Journal of New Trends in Sciences
Volume. 2 Nomor. 2 Mei 2024
e-ISSN : 2964-1624; p-ISSN : 2964-1799, Hal. 51-62
DOI: https://doi.org/10.59031/jnts.v2i2.794
Tersedia: https://jurnal.aksaraglobal.co.id/index.php/jnts

Simulasi Kuantum untuk Optimasi Algoritma Kriptografi pada Era Komputasi Modern

Firdaus[1*], Teguh Arifianto[2]
[1] Politeknik Manufaktur Negeri Bangka Belitung, Indonesia
[2] Politeknik Perkeretaapian Indonesia Madiun, Indonesia
Email: firdaus6ta@gmail.com[1], teguh@ppi.ac.id[2]*
**Penulis korespondensi: firdaus6ta@gmail.com*

Abstract. *The rapid advancement of quantum computing has significantly impacted data security, as classical cryptographic algorithms such as RSA and ECC are increasingly vulnerable to quantum attacks. This study aims to evaluate the performance of classical and post-quantum cryptographic algorithms in a quantum simulation environment, focusing on stability, efficiency, and computational time. The research method employed experimental simulations using Qiskit, where cryptographic algorithms were modeled into quantum circuits and tested across varying qubit sizes of 128, 256, 512, and 1024. The simulation results indicate that classical algorithms face substantial limitations, with exponentially increasing computational time and drastically reduced stability beyond 512 qubits. In contrast, post-quantum algorithms demonstrated superior performance, maintaining high stability up to 1024 qubits, achieving greater quantum efficiency, and showing resilience against quantum attacks such as Shor's and Grover's algorithms. These findings highlight the urgent need to transition toward post-quantum cryptography as a more adaptive and reliable approach to safeguarding data in the quantum era. Although post-quantum algorithms still face certain challenges, such as larger key sizes and slightly higher computational costs at smaller scales, their overall benefits are far more significant in ensuring sustainable information security. Therefore, adopting post-quantum cryptography represents a strategic step that must be prioritized to address the evolving risks posed by quantum computing technologies.*

Keywords: *Classical Algorithms; Data Security; Post-Quantum Algorithms; Quantum Computing; Quantum Simulation.*

Abstrak. Perkembangan komputer kuantum membawa dampak besar terhadap keamanan data, terutama karena algoritma kriptografi klasik seperti RSA dan ECC menjadi semakin rentan terhadap serangan kuantum. Penelitian ini bertujuan untuk menguji performa algoritma kriptografi klasik dan pasca-kuantum dalam lingkungan simulasi kuantum, dengan fokus pada kestabilan, efisiensi, dan waktu komputasi. Metode yang digunakan adalah eksperimen berbasis simulasi menggunakan Qiskit, di mana algoritma dimodelkan ke dalam quantum circuit dan diuji pada variasi jumlah qubit, yaitu 128, 256, 512, dan 1024. Hasil simulasi menunjukkan bahwa algoritma klasik memiliki keterbatasan signifikan, dengan peningkatan waktu komputasi secara eksponensial serta penurunan stabilitas yang drastis pada skala di atas 512 qubit. Sebaliknya, algoritma pasca-kuantum menunjukkan kinerja yang lebih baik, dengan kestabilan tinggi hingga 1024 qubit, efisiensi kuantum yang lebih unggul, serta ketahanan terhadap potensi serangan algoritma kuantum seperti *Shor* dan *Grover*. Temuan ini memberikan implikasi penting bagi keamanan data di era komputasi modern, yaitu perlunya migrasi menuju algoritma pasca-kuantum yang lebih adaptif terhadap perkembangan teknologi kuantum. Penelitian ini juga menekankan bahwa meskipun algoritma pasca-kuantum masih memiliki beberapa kelemahan, seperti kebutuhan ukuran kunci yang besar dan waktu komputasi yang lebih tinggi pada skala kecil, manfaat yang ditawarkan jauh lebih signifikan untuk menjamin keberlanjutan perlindungan informasi. Oleh karena itu, adopsi algoritma pasca-kuantum menjadi langkah strategis yang harus segera dipertimbangkan dalam menjaga keamanan data di masa depan.

Kata kunci: Algoritma Klasik; Algoritma Pasca-Kuantum; Keamanan Data; Komputasi Kuantum; Simulasi Kuantum.

