Jurnal Ilmiah Ilmu Komputer & Elektronika (MURAKOM)
Volume. 2 Nomor. 2 April 2026
e-ISSN : 3123-1985; p-ISSN : 3110-4754, Hal.50-61
DOI: https://doi.org/10.64365/murakom.v2i2.290
Available online at: *https://jurnal.muaraedukasi.id/index.php/murakom*

Kerja Kriptografi Pasca-Kuantum untuk Jaringan Internet of Things (IoT)

Erlangga Ramadhan Fauzi[1*], Fitria Nur Aulia[2]
[1,2] Universitas Komputer, Indonesia
Alamat: Jl. Dipati Ukur No.112-116, Lebakgede, Kecamatan Coblong, Kota Bandung, Jawa Barat
Email : erlangga.fauzi@unikom.ac.id [1*], fitria.aulia@unikom.ac.id [2]
Korespondensi penulis ; erlangga.fauzi@unikom.ac.id

Abstract*. The advent of the quantum computing era poses a significant threat to conventional cryptographic systems widely used to secure Internet of Things (IoT) networks, such as RSA and ECC. Shor's algorithm enables quantum computers to solve the mathematical problems underlying these algorithms in a short amount of time, rendering the confidentiality and integrity of data on IoT devices vulnerable. This research aims to examine the implementation and performance of Post-Quantum Cryptography (PQC) as a security solution for IoT networks, which are characterized by resource constraints including limited computational power, memory, and energy consumption.The methodology employed in this research includes a literature review of PQC algorithms that have progressed to the final stages of the NIST standardization process, with a particular focus on lattice-based cryptography algorithms (such as CRYSTALS-Kyber and CRYSTALS-Dilithium) noted for their efficiency. The analysis involves comparing the security parameters, key sizes, ciphertext sizes, and computational speed of PQC algorithms against conventional cryptographic algorithms within a simulated IoT environment.The findings indicate that while PQC algorithms require larger key sizes and greater communication overhead compared to conventional algorithms, certain candidates like Kyber demonstrate competitive performance and are feasible for implementation on mid-to-high-tier IoT devices. However, for severely resource-constrained IoT devices, further optimization, both in terms of hardware and software, is still necessary.This research concludes that the transition towards post-quantum cryptography for IoT is inevitable. Recommendations include the gradual adoption of PQC standards and the development of hybrid protocols that combine classical and post-quantum cryptography during the transition period to ensure the long-term security sustainability of IoT networks.*

Keywords: *Post-Quantum Cryptography, Internet of Things (IoT), Network Security, Quantum Computing, Lattice-based Algorithms.*

Abstrak. Era komputasi kuantum membawa ancaman signifikan terhadap sistem kriptografi konvensional yang saat ini banyak digunakan untuk mengamankan jaringan Internet of Things (IoT), seperti RSA dan ECC. Algoritma Shor memungkinkan komputer kuantum memecahkan permasalahan matematis yang mendasari algoritma tersebut dalam waktu singkat, sehingga kerahasiaan dan integritas data pada perangkat IoT menjadi rentan. Penelitian ini bertujuan untuk mengkaji implementasi dan kinerja Kriptografi Pasca-Kuantum (PQC) sebagai solusi pengamanan untuk jaringan IoT yang memiliki keterbatasan sumber daya, seperti daya komputasi, memori, dan konsumsi energi.Metodologi yang digunakan dalam penelitian ini meliputi studi literatur terhadap algoritma PQC yang menjadi finalis dalam kompetisi NIST, khususnya algoritma berbasis lattice-based cryptography (seperti CRYSTALS-Kyber dan CRYSTALS-Dilithium) yang dinilai efisien. Analisis dilakukan dengan membandingkan parameter keamanan, ukuran kunci, ukuran ciphertext, serta kecepatan komputasi dari algoritma PQC terhadap algoritma kriptografi konvensional dalam simulasi lingkungan IoT.Hasil penelitian menunjukkan bahwa meskipun algoritma PQC memerlukan ukuran kunci dan overhead komunikasi yang lebih besar dibandingkan algoritma konvensional, beberapa kandidat seperti Kyber menunjukkan kinerja yang cukup kompetitif dan memungkinkan untuk diimplementasikan pada perangkat IoT dengan kelas menengah ke atas. Namun, untuk perangkat IoT dengan sumber daya sangat terbatas (constrained devices), masih diperlukan optimalisasi lebih lanjut, baik dari sisi perangkat keras maupun perangkat lunak.Penelitian ini menyimpulkan bahwa transisi menuju kriptografi pasca-kuantum untuk IoT adalah sebuah keniscayaan. Rekomendasi yang diberikan mencakup perlunya adopsi standar PQC secara bertahap serta pengembangan protokol hibrida yang menggabungkan kriptografi klasik dan PQC selama masa transisi, guna memastikan keberlanjutan keamanan jaringan IoT di masa depan.

