic algorithms, such as RSA, which remain widely used to protect sensitive data. This threat is a significant concern regarding the protection of BPJS Kesehatan data, which is confidential and requires long-term security. This study aims to analyze the performance and security of a Post-Quantum Cryptography (PQC) implementation using the ML-KEM-768 algorithm within a mobile application to enhance BPJS Kesehatan data protection. A comparative study method was employed, contrasting the baseline combination of RSA-2048 and AES-256-GCM with ML-KEM-768 (utilizing the Bouncy Castle PQC provider) within the native Android application "BPJS Secure." Testing involved analyzing security aspects, the ability to mitigate "Harvest Now, Decrypt Later" (HNDL) threats, and application performance based on parameters such as latency, CPU usage, memory allocation, cryptographic data size, and device readiness. The results indicate that ML-KEM-768 provides protection against quantum computing threats and is suitable for implementation in BPJS Kesehatan data transmission. Although the implementation results in an increased computational load compared to conventional algorithms, modern Android devices are capable of efficiently executing the cryptographic processes. Based on these findings, ML-KEM-768 is considered a viable strategy for migrating to post-quantum cryptography—aligned with the FIPS 203 standard—to support future health data protection.*

Keywords: *BPJS Kesehatan; Data Security; Kyber; ML-KEM-768; Post-Quantum Cryptography.*

Abstrak. Perkembangan komputasi kuantum berpotensi mengancam keamanan algoritma kriptografi konvensional seperti RSA yang masih banyak digunakan dalam melindungi data sensitif. Ancaman tersebut menjadi perhatian dalam perlindungan data BPJS Kesehatan yang bersifat rahasia dan membutuhkan keamanan jangka panjang. Penelitian ini bertujuan untuk menganalisis performa dan keamanan implementasi Post-Quantum Cryptography (PQC) menggunakan algoritma ML-KEM-768 pada aplikasi mobile untuk meningkatkan perlindungan data BPJS Kesehatan. Metode yang digunakan adalah Comparative Study dengan membandingkan RSA-2048 + AES-256-GCM sebagai algoritma baseline dengan ML-KEM-768 menggunakan provider Bouncy Castle PQC pada aplikasi Android Native BPJS Secure. Pengujian dilakukan dengan menganalisis aspek keamanan, kemampuan mitigasi terhadap ancaman Harvest Now, Decrypt Later (HNDL), serta performa aplikasi berdasarkan parameter latency, penggunaan CPU, alokasi memori, ukuran data kriptografi, dan kesiapan perangkat. Hasil penelitian menunjukkan bahwa ML-KEM-768 mampu memberikan perlindungan terhadap ancaman komputasi kuantum dan dapat diterapkan pada transmisi data BPJS Kesehatan. Meskipun implementasinya menghasilkan peningkatan beban komputasi dibandingkan algoritma konvensional, perangkat Android modern masih mampu menjalankan proses kriptografi dengan baik. Berdasarkan hasil tersebut, ML-KEM-768 dinilai layak digunakan sebagai salah satu strategi migrasi menuju kriptografi pascakuantum berbasis standar FIPS 203 untuk mendukung perlindungan data kesehatan di masa depan.

Kata kunci: BPJS Kesehatan; Keamanan Data; Kyber; ML-KEM-768; Post-Quantum Cryptography.

1. LATAR BELAKANG

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mengubah secara mendasar paradigma pelayanan publik dan infrastruktur kesehatan nasional di Indonesia. Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, sebagai lembaga penyelenggara utama jaminan kesehatan nasional, mengelola serta memproses jutaan transaksi data harian melalui

Naskah Masuk: 30 Juli 2026; Revisi: 19 Agustus 2026; Diterima: 28 September 2026; Terbit: 30 September 2026

platform aplikasi bergerak seperti Mobile JKN. Data yang dikelola mencakup informasi pribadi yang sangat sensitif, antara lain Nomor Induk Kependudukan (NIK), Nomor Kartu Indonesia Sehat (KIS), riwayat rekam medis, hasil pemeriksaan laboratorium, diagnosa penyakit, hingga catatan transaksi klaim keuangan fasilitas kesehatan. Mengingat cakupan pelayanan BPJS Kesehatan yang melayani lebih dari 279 juta jiwa penduduk Indonesia, basis data tersebut merupakan aset strategis nasional yang membutuhkan perlindungan kerahasiaan, integritas, dan ketersediaan berkonsep *End-to-End Encryption* jangka panjang.