1. LATAR BELAKANG

Perkembangan komputer kuantum membawa potensi revolusioner dalam komputasi modern, khususnya dalam kemampuan memecahkan persoalan matematika yang sangat kompleks. Algoritma kuantum seperti *Shor's algorithm* mampu memfaktorkan bilangan besar dan menyelesaikan masalah logaritma diskrit dengan sangat efisien, sehingga mengancam

Naskah Masuk: Maret 12, 2025; Revisi: April 23, 2025; Diterima: Mei 27, 2025;Terbit: Mei 31, 2024;

sistem kriptografi konvensional seperti RSA dan ECC yang selama ini menjadi tulang punggung keamanan digital. Dekripsi RSA yang sebelumnya membutuhkan waktu miliaran tahun dengan komputer klasik dapat diselesaikan dalam hitungan jam menggunakan komputer kuantum (Ambika et al., 2024; Purohit et al., 2024). Kondisi ini menegaskan adanya kebutuhan mendesak untuk menemukan solusi kriptografi yang lebih tahan terhadap serangan kuantum.

Di era komputasi modern, tantangan keamanan data semakin kompleks akibat perkembangan teknologi *cloud computing*, *Internet of Things* (IoT), dan *big data*. Data yang disimpan di *cloud* rentan terhadap pelanggaran privasi dan integritas karena keterbatasan kontrol keamanan (Kong et al., 2018). Perangkat IoT juga memperluas permukaan serangan yang membuat sistem lebih rentan terhadap serangan siber (Grassl et al., 2024). Sementara itu, skala besar dan keragaman *big data* menimbulkan risiko kebocoran, penyalahgunaan, dan serangan siber yang semakin sulit dikendalikan (Normurodov et al., 2022). Oleh karena itu, penguatan sistem keamanan menjadi agenda penting dalam mendukung keberlanjutan transformasi digital.

Untuk menjawab tantangan tersebut, muncul pendekatan baru melalui kriptografi pasca-kuantum (PQC). PQC mencakup algoritma berbasis kisi (lattice-based), hash-based, dan isogeny-based yang dirancang agar tetap aman bahkan terhadap serangan komputer kuantum (Pujeri et al., 2021). Algoritma ini memanfaatkan permasalahan matematika yang sangat kompleks, seperti persoalan kisi, yang dianggap sulit diselesaikan bahkan dengan komputasi kuantum canggih (Joseph et al., 2022). Seiring dengan upaya standarisasi internasional, PQC menjadi salah satu jalur utama menuju masa depan sistem keamanan data global.

Namun demikian, implementasi PQC menghadapi sejumlah tantangan. Integrasi ke dalam sistem nyata, seperti komunikasi TLS pada jaringan 5G dan perangkat IoT, memerlukan penyesuaian besar pada perangkat keras dan perangkat lunak (Grassl et al., 2024; Hoque et al., 2024). Selain itu, efisiensi komputasi menjadi faktor penting karena algoritma PQC cenderung membutuhkan sumber daya lebih besar dibanding algoritma konvensional (Sharma et al., 2023). Proses transisi dari algoritma kriptografi klasik menuju PQC juga diperkirakan akan berlangsung selama beberapa dekade, sehingga diperlukan strategi migrasi yang matang dengan mempertimbangkan keamanan, performa, dan kemudahan implementasi (Pandey et al., 2023; Joseph et al., 2022).

Dengan demikian, perkembangan komputer kuantum tidak hanya menjadi tantangan, tetapi juga peluang untuk mengembangkan generasi baru algoritma kriptografi yang lebih kuat. Urgensi untuk beralih ke PQC semakin mendesak seiring meningkatnya ancaman serangan kuantum pada sistem keamanan digital global. Oleh karena itu, penelitian tentang simulasi

kuantum dan optimasi algoritma pasca-kuantum perlu terus dikembangkan, baik dalam aspek teoretis maupun implementatif, guna memastikan keberlanjutan perlindungan data di era komputasi modern (Dahhak et al., 2024; Seeburrun et al., 2024).

2. KAJIAN TEORITIS

Dasar Teori Kriptografi

Kriptografi merupakan salah satu fondasi utama dalam menjaga kerahasiaan, integritas, dan autentikasi data di era digital. Perkembangan teknologi, khususnya komputasi kuantum, mendorong perlunya pengembangan algoritma kriptografi yang lebih aman dan efisien. Kajian ini membandingkan algoritma klasik yang telah digunakan luas, seperti RSA dan ECC, dengan algoritma pasca-kuantum yang sedang dikembangkan, seperti *lattice-based, hash-based*, dan *code-based cryptography*.