Kata Kunci: Kriptografi Pasca-Kuantum, Internet of Things (IoT), Keamanan Jaringan, Komputasi Kuantum, Algoritma Lattice-based.

Received: Februari 15, 2026; Revised: Maret 20, 2026; Accepted: April 01, 2026; Online Available: April 02, 2026; Published: April 30, 2026

1. LATAR BELAKANG

Revolusi industri 4.0 dan transformasi digital telah mendorong adopsi teknologi *Internet of Things (IoT)* secara masih di berbagai sektor kehidupan, mulai dari rumah pintar (smart home), kota pintar *(smart city),* layanan kesehatan, hingga otomatisasi industri. Jaringan IoT menghubungkan miliaran perangkat, mulai dari sensor sederhana hingga perangkat kompleks, yang secara konstan mengumpulkan, mengirimkan, dan memproses data. Keberadaan data yang sangat besar dan sensitif ini menjadikan keamanan sebagai aspek krusial yang tidak dapat diabaikan. Kegagalan dalam mengamankan jaringan IoT dapat berakibat fatal, mulai dari kebocoran data pribadi hingga gangguan pada infrastruktur kritis.

Saat ini, sebagian besar protokol keamanan IoT bergantung pada kriptografi kunci publik konvensional, seperti RSA (Rivest-Shamir-Adleman) dan ECC *(Elliptic Curve Cryptography).* Keamanan algoritma ini bertumpu pada kesulitan matematis dalam menyelesaikan masalah faktorisasi bilangan besar dan logaritma diskrit. Selama beberapa dekade, algoritma ini terbukti tangguh terhadap serangan dari komputer klasik. Namun, lanskap keamanan global menghadapi ancaman eksistensial dengan pesatnya perkembangan komputasi kuantum.

Komputer kuantum, yang memanfaatkan prinsip-prinsip mekanika kuantum seperti superposisi dan belitan kuantum, memiliki potensi untuk memecahkan permasalahan matematis tersebut secara eksponensial lebih cepat daripada komputer klasik. Algoritma yang ditemukan oleh Peter Shor pada tahun 1994 secara teoritis mampu memfaktorkan bilangan besar dan menghitung logaritma diskrit dalam waktu polinomial. Ini berarti bahwa di masa depan, ketika komputer kuantum yang cukup kuat dan toleran terhadap kesalahan (fault-tolerant) berhasil direalisasikan, seluruh infrastruktur keamanan yang bergantung pada RSA dan ECC akan runtuh dalam sekejap. Ancaman ini dikenal dengan istilah "Harvest Now, Decrypt Later", di mana penyerang dapat mengumpulkan data terenkripsi saat ini dan menyimpannya hingga komputer kuantum tersedia untuk mendekripsinya di masa depan.

Permasalahan ini menjadi semakin kompleks ketika dikaitkan dengan karakteristik jaringan Internet of Things (IoT). Perangkat IoT umumnya memiliki keterbatasan sumber daya *(resource-constrained),* seperti daya komputasi yang rendah, kapasitas memori (RAM) dan penyimpanan (ROM) yang kecil, serta pasokan energi yang terbatas (bergantung pada baterai). Oleh karena itu, solusi kriptografi pasca-kuantum (PQC) yang ditawarkan tidak hanya harus aman secara kriptanalitik, tetapi juga harus efisien dan ringan agar dapat diimplementasikan pada perangkat dengan keterbatasan tersebut.

Kriptografi Pasca-Kuantum (PQC) merujuk pada algoritma kriptografi yang dirancang untuk tahan terhadap serangan dari komputer kuantum maupun klasik. Dalam upaya standardisasi global, National Institute of Standards and Technology (NIST) telah menyeleksi berbagai kandidat algoritma PQC, dengan algoritma berbasis lattice-based cryptography (seperti Kyber dan Dilithium) menunjukkan performa terbaik. Meskipun demikian, penelitian mengenai implementasi dan kerja algoritma PQC secara spesifik pada lingkungan IoT yang terbatas sumber daya masih terus berkembang dan menghadirkan tantangan tersendiri.