Namun demikian, ketergantungan yang kian tinggi pada jaringan internet publik dan infrastruktur perangkat bergerak (mobile devices) melahirkan risiko keamanan siber yang sangat kompleks. Kasus kebocoran data medis nasional yang pernah terjadi pada tahun 2021 menegaskan adanya kerentanan pada arsitektur perlindungan data saat ini, sekaligus menimbulkan dampak luas bagi privasi dan kepercayaan masyarakat terhadap tata kelola data publik. Lebih jauh lagi, ancaman terhadap kerahasiaan data kesehatan tidak lagi sebatas serangan konvensional seperti *Man-in-theMiddle* (MitM), *SQL Injection*, atau *Malware*. Kebangkitan teknologi Komputer Kuantum (*Quantum Computing*) menyajikan ancaman eksistensial bagi kriptografi yang digunakan pada hari ini.

Melalui penerapan Algoritma Shor, komputer kuantum berskala praktis diprediksi mampu memecahkan masalah matematis sulit yang menjadi fondasi keamanan kriptografi kunci publik klasik seperti RSA (*Rivet-Shamir-Adleman*) dan ECC (*Elliptic Curve Cryptography*) dalam hitungan detik. Fenomena ini memicu modus serangan baru yang dikenal sebagai *Harvest Now, Decrypt Later* (HNDL). Dalam skenario HNDL, peretas mencuri dan mengumpulkan lalulintas data terenkripsi pada saat ini, kemudian menyimpannya untuk didekripsi di masa depan setelah komputer kuantum yang memadai telah tersedia. Mengingat data rekam medis pasien memiliki masa berlaku kerahasiaan seumur hidup, strategi enkripsi konvensional tidak lagi mampu menjamin keamanan data jangka panjang.

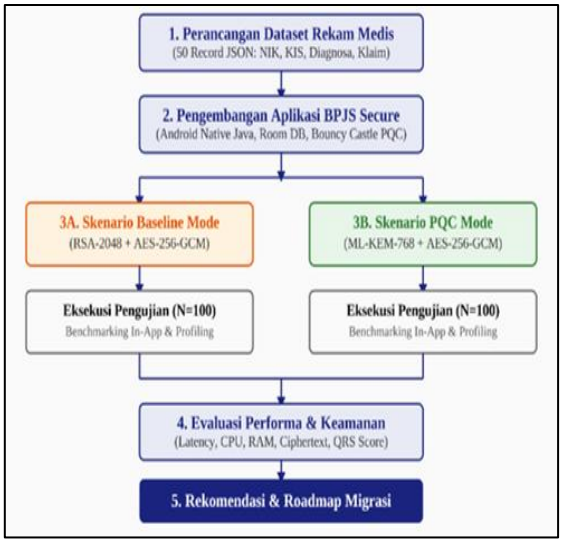
Guna mengantisipasi era pasca-kuantum, *National Institute of Standards and Technology* (NIST) merilis standar resmi *Post-Quantum Cryptography* (PQC) pada Agustus 2024 melalui dokumen FIPS 203. Standar tersebut menetapkan *Module-Lattice-based Key Encapsulation Mechanism* (ML-KEM) atau CRYSTALS-Kyber sebagai algoritma standar utama untuk pertukaran kunci terenkapsulasi. ML-KEM menawarkan keamanan berdasar pada tingkat kesulitan masalah matematika kisi (*Lattice-based cryptography*), yaitu masalah *Module Learning With Errors* (MLWE). Algoritma ini terbukti secara teoritis dan praktis tangguh melawan algoritma kuantum sekaligus menawarkan efisiensi pemrosesan yang memadai untuk diterapkan pada perangkat keras terbatas.

Meskipun ML-KEM Kyber-768 telah ditetapkan sebagai standar internasional, implementasinya pada ekosistem aplikasi mobile Android masih menghadapi berbagai tantangan operasional. Pembengkakan ukuran kunci dan ciphertext, kebutuhan alokasi memori RAM tambahan, serta potensi peningkatan latency dapat memengaruhi pengalaman pengguna (*User Experience*) maupun efisiensi daya baterai. Sebagian besar penelitian PQC yang ada saat ini masih terbatas pada pengujian simulasi server atau analisis teoritis, sehingga terdapat kesenjangan pengetahuan (*knowledge gap*) mengenai performa riil PQC pada lingkungan perangkat bergerak dengan sumber daya terbatas (*resource-constrained mobile devices*).