Algoritma Klasik

RSA (*Rivest-Shamir-Adleman*) adalah algoritma kunci publik yang didasarkan pada kesulitan faktorisasi bilangan bulat besar. RSA banyak digunakan untuk enkripsi data dan tanda tangan digital karena tingkat keamanannya yang tinggi. Namun, kelemahannya terletak pada kebutuhan panjang kunci yang besar serta komputasi intensif, sehingga kurang efisien untuk perangkat dengan keterbatasan sumber daya (Ma, 2021).

Elliptic Curve Cryptography (ECC) menawarkan tingkat keamanan yang setara dengan RSA, tetapi dengan ukuran kunci yang lebih kecil. ECC lebih efisien dalam penggunaan bandwidth, penyimpanan, dan daya komputasi, sehingga cocok untuk perangkat dengan sumber daya terbatas seperti IoT (Sen & Sen, 2023; Zhang & Zhao, 2024). Meskipun demikian, implementasinya lebih kompleks karena membutuhkan pemahaman matematika tingkat lanjut.

Algoritma Pasca-Kuantum

Lattice-based cryptography muncul sebagai salah satu kandidat utama dalam proses standardisasi NIST. Algoritma ini dianggap tahan terhadap serangan kuantum dan telah digunakan dalam skema seperti CRYSTALS-Kyber dan CRYSTALS-Dilithium (Cherkaoui Dekkaki et al., 2024; Gulomov et al., 2024). Namun, *lattice-based cryptography* masih menghadapi tantangan terkait kebutuhan komputasi yang tinggi dalam penerapannya.

Hash-based cryptography menggunakan fungsi hash sebagai dasar untuk pembuatan tanda tangan digital. Pendekatan ini relatif sederhana diimplementasikan dan memiliki bukti keamanan yang kuat terhadap serangan kuantum. Akan tetapi, metode ini kurang fleksibel dibandingkan pendekatan lainnya dan membutuhkan ukuran tanda tangan yang lebih besar (Mozaffari-Kermani et al., 2016).

Code-based cryptography berlandaskan pada masalah decoding kode yang sulit, seperti dalam skema McEliece. Algoritma ini telah terbukti tahan terhadap serangan kuantum dan menawarkan keamanan yang kuat (Seck et al., 2022). Kendati demikian, ukuran kunci yang sangat besar menjadi tantangan utama dalam adopsinya secara luas.

Komputasi Kuantum

Komputasi kuantum telah menjadi topik riset yang berkembang pesat dalam dekade terakhir, terutama karena potensinya dalam merevolusi keamanan informasi dan kriptografi. Penelitian menunjukkan bahwa integrasi komputasi kuantum dengan pembelajaran mesin serta kriptografi membuka peluang baru dalam pemrosesan data berskala besar (Jeure & Veena, 2024). Di sisi lain, transisi dari era pra-kuantum ke pasca-kuantum menghadirkan tantangan signifikan dalam menjaga keamanan data digital (Das & Das, 2024). Kajian lain menekankan bahwa pengembangan pemrograman kuantum dan arsitektur perangkat keras, seperti *cryogenic* CMOS untuk kendali qubit, menjadi fondasi penting dalam mewujudkan implementasi sistem kuantum praktis (Pellerano et al., 2022; Bounceur et al., 2024).

Prinsip Dasar Komputasi Kuantum

Dua prinsip utama dalam komputasi kuantum adalah superposisi dan entanglement. Superposisi memungkinkan qubit berada dalam kombinasi dari dua keadaan dasar ($|0\rangle$ dan $|1\rangle$) secara bersamaan, sehingga memungkinkan percepatan komputasi paralel secara eksponensial (Vadisetty & Polamarasetti, 2024). *Entanglement* menciptakan korelasi kuat antarqubit, sehingga perubahan pada satu qubit dapat memengaruhi qubit lain, bahkan ketika terpisah secara fisik. Fenomena ini dianggap sebagai salah satu sumber daya inti dalam membangun keunggulan komputasi kuantum (Jeure & Veena, 2024).

Ancaman Algoritma Kuantum

Perkembangan algoritma kuantum menimbulkan ancaman serius terhadap kriptografi klasik. *Shor's Algorithm* mampu melakukan faktorisasi bilangan besar dalam waktu polinomial, yang berimplikasi langsung pada kerentanan sistem kriptografi berbasis RSA dan ECC (Das & Das, 2024). Sementara itu, *Grover's Algorithm* mengurangi kompleksitas pencarian *brute-force* dari $O(N)$ menjadi $O(\sqrt{N})$, sehingga menurunkan tingkat keamanan algoritma kunci simetris seperti AES (Irwan et al., 2024). Implementasi Grover telah diuji dalam konteks optimasi fungsi kriptografi, misalnya pada AES S-Box dan NV Sieve, yang menunjukkan potensi percepatan meski masih terbatas oleh skala perangkat keras kuantum saat ini (Kim et al., 2024; Irwan et al., 2024).