Berdasarkan latar belakang tersebut, penelitian ini dirumuskan untuk mengkaji secara mendalam mengenai kerja atau kinerja dari algoritma Kriptografi Pasca-Kuantum jika diterapkan pada jaringan Internet of Things (IoT). Fokus kajian akan meliputi aspek keamanan, efisiensi komputasi, konsumsi memori, serta energi, untuk menentukan kelayakan dan tantangan implementasinya di era komputasi kuantum yang akan datang.

2. KAJIAN TEORITIS

2.1 Internet of Things (IoT) dan Karakteristiknya

2.1.1 Definisi dan Arsitektur IoT

Internet of Things (IoT) merujuk pada jaringan global perangkat fisik yang tertanam dengan elektronik, perangkat lunak, sensor, dan konektivitas jaringan, yang memungkinkan objek-objek tersebut untuk mengumpulkan, bertukar, dan memproses data . Arsitektur IoT umumnya terdiri dari tiga lapisan utama: perception layer (sensor dan aktuator), network layer (infrastruktur komunikasi), dan application layer (antarmuka pengguna dan aplikasi). Dalam perkembangannya, arsitektur end-edge-cloud menjadi populer untuk mengatasi latensi dan beban komputasi, di mana pemrosesan data dilakukan secara terdistribusi antara perangkat, gateway tepi, dan pusat data awan .

2.1.2 Karakteristik dan Keterbatasan Sumber Daya

Perangkat IoT memiliki karakteristik unik yang membedakannya dari sistem komputasi pada umumnya, terutama dalam hal keterbatasan sumber daya (resource-constrained) :

a. Daya Komputasi Terbatas: Umumnya menggunakan mikrokontroler dengan kecepatan clock rendah (ratusan MHz) seperti ARM Cortex-M series.
b. Memori Terbatas: Kapasitas RAM seringkali di bawah 10 KB hingga puluhan KB, dan ROM/Flash untuk penyimpanan kode juga terbatas .
c. Konsumsi Daya: Banyak perangkat beroperasi dengan baterai, sehingga efisiensi energi menjadi faktor kritis .

d. Bandwidth Jaringan: Koneksi jaringan seringkali tidak stabil dengan bandwidth terbatas, terutama untuk perangkat yang menggunakan teknologi LPWAN (*Low-Power Wide-Area Network*).

2.2 Ancaman Komputasi Kuantum terhadap Kriptografi Konvensional

2.2.1 Prinsip Dasar Komputasi Kuantum

Komputasi kuantum memanfaatkan fenomena mekanika kuantum seperti superposisi dan belitan (entanglement). Qubit, unit dasar informasi kuantum, dapat berada dalam superposisi dari state 0 dan 1 secara simultan, memungkinkan komputer kuantum memproses informasi dalam jumlah besar secara paralel . Kemampuan ini menjadi dasar bagi algoritma kuantum yang memiliki kompleksitas lebih rendah daripada algoritma klasik untuk masalah tertentu.

2.2.2 Algoritma Shor dan Dampaknya pada Kriptografi Kunci Publik

Algoritma yang ditemukan oleh Peter Shor pada tahun 1994 menjadi ancaman eksistensial bagi kriptografi kunci publik konvensional. Algoritma Shor mampu menyelesaikan masalah faktorisasi bilangan bulat dan logaritma diskrit dalam waktu polinomial . Hal ini secara langsung mengancam keamanan algoritma yang saat ini dominan digunakan:

a. RSA *(Rivest-Shamir-Adleman)*: Keamanannya bergantung pada kesulitan memfaktorkan hasil kali dua bilangan prima besar.
b. ECC *(Elliptic Curve Cryptography)*: Keamanannya bergantung pada kesulitan memecahkan Elliptic Curve Discrete Logarithm Problem (ECDLP).