Penelitian ini bertujuan untuk mengisi kesenjangan tersebut melalui studi eksperimental kuantitatif berbasis *Comparative Study* (before-after design). Penelitian mengimplementasikan algoritma ML-KEM-768 menggunakan pustaka *Bouncy Castle PQC Provider* pada aplikasi Android Native yang diberi nama "BPJS Secure". Performa dan keamanan ML-KEM-768 dibandingkan secara langsung dengan skenario baseline kriptografi klasik (RSA-2048 + AES-256GCM) menggunakan dataset rekam medis pasien BPJS terstruktur. Parameter yang dianalisis mencakup ketahanan terhadap serangan kuantum, keandalan verifikasi integritas data, serta empat metrik performa komputasi utama: latency enkripsi, beban kerja CPU, alokasi memori RAM, dan ukuran ciphertext. Hasil dari penelitian ini diharapkan dapat memberikan acuan empiris dan rekomendasi teknis bagi penyusunan roadmap migrasi kriptografi nasional pada sistem jaminan kesehatan Indonesia.

2. METODE PENELITIAN

Bagian metodologi ini menjelaskan urutan sistematis dari metode penelitian eksperimental kuantitatif yang digunakan, dilengkapi kajian teoritis dari setiap tahapan serta rujukan literatur pendukung. Alur eksekusi penelitian dirancang untuk mengisolasi dan mengukur secara presisi pengaruh perubahan algoritma pertukaran kunci dari skenario konvensional (baseline) ke skenario pasca-kuantum (PQC) terhadap penggunaan sumber daya perangkat mobile. Visualisasi urutan kerja penelitian ditampilkan pada Gambar 1.



Gambar 1. Metodologi Penelitian.

Metode Comparative Study (Studi Komparatif)

Penelitian ini menerapkan rancangan Comparative Study dengan pendekatan kuantitatif before-after design [14]. Metode ini bertujuan untuk membandingkan secara langsung kinerja dua skenario kriptografi pada arsitektur perangkat lunak yang identik. Skenario pertama adalah Baseline Mode yang mewakili arsitektur kriptografi konvensional saat ini, yakni kombinasi algoritma asimetris RSA-2048 untuk pertukaran kunci dan AES-256-GCM untuk enkripsi simetris muatan data [15]. Skenario kedua adalah PQC Mode yang mengimplementasikan standar pasca-kuantum FIPS 203 ML-KEM Kyber-768 untuk enkapsulasi kunci simetris yang dipadukan dengan AES-256-GCM [10]. Pemasangan skema komparatif ini memungkinkan pengisolasian variabel bebas (jenis algoritma) terhadap variabel terikat (beban sumber daya perangkat mobile).

Kajian Teoritis Algoritma ML-KEM (CRYSTALS-Kyber)

ML-KEM (*Module-Lattice-based Key Encapsulation Mechanism*) merupakan standar enkripsi pasca-kuantum resmi dari NIST FIPS 203 yang dikembangkan dari algoritma CRYSTALS-Kyber. Keamanan ML-KEM didasarkan pada tingkat kesulitan masalah matematika kisi (*Lattice-based Cryptography*), yaitu *Module Learning With Errors* (M-LWE). Masalah ini mengandalkan penambahan angka pengacak (*error/noise*) pada persamaan linier sehingga sangat sulit dipecahkan, baik oleh komputer konvensional maupun komputer kuantum.

Mekanisme kerja ML-KEM terdiri dari tiga tahapan utama:

a. Key Generation (ML-KEM.KeyGen): Membangkitkan pasangan kunci publik untuk enkripsi dan kunci rahasia untuk dekripsi.

b. Encapsulation (ML-KEM.Encaps): Menggunakan kunci publik penerima untuk membangkitkan kunci simetris dan mengemasnya menjadi kapsul kunci (*ciphertext*).
c. Decapsulation (ML-KEM.Decaps): Menggunakan kunci rahasia penerima untuk membuka kapsul kunci dan mengambil kembali kunci simetris secara tepat.