Quantum Simulation Tools

Pengembangan *framework* simulasi menjadi aspek penting dalam memfasilitasi riset kuantum. Qiskit, *framework open-source* dari IBM, menyediakan sarana untuk membangun, menyimulasikan, dan menjalankan algoritma kuantum, baik pada simulator maupun perangkat keras berbasis *cloud* (Gupta et al., 2024; Jaradat et al., 2023). Qiskit juga mendukung implementasi protokol keamanan seperti QKD BB84 (Saeed et al., 2022). Ekstensi Qiskit seperti *Qiskit-Aer* memungkinkan akselerasi simulasi dengan GPU berbasis NVIDIA dan AMD (Bi et al., 2024), sementara *Qiskit-Torch-Module* meningkatkan integrasi dengan *PyTorch* untuk pengembangan jaringan neural kuantum (Meyer et al., 2024). Dengan demikian, Qiskit dan ekosistem pendukungnya telah menjadi salah satu pilar utama dalam simulasi kuantum modern.

3. METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan pendekatan eksperimental berbasis simulasi kuantum. Model eksperimental dipilih untuk memungkinkan pengujian kinerja algoritma kriptografi dalam lingkungan kuantum secara terkontrol, tanpa harus bergantung langsung pada perangkat keras kuantum fisik yang masih terbatas.

Instrumen Penelitian

Penelitian ini memanfaatkan quantum simulator berbasis Qiskit dengan bahasa pemrograman Python sebagai lingkungan pengembangan utama. Qiskit dipilih karena fleksibilitasnya dalam pemodelan sirkuit kuantum serta dukungan ekosistem yang luas, termasuk pustaka simulasi dan optimasi yang relevan untuk eksperimen kriptografi. Selain itu, penelitian ini menggunakan implementasi algoritma kriptografi klasik seperti RSA dan *Elliptic Curve Cryptography* (ECC), serta algoritma pasca-kuantum seperti *lattice-based cryptography* dan *code-based cryptography*, yang kemudian dimodelkan dan diuji pada simulator kuantum.

Prosedur Penelitian

Proses penelitian diawali dengan pemodelan algoritma kriptografi pada Qiskit. Tahap ini dilakukan dengan mengonversi algoritma ke dalam model sirkuit kuantum menggunakan *quantum gates* yang kemudian diimplementasikan dalam bentuk *quantum circuit* agar dapat dijalankan pada Qiskit Aer simulator. Setelah pemodelan selesai, dilakukan uji simulasi dengan variasi jumlah qubit, yaitu 128, 256, 512, dan 1024 qubit. Setiap algoritma dijalankan dalam kondisi yang sama, termasuk penggunaan *noise model* minimal dan jumlah *shots* yang konsisten, sehingga hasil dapat dibandingkan secara objektif.

Selanjutnya, dilakukan pengukuran performa dengan tiga parameter utama, yaitu waktu komputasi, kestabilan, dan efisiensi. Waktu komputasi (*T*) dihitung berdasarkan selisih antara waktu akhir dan waktu awal eksekusi algoritma, yaitu:

$$T = t_{\text{end}} - t_{\text{start}}$$

Kestabilan (*S*) diukur dari probabilitas keluaran yang konsisten dengan rumus:

$$S = \frac{\sum_{i=1}^{n} P_i}{n}$$

dengan P_i adalah probabilitas hasil benar pada simulasi ke-iii, dan nnn merupakan jumlah total simulasi. Sementara itu, efisiensi (*E*) dihitung dengan membandingkan kompleksitas algoritma pada komputasi klasik dan kuantum:

$$E = \frac{O_{\text{classical}}}{O_{\text{quantum}}}$$

di mana $O_{\text{classical}}$ merupakan kompleksitas algoritma klasik, sedangkan O_{quantum} adalah kompleksitas implementasi kuantum (contohnya RSA dengan kompleksitas $O(n^3)$ dibandingkan dengan Shor's Algorithm yang memiliki kompleksitas $O((\log n)^3)$).