Jika komputer kuantum skala besar yang toleran terhadap kesalahan (fault-tolerant) berhasil direalisasikan, maka seluruh infrastruktur keamanan yang bergantung pada RSA dan ECC akan menjadi rentan. Ancaman ini diperparah dengan strategi serangan "Harvest Now, Decrypt Later", di mana penyerang mengumpulkan data terenkripsi saat ini untuk didekripsi di masa depan ketika komputer kuantum telah tersedia

2.3 Kriptografi Pasca-Kuantum (Post-Quantum Cryptography/PQC)

2.3.1 Definisi dan Tujuan PQC

Kriptografi Pasca-Kuantum (PQC) didefinisikan sebagai algoritma kriptografi yang dirancang untuk tetap aman terhadap serangan dari komputer kuantum dan klasik . Tidak seperti Kriptografi Kuantum (yang memanfaatkan sifat kuantum seperti QKD/Quantum Key Distribution), PQC beroperasi pada komputer klasik tetapi menggunakan masalah matematika yang diyakini sulit dipecahkan baik oleh komputer klasik maupun kuantum.

2.3.2 Keluarga Algoritma PQC dan Landasan Matematis

Tabel pendekatan utama dalam PQC

Keluarga Algoritma	Landasan Matematis	Contoh Algoritma
Lattice-based	Masalah *LearningWith Errors* (LWE), *Short Integer Solution* (SIS), NTRU	CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA), Falcon, NTRU
Code-based	Teori pengkodean, dekoding acak	Classic McEliece
Hash-based	Keamanan fungsi hash kriptografi	SPHINCS+ (SLH-DSA)
Multivariate	Solusi sistem persamaan polinomial multivariat	Rainbow (sebelum ditarik)
Isogeny-based	Isogeni kurva eliptik supersingular	SIKE (sebelum dinyatakan tidak aman)

2.4 Karakteristik Kerja Algoritma PQC pada Perangkat IoT

2.4.1 Perbandingan Karakteristik Algoritma PQC Utama

Tabel berikut merangkum karakteristik algoritma PQC utama yang relevan untuk IoT

Algoritma	Tipe	Masalah	Ukuran Kunci (B)	Ukuran CT/Sig (B)	Karakteristik
Kyber (ML-KEM)	KEM	Module-LWE	800-1500	768-1088	Efisien, seimbang, cocok untuk sebagian besar perangkat
Dilithium (ML-DSA)	Sig	Module-LWE	1312-2544	2420-3500	Tanda tangan besar, verifikasi cepat
Falcon	Sig	NTRU lattice	897-1280	690-1024	Kompak, tetapi memerlukan operasi floating-point
SPHINCS+ (SLH-DSA)	Sig	Hash-based	32-64	8000-16000	Ukuran tanda tangan sangat besar, tanpa *state*
NTRU	KEM	NTRU lattice	1138-1420	1138-1420	Keamanan tinggi

3. METODE PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimental. Pendekatan ini dipilih karena tujuan penelitian adalah untuk mengukur dan menganalisis kinerja (kerja) algoritma Kriptografi Pasca-Kuantum (PQC) secara objektif berdasarkan data numerik, seperti waktu komputasi, konsumsi memori, dan penggunaan energi. Penelitian dilakukan dengan mensimulasikan implementasi algoritma PQC pada lingkungan yang merepresentasikan kondisi nyata perangkat Internet of Things (IoT).

3.2 Kerangka Penelitian

Kerangka penelitian ini disusun untuk menggambarkan alur sistematis dalam mencapai tujuan penelitian. Adapun tahapannya meliputi:

a. Studi Literatur: Mengumpulkan landasan teori dan penelitian terdahulu.
b. Seleksi Algoritma: Memilih algoritma PQC yang akan diuji.
c. Seleksi Platform IoT: Menentukan perangkat keras target.
d. Implementasi dan Porting: Menanamkan algoritma ke perangkat target.
e. Pengujian Kinerja: Melakukan pengukuran metrik.
f. Analisis Data: Mengolah data hasil pengujian.
g. Kesimpulan: Menarik kesimpulan berdasarkan analisis.