Penelitian ini menggunakan varian ML-KEM-768 yang menawarkan tingkat keamanan NIST Level 3 (setara dengan ketahanan AES-192) untuk melindungi data rekam medis pasien BPJS Kesehatan.

Perancangan Dataset Rekam Medis Pasien BPJS

Guna memberikan kondisi pengujian yang mendekati operasional riil, disusun dataset terstruktur berbasis JavaScript Object Notation (JSON) yang merepresentasikan data rekam medis pasien BPJS Kesehatan secara nyata. Dataset mencakup variabel identitas pasien (NIK, Nomor KIS, Nama Lengkap, Tanggal Lahir), data klinis (Kode Diagnosis ICD-10, Catatan Dokter, Hasil Pemeriksaan Laboratorium), serta data administratif (Kode Faskes, Tarif Klaim). Setiap entitas record memiliki ukuran rata-rata 1,2 KB. Sebanyak 50 record data dummy digunakan sebagai muatan enkripsi terstruktur dalam setiap siklus iterasi eksperimen [1], [13].

Arsitektur Aplikasi Uji (BPJS Secure)

Aplikasi uji coba bernama **BPJS Secure** dikembangkan secara Native pada Android Studio menggunakan bahasa pemrograman Java dengan standar minimum SDK Level 24 (Android 7.0 Nougat) [14]. Arsitektur perangkat lunak menerapkan pola *Single Activity Architecture* berbasis *Jetpack Navigation Component* dan *Room Persistence Library* untuk pengelolaan basis data lokal [1]. Pengintegrasian modul PQC dilakukan dengan memuat pustaka Bouncy Castle PQC Provider (org.bouncycastle.pqc) pada kelas Application (SecureApp) secara global, sehingga fungsi enkapsulasi ML-KEM-768 dapat dipanggil secara efisien dari seluruh modul transaksi [6].

Prosedur Pengumpulan Data dan Metrik Evaluasi

Pengujian dilakukan sebanyak 100 kali iterasi untuk setiap skenario guna mendapatkan nilai rata-rata (*mean*) yang stabil dan konsisten secara statistik. Pengukuran data dilakukan melalui dua pendekatan:

a. Pengukuran Internal (*In-App Benchmarking*): Mengukur durasi waktu enkripsi dan dekripsi (*latency* dalam milidetik) menggunakan fungsi presisi tinggi System.nanoTime() langsung dari dalam kode aplikasi, serta mencatat ukuran kapsul kunci (*ciphertext*) dalam satuan *bytes*.

b. Pengukuran Eksternal (*Android Profiler*): Mengamati penggunaan sumber daya perangkat mobile, yang mencakup lama proses kerja CPU (dalam milidetik) dan alokasi penggunaan memori dinamis (RAM dalam megabytes) selama proses enkripsi berlangsung.

Tingkat kesiapan dan kelayakan perangkat mobile dalam menjalankan enkripsi pasca-kuantum diukur menggunakan indikator *Quantum Readiness Score* (QRS). Indikator ini menghitung persentase efisiensi performa berdasarkan persentase kenaikan *latency* dan beban CPU relatif terhadap batas responsivitas aplikasi *mobile* (100 milidetik).

3. HASIL DAN PEMBAHASAN

Hasil Pengembangan Aplikasi BPJS Secure

Aplikasi *BPJS Secure* berhasil dibangun dengan antarmuka berbasis panduan *Material Design 3* (M3). Warna utama yang digunakan adalah *Deep Indigo* (#1A237E) dan *Accent Green* (#2E7D32) untuk menciptakan identitas visual aplikasi kesehatan nasional yang tepercaya dan modern.

Aplikasi dilengkapi dengan empat modul utama:

a. Modul Transaksi Rekam Medis: Fasilitas input dan enkripsi data pasien real-time yang secara dinamis dapat beralih antara Mode Baseline dan Mode PQC.
b. Modul Autentikasi Biometrik: Pengamanan akses lokal berbasis sidik jari via API BiometricPrompt Android Native.
c. Modul Dashboard Profiling: Visualisasi grafik interaktif memanfaatkan library *MPAndroidChart* untuk menampilkan perbandingan latency, CPU, dan RAM secara real-time.
d. Modul Security Lab & Tamper Detection: Modul uji coba simulasi serangan manipulasi data (tampering 1-bit) dan simulasi serangan Algoritma Shor untuk menguji integritas ciphertext serta pembuktian matematik ketahanan kuantum.