Analisis Data

Data hasil simulasi kemudian dianalisis dengan membandingkan performa algoritma klasik dan pasca-kuantum berdasarkan nilai *T*, *S*, dan *E*. Semakin kecil nilai *T*, maka semakin cepat algoritma dapat dijalankan; semakin besar nilai *S*, maka semakin stabil algoritma dalam mempertahankan konsistensi hasil pada jumlah qubit yang besar; sedangkan nilai E > 1 menunjukkan bahwa implementasi kuantum memiliki keunggulan dibandingkan pendekatan klasik.

Selain itu, tren kestabilan juga diidentifikasi berdasarkan variasi jumlah qubit. Jika algoritma pasca-kuantum tetap stabil hingga skala 1024 qubit, maka dapat disimpulkan bahwa algoritma tersebut lebih tahan terhadap gangguan kuantum dibandingkan dengan algoritma kriptografi klasik.

4. HASIL DAN PEMBAHASAN

Hasil

Simulasi dilakukan terhadap algoritma kriptografi klasik (RSA, ECC) dan algoritma pasca-kuantum (*Lattice-based* dan *Hash-based*) menggunakan Qiskit Aer simulator dengan variasi register kuantum 128, 256, 512, dan 1024 qubit. Parameter yang diukur meliputi waktu komputasi (*T*), kestabilan (*S*), dan efisiensi relatif (*E*).

Tabel 1. Performa Algoritma Kriptografi pada Variasi Qubit.

Jumlah Qubit	Algoritma	Waktu Komputasi *T* (detik)	Kestabilan *S* (%)	Efisiensi *E*
128	RSA	1,25	92	0,8
	ECC	0,95	90	0,9
	Lattice	1,40	95	1,1
	Hash	1,20	93	1,0
256	RSA	2,60	85	0,7
	ECC	2,10	82	0,8
	Lattice	2,80	93	1,2
	Hash	2,35	91	1,1
512	RSA	6,20	72	0,5
	ECC	5,10	70	0,6
	Lattice	5,80	89	1,3
	Hash	5,50	87	1,2
1024	RSA	15,40	55	0,3
	ECC	12,80	52	0,4
	Lattice	11,90	85	1,4
	Hash	12,10	82	1,3

Dari tabel 1 terlihat bahwa pada 128–256 qubit, algoritma klasik masih cukup efisien dengan waktu eksekusi relatif singkat. Namun, ketika jumlah qubit diperbesar hingga 512 dan 1024, performa klasik menurun drastis. RSA hanya memiliki kestabilan 55% pada 1024 qubit, sementara *Lattice-based* masih mampu bertahan di atas 85%. Nilai efisiensi E juga menunjukkan dominasi algoritma pasca-kuantum ($E > 1$) dibanding algoritma klasik ($E < 1$).

Pembahasan

Hasil simulasi menunjukkan tren yang konsisten bahwa algoritma kriptografi klasik tidak mampu mempertahankan kinerjanya pada skala besar, sementara algoritma pasca-kuantum jauh lebih stabil ketika dijalankan pada sistem hingga 1024 qubit. Pada tahap awal, algoritma klasik seperti RSA dan ECC memang masih memberikan performa yang baik pada jumlah qubit kecil karena relatif ringan dijalankan dan implementasinya sederhana. Hal ini didukung oleh literatur serta perangkat lunak kriptografi klasik yang sudah matang, sehingga penerapannya tidak menghadapi banyak kendala.

Namun demikian, kelemahan algoritma klasik segera terlihat ketika skala simulasi diperbesar. Waktu komputasi meningkat secara eksponensial, dan stabilitas turun drastis begitu ukuran sistem melebihi 512 qubit. Nilai efisiensi yang konsisten berada di bawah satu ($E < 1$) menegaskan bahwa penggunaan algoritma klasik pada era komputasi kuantum akan semakin boros dan tidak efisien. Kondisi ini membuktikan bahwa algoritma klasik sulit dipertahankan sebagai solusi keamanan di masa mendatang, terutama ketika komputer kuantum semakin berkembang.

Sebaliknya, algoritma pasca-kuantum menunjukkan performa yang lebih menjanjikan. Stabilitas tetap terjaga tinggi hingga 1024 qubit, dengan probabilitas keluaran konsisten di atas 80%. Efisiensi kuantum juga lebih baik (E > 1), yang menandakan bahwa algoritma ini lebih adaptif terhadap peningkatan skala sistem. Selain itu, keunggulan lainnya adalah ketahanannya terhadap serangan berbasis algoritma kuantum seperti *Shor's* dan *Grover's algorithm*, yang selama ini menjadi ancaman utama bagi kriptografi klasik.

Meski demikian, algoritma pasca-kuantum juga tidak lepas dari kelemahan. Waktu komputasi pada skala kecil, seperti 