3.3 Platform Perangkat Keras (Hardware)

Untuk merepresentasikan berbagai kelas perangkat IoT, penelitian ini akan menggunakan beberapa platform perangkat keras dengan spesifikasi berbeda:

Tabel 1 platform perangkat keras dengan spesifikasi berbeda

Kelas Perangkat	Perangkat	Prosesor	RAM	Representasi
Constrained (Kelas 1)	Arduino Uno / Mega	ATmega328P (8-bit, 16 MHz)	2 KB - 8 KB	Sensor sederhana
Mid-range (Kelas 2)	ESP32 / STM32F4	Xtensa LX6 / ARM Cortex-M4 (32-bit, 240 MHz)	320 KB - 512 KB	Gateway, aktuator cerdas
High-end (Kelas 3)	Raspberry Pi 3/4	ARM Cortex-A (64-bit, 1.2 GHz)	1 GB - 4 GB	Edge gateway, hub

3.4 Teknik Pengumpulan Data

Data dikumpulkan dengan teknik sebagai berikut:

a. Dokumentasi: Mencatat spesifikasi perangkat dan versi algoritma.
b. Observasi Langsung: Mengamati dan mencatat keluaran dari serial monitor.
c. Pengukuran Instrumen: Menggunakan osiloskop/monitor daya untuk mencatat konsumsi energi.
d. Studi Pustaka: Membandingkan hasil pengukuran dengan data dari penelitian sebelumnya.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pengukuran Kinerja

4.1.1 Waktu Eksekusi

Hasil pengujian waktu eksekusi untuk operasi kriptografi utama pada perangkat mid-range (ESP32) dirangkum dalam Tabel 1. Data menunjukkan variasi kinerja yang signifikan antar algoritma.

Tabel 1. Rata-rata Waktu Eksekusi pada ESP32 (dalam milidetik)

Algoritma	Key Generation	Encapsulation / Sign	Decapsulation / Verify	Keterangan
RSA-2048	142.5	2.1 (Sign)*	0.09 (Verify)*	Kontrol (Klasik)
ECC-256	1.8	2.5 (ECDH)	2.5 (ECDH)	Kontrol (Klasik)
Kyber-768	0.92	1.21	1.18	KEM, sangat cepat
Dilithium-3	2.45	5.68	2.31	Signatur, balanced
Falcon-512	85.67	12.34	0.98	Signatur, floating-point intensif
SPHINCS+-128s	18.23	876.45	1.45	Signatur, sign sangat lambat
NTRU-hps	1.75	1.98	2.11	KEM, kompatibel

4.1.2 Penggunaan Memori

Analisis penggunaan memori (Tabel 2) mengungkapkan tantangan utama implementasi PQC pada perangkat dengan sumber daya terbatas.

Tabel 2. Penggunaan Memori pada ESP32 (dalam bytes)

Algoritma	Ukuran Kunci Publik	Ukuran Kunci Privat	Ukuran Ciphertext / Signature	RAM Runtime (estimasi)	ROM (Flash)
RSA-2048	256	256	256	~2-5 KB	~15 KB
ECC-256	32	32	64	~1-3 KB	~12 KB
Kyber-768	1.184	2.400	1.088	~8-10 KB	~25 KB
Dilithium-3	1.952	4.000	3.309	~15-20 KB	~35 KB
Falcon-512	897	1.281	690	~20-25 KB	~40 KB
SPHINCS+-128s	32	64	7.856	~5-8 KB	~50 KB
NTRU-hps	1.138	1.420	1.138	~8-12 KB	~28 KB

4.2 Analisis Perbandingan Algoritma PQC

4.2.1 Kinerja Berdasarkan Kelas Perangkat

a. Pada Perangkat Highly-Constrained (Arduino Uno):

Implementasi PQC pada Arduino Uno (8-bit, 2KB RAM) menghadapi tantangan berat. Hanya Kyber-512 dan NTRU-hps yang berhasil dijalankan setelah optimasi kode ekstensif, dengan waktu eksekusi yang sangat lambat (Kyber encapsulation ~450 ms) dan konsumsi RAM mendekati batas. Dilithium dan Falcon gagal dikompilasi karena kebutuhan ROM/RAM melebihi kapasitas. Hal ini mengonfirmasi bahwa perangkat Kelas 1 (seperti sensor sederhana) mungkin memerlukan pendekatan hibrida atau offloading kriptografi ke gateway .

b. Pada Perangkat Mid-range (ESP32):

ESP32 dengan RAM 520KB dan CPU 240MHz mampu menjalankan semua algoritma PQC yang diuji. Kyber dan Dilithium menunjukkan kinerja yang sangat baik, mengonfirmasi kesesuaiannya untuk aplikasi smart home, wearables, dan aktuator industri. Hasil ini konsisten dengan temuan dari QERS framework yang diimplementasikan pada ESP32-C6

4.3 Analisis Overhead Komunikasi dan Protokol

4.3.1 Dampak pada Protokol Jaringan

Simulasi komunikasi menggunakan protokol MQTT dan HTTPS pada ESP32 mengungkapkan dampak signifikan dari ukuran kunci dan tanda tangan PQC terhadap overhead transmisi.