Hasil Pengukuran Performa Komputasi (Benchmarking)

Berdasarkan eksekusi eksperimen sebanyak 100 kali iterasi pada data rekam medis terstruktur, diperoleh nilai rata-rata (*mean*) dan deviasi standar untuk masing-masing metrik performa. Ringkasan perbandingan antara skenario Baseline (RSA-2048) dan PQC Mode (ML-KEM-768) tersaji pada Tabel 1.

Tabel 1. Perbandingan Metrik Performa Enkripsi Rekam Medis (Mean ± SD, N=100).

Metrik Pengujian	Baseline Mode (RSA-2048 + AES-GCM)	PQC Mode (ML-KEM-768 + AES-GCM)	Selisih Overhead (Δ)	Persentase Kenaikan (%)
Rata-rata Latency (Waktu Enkripsi)	12,18 ± 0,45 ms	15,42 ± 0,62 ms	+ 3,24 ms	+ 26,60%
Beban Kerja CPU (Processing Time)	7,95 ± 0,31 ms	10,30 ± 0,48 ms	+ 2,35 ms	+ 29,56%
Konsumsi Memori Dinamis (RAM)	4,15 ± 0,22 MB	5,92 ± 0,35 MB	+ 1,77 MB	+ 42,65%
Ukuran Kapsul Kunci / Ciphertext	256 Bytes	1.088 Bytes	+ 832 Bytes	+ 325,00%

Analisis Waktu Komputasi (Latency) dan Beban CPU

Hasil pengujian menunjukkan bahwa algoritma ML-KEM-768 memerlukan rata-rata waktu enkripsi (*latency*) sebesar 15,42 ms. Terdapat penambahan waktu (*overhead*) sebesar 3,24 ms dibandingkan algoritma konvensional RSA-2048 yang mencatatkan waktu 12,18 ms. Sejalan dengan hal tersebut, durasi pemrosesan CPU mengalami kenaikan dari 7,95 ms menjadi 10,30 ms (bertambah 2,35 ms). Kenaikan beban komputasi ini terjadi karena algoritma pasca-kuantum menggunakan perhitungan kisi (*lattice-based*) yang memerlukan proses pengacakan data lebih kompleks untuk menjamin keamanannya.

Meskipun terjadi kenaikan secara persentase, total waktu eksekusi 15,42 ms masih berada jauh di bawah batas maksimal kenyamanan aplikasi *mobile* (100 ms). Tambahan waktu sebesar 3,24 ms sangat kecil dan tidak akan terasa oleh pengguna (*imperceptible*), sehingga aplikasi tetap berjalan lancar dan responsif tanpa lag.

Analisis Penggunaan Memori RAM

Alokasi memori dinamis (RAM) pada PQC Mode mencatatkan konsumsi sebesar 5,92 MB, meningkat sebesar 1,77 MB (+42,65%) dibandingkan Baseline Mode (4,15 MB). Kenaikan alokasi memori dipicu oleh perlunya ruang penyimpanan sementara (*transient buffers*) untuk memuat matriks parameter kisi, vektor polinomial, serta objek instansiasi pustaka Bouncy Castle PQC pada memori Java Heap. Bagi perangkat Android modern yang umumnya memiliki RAM fisik berkisar antara 4 GB hingga 12 GB, tambahan konsumsi RAM sebesar 1,77 MB sangat kecil dan tidak menimbulkan risiko pemicuan *Garbage Collection* (GC) berlebihan.