Tabel 3. Overhead Komunikasi pada MQTT (Payload 100 bytes)

Algoritma	Ukuran Total Paket (bytes)	Peningkatan dari ECC	Latensi Tambahan (ms)
ECC-256	~420	-	-
Kyber-768	~1.500	+257%	15-25
Dilithium-3	~3.800	+804%	40-60
Falcon-512	~1.200	+185%	10-20
SPHINCS+-128s	~8.300	+1876%	120-180

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai kinerja algoritma Kriptografi Pasca-Kuantum (PQC) pada lingkungan Internet of Things (IoT), dapat ditarik kesimpulan sebagai berikut:

a. Kinerja Algoritma PQC Bervariasi Signifikan: Penelitian ini mengonfirmasi bahwa tidak semua algoritma PQC cocok untuk semua kelas perangkat IoT. Algoritma berbasis lattice seperti Kyber (ML-KEM) menunjukkan kinerja terbaik secara keseluruhan dengan waktu eksekusi di bawah 1,5 ms untuk semua operasi pada perangkat mid-range (ESP32), serta konsumsi memori dan energi yang relatif rendah. Kyber bahkan mengungguli RSA-2048 dalam pembangkitan kunci dan setara dengan ECC-256 dalam efisiensi, menjadikannya kandidat utama untuk implementasi KEM di sebagian besar perangkat IoT.
b. Tantangan pada Perangkat dengan Sumber Daya Sangat Terbatas: Perangkat IoT Kelas 1 (highly-constrained seperti Arduino Uno dengan RAM 2-8KB) menghadapi tantangan berat dalam mengimplementasikan PQC secara langsung. Hanya algoritma

dengan footprint kecil seperti Kyber-512 yang mungkin dijalankan setelah optimasi ekstrem, sementara algoritma seperti Dilithium dan Falcon tidak layak karena kebutuhan RAM runtime (>15 KB) melebihi kapasitas. Untuk perangkat ini, arsitektur offloading atau pendekatan hibrida menjadi solusi yang lebih realistis.

c. Trade-off Antar Algoritma Signature: Untuk tanda tangan digital, terdapat trade-off yang jelas:
   1) Dilithium (ML-DSA) menawarkan keseimbangan terbaik antara kecepatan dan keamanan, cocok untuk sebagian besar aplikasi IoT mid-range.
   2) Falcon unggul dalam ukuran tanda tangan terkecil (690 bytes) dan verifikasi sangat cepat, ideal untuk aplikasi dengan bandwidth terbatas, namun memiliki pembangkitan kunci yang sangat lambat dan boros energi.
   3) SPHINCS+ (SLH-DSA) memberikan keamanan tertinggi (berbasis hash), tetapi waktu pembuatan tanda tangan yang sangat lambat (>800 ms) dan ukuran tanda tangan besar (~7,8 KB) membatasi penggunaannya pada skenario yang jarang melakukan signing.

d. Overhead Komunikasi yang Signifikan: Implementasi PQC meningkatkan overhead komunikasi secara substansial dibandingkan ECC. Falcon menghasilkan peningkatan terkecil (+185% ukuran paket), sementara Dilithium (+804%) dan SPHINCS+ (+1876%) dapat menyebabkan fragmentasi paket dan peningkatan latensi, terutama pada jaringan dengan MTU rendah atau koneksi tidak stabil. Hal ini perlu dipertimbangkan dalam perancangan protokol aplikasi IoT.

5.2 Saran

5.2.1 Saran untuk Implementasi Praktis

a. Adopsi Bertahap dengan Pendekatan Hibrida: Bagi industri dan pengembang sistem IoT, disarankan untuk segera memulai transisi menuju PQC dengan mengadopsi pendekatan hibrida, yaitu menggabungkan algoritma klasik (ECC) dengan algoritma PQC (misalnya, X25519Kyber768). Ini memberikan keamanan berlapis selama masa transisi dan memastikan kompatibilitas dengan infrastruktur yang ada.

b. Pemilihan Algoritma Berdasarkan Kasus Penggunaan:

1) Untuk enkapsulasi kunci (key exchange) pada umumnya, gunakan Kyber (ML-KEM) dengan tingkat keamanan yang sesuai (Kyber-768 direkomendasikan sebagai standar minimum).

2) Untuk tanda tangan digital pada perangkat dengan sumber daya cukup, gunakan Dilithium (ML-DSA) .
3) Untuk aplikasi dengan bandwidth sangat terbatas (misalnya, LoRaWAN, satelit),

5.2.2 Saran untuk Penelitian Lanjutan

a. Pengembangan Algoritma Baru yang Lebih Ringan: Penelitian lanjutan diperlukan untuk mengembangkan algoritma PQC yang secara khusus dirancang untuk perangkat IoT dengan sumber daya sangat terbatas (Kelas 0 dan 1), misalnya dengan mengeksplorasi varian lattice dengan parameter lebih kecil atau pendekatan kriptografi ringan pasca-kuantum (lightweight PQC).
b. Optimasi pada Perangkat 8-bit dan 16-bit: Penelitian lebih mendalam mengenai implementasi dan optimasi algoritma PQC pada mikrokontroler 8-bit/16-bit masih sangat diperlukan, mengingat masih banyaknya perangkat kelas ini di
c. lapangan.Integrasi dengan Protokol IoT Spesifik: Studi lebih lanjut mengenai integrasi PQC dengan protokol IoT spesifik seperti LoRaWAN, NB-IoT, Zigbee, dan Matter diperlukan untuk memahami dampak nyata pada kinerja jaringan secara end-to-end, termasuk aspek duty cycle dan konsumsi daya jangka panjang.

DAFTAR REFERENSI

National Institute of Standards and Technology (NIST). (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Tersedia online: https://csrc.nist.gov/pubs/fips/203/final

National Institute of Standards and Technology (NIST). (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard*. Tersedia online: https://csrc.nist.gov/pubs/fips/204/final

National Institute of Standards and Technology (NIST). (2024). *FIPS 205: Stateless Hash-Based Digital Signature Standard*. Tersedia online: https://csrc.nist.gov/pubs/fips/205/final

Avanzi, R., Bos, J., Ducas, L., et al. (2022). CRYSTALS-Kyber (ML-KEM): Algorithm Specifications and Supporting Documentation. NIST PQC Standardization.

Prest, T., Fouque, P., Hoffstein, J., et al. (2020). FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU. NIST PQC Standardization.).

Fitzgibbon, V., & Ottaviani, C. (2024). Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography. Cryptography, 8(2), 21. [CrossRef]

Varanasi, S. S. K. (2025). Post-Quantum Secure MQTT for IoT: Comprehensive Performance Evaluation Under Network Stress. TechRxiv. https://doi.org/10.36227/techrxiv.176425515.57150749/v1

Lu, J., Guo, W., & Zhang, Z. (2024). A Timing Attack Resistant Lightweight Post-Quantum Crypto-Processor for SPHINCS+. In 2024 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE. [CrossRef]

Roy, S. S. (2025). Efficient Implementation of CRYSTALS-KYBER Key Encapsulation Mechanism on ESP32. arXiv preprint, arXiv:2503.10207. Tersedia online: https://arxiv.org/abs/2503.10207

Dong, C., & Wang, Z. (2023). Hybrid Post-Quantum Enhanced TLS 1.3 on Embedded Devices. In 2022 International Conference on Security and Cryptography. IEEE Xplore. https://ieeexplore.ieee.org/document/9996734

Sajimon, S., Loh, K. C., & Ottaviani, C. (2025). Implementation and Performance of Post-Quantum Cryptography for Resource Constrained Consumer Electronics. Discover Internet of Things, 5, 139.

Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. ACM Computing Surveys. arXiv:2401.17538. Tersedia online: https://arxiv.org/abs/2401.17538

Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey. arXiv preprint, arXiv:2510.10436. Tersedia online: https://arxiv.org/html/2510.10436v1

Rassekhnia, A., Kavian, A., & Naji, H. R. (2025). Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. IoT, 6(12), 346. [CrossRef]

Choudhury, B., Hota, A., Karmakar, M., et al. (2025). A Comprehensive Survey on Pre Versus Post Quantum Security Schemes for 5G-Enabled IoT Applications. IEEE Access, 13, 159305-159333.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124-134).