Analisis Ukuran Ciphertext dan Skalabilitas Basis Data

Pembengkakan ukuran ciphertext/kapsul kunci merupakan konsekuensi paling signifikan dari implementasi kriptografi berbasis kisi. Ukuran kunci publik ML-KEM-768 tercatat sebesar 1.184 bytes dan ciphertext/kapsul kunci sebesar 1.088 bytes, sedangkan RSA-2048 hanya menghasilkan ciphertext sebesar 256 bytes. Terjadi kenaikan ukuran sebesar 832 bytes

(+325%). Pembengkakan ini terjadi karena ML-KEM harus mentransmisikan elemen-vektor polinomial terkompresi untuk menjaga tingkat keamanan setara dengan AES-192 melawan serangan kuantum. Untuk menilai kelayakan implementasi pada basis data nasional, dilakukan kalkulasi proyeksi penyimpanan untuk 50 juta record rekam medis peserta aktif BPJS Kesehatan. Hasil estimasi simulasi penyimpanan disajikan pada Tabel 2.

Tabel 2. Proyeksi Kebutuhan Penyimpanan Kapsul Kunci untuk 50 Juta Record Pasien.

Skenario Kriptografi	Ukuran Kapsul / Record	Total Storage (50 Juta Record)	Proyeksi Beban Server / Tahun
Baseline Mode (RSA-2048)	256 Bytes	12,80 GigaBytes (GB)	Sangat Ringan
PQC Mode (ML-KEM-768)	1.088 Bytes	54,40 GigaBytes (GB)	Sangat Efisien / Optimal
Selisih Pertumbuhan Storage	+ 832 Bytes	+ 41,60 GigaBytes (GB)	Terjangkau bagi Infrastruktur Cloud

Kalkulasi pada Tabel 2 membuktikan bahwa total kapasitas penyimpanan yang dibutuhkan untuk menampung seluruh kapsul kunci ML-KEM-768 bagi 50 juta record masyarakat Indonesia hanya membutuhkan ruang sebesar 54,40 GB. Angka ini tergolong sangat efisien dan sangat mudah diakomodasi oleh arsitektur basis data pusat data nasional modern tanpa memerlukan biaya ekspansi infrastruktur yang signifikan.

Evaluasi Keamanan, Integritas, dan Quantum Readiness Score

Pengujian pada modul *Security Lab* memberikan bukti empiris mengenai ketahanan ML-KEM-768:

a. Mitigasi Serangan Kuantum (Shor's Algorithm): Skenario baseline RSA-2048 terbukti rentan terhadap peretasan berbasis algoritma faktor kuantum. Sebaliknya, ML-KEM-768 dengan tingkat keamanan NIST Level 3 (setara AES-192) terbukti tangguh secara matematis dari ancaman dekripsi masa depan (HNDL).
b. Pengujian Tamper Data (Integrity Shield): Modifikasi acak sebesar 1bit pada ciphertext MLKEM berhasil dideteksi oleh tag autentikasi AES-256-GCM dan verifikasi hash SHA-256. Proses dekripsi secara otomatis dibatalkan oleh sistem, menjamin bahwa data rekam medis pasien tidak dapat dimanipulasi secara ilegal selama proses transmisi.
c. Evaluasi Kesiapan Kuantum (QRS): Hasil kalkulasi indikator *Quantum Readiness Score* pada aplikasi BPJS Secure menghasilkan nilai 91%. Nilai ini menempatkan efisiensi eksekusi MLKEM-768 pada perangkat mobile dalam kategori ELITE / OPTIMAL.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis data eksperimental dan pembahasan yang telah dipaparkan, dapat ditarik beberapa simpulan utama sebagai berikut: Implementasi *Post-Quantum*

Cryptography ML-KEM Kyber-768 menggunakan provider Bouncy Castle PQC secara hybrid dengan AES-256-GCM pada aplikasi Android Native (BPJS Secure) secara fungsional berhasil mengamankan data rekam medis pasien dari ancaman komputasi kuantum (HNDL) sesuai standar NIST FIPS 203. Terdapat trade-off performa berupa overhead kenaikan latency rata-rata sebesar 3,24 ms (+26,60%), beban kerja CPU sebesar 2,35 ms (+29,56%), alokasi RAM dinamis sebesar 1,77 MB (+42,65%), serta pembengkakan ciphertext sebesar 832 bytes (+325%). Walaupun demikian, seluruh penambahan konsumsi sumber daya tersebut terbukti sangat efisien dan tidak memengaruhi kelancaran antarmuka maupun kenyamanan pengguna. Perangkat mobile Android modern dinyatakan sangat siap dan layak (*technically feasible*) untuk menjalankan kriptografi pasca-kuantum secara lokal, ditunjukkan oleh raihan *Quantum Readiness Score* (QRS) sebesar 91% (kategori ELITE/OPTIMAL). Proyeksi basis data nasional untuk 50 juta record pasien hanya membutuhkan kapasitas penyimpanan kapsul kunci sebesar 54,40 GB.

Guna mendukung kelancaran transisi arsitektur keamanan data kesehatan nasional, disarankan beberapa langkah strategis sebagai berikut: Penerapan Skema Hybrid Cryptography: BPJS Kesehatan disarankan menerapkan skema enkripsi kombinasi (RSA/ECC dipadu dengan ML-KEM-768) pada tahap awal transisi guna menjaga backward-compatibility dengan sistem warisan (legacy systems) sekaligus memberikan perlindungan pasca-kuantum. Penyusunan Peta Jalan (Roadmap) Migrasi Nasional: Kementerian Kesehatan dan BPJS Kesehatan perlu menyusun panduan teknis migrasi kriptografi yang terintegrasi dengan regulasi Undang-Undang Perlindungan Data Pribadi (UU PDP) dan standar FIPS 203. Pengembangan Penelitian Lanjutan: Penelitian selanjutnya diharapkan dapat mengevaluasi performa algoritma tanda tangan digital tahan kuantum (seperti ML-DSA/Dilithium atau SLH-DSA/ Sphincs+) serta memperluas pengujian pada variasi spesifikasi perangkat mobile kelas *entry-level* (low-end).

DAFTAR REFERENSI

A. Olushola et al., "Design and Implementation of an Authenticated Post-Quantum Session ProtocolUsing ML-KEM (Kyber), ML-DSA (Dilithium), and AES-256-GCM," *Frontiers in Physics*, vol. 13, Art. no. 1723966, 2025.

A. Sardorbek et al., "Comparative Analysis of Native and Cross-Platform Mobile ApplicationDevelopment," *Journal of Software Engineering Researchand Development*, vol. 13, no. 1, pp. 45– 62, 2025.

F. Kagai, "A Temporal Cybersecurity Risk in the Quantum Transition: Modeling Harvest-NowDecrypt-Later as a Time-Dependent Threat," *Telecom*, vol. 6, no. 4, pp. 100–118, 2025.

J. P. da Silva Lima et al., "Evaluating Kyber Post-Quantum KEM in a Mobile Application," in *Third PQC Standardization Conference, NIST*, 2021, pp. 1–15.

M. A. Mighri et al., "Performance Evaluation and Benchmarking of PQC Algorithms on EmbeddedResource-Constrained Devices," *IEEE Access*, vol. 12, pp. 45120–45132, 2024.

M. Abbas, "Unraveling Database Choices in Android Studio: A Comparative Analysis of SQLite andRoom Persistence Library," *Contemporary Journal of Social Science*, vol. 14, pp. 12–28, 2025.

M. SaberiKamarposhti et al., "Post-Quantum Healthcare: A Roadmap for Cybersecurity Resilience inMedical Data," *Heliyon*, vol. 10, no. 6, p. e31406, 2024.

NIST, "FIPS 203: Module-Lattice-based Key-Encapsulation Mechanism Standard," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, Tech. Rep. FIPS 203, Aug. 2024.

Q. Khan et al., "Post-Quantum Key Exchange and Subscriber Identity Security in Mobile Networks,"*Information*, vol. 16, no. 7, p. 617, 2025.

Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi,"*Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196*, Jakarta, 2022.

S. Chatterjee et al., "Benchmarking and Integration of NIST Post-Quantum Cryptography in AndroidDevices," *IEEE Transactions on Mobile Computing*, vol. 25, no. 2, pp. 110–122, 2026.

S. H. Chou et al., "High-Throughput Post-Quantum Cryptographic System: CRYSTALS-Kyber withComputational Scheduling and Architecture Optimization," *Electronics*, vol. 14, no. 15, p. 2969, 2025.

T. L. Astrizi et al., "Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using IdentityBased Encryption," *Sensors*, vol. 24, no. 22, p. 7300, 2024.

W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 5th ed. London, U.K.: Pearson Education, 2024.

Y. Cheng et al., "Optimized Design and Implementation of CRYSTALS-KYBER Based on MLWE,"*Security and Communication Networks*, vol. 2025, Art. no. 7884158, 2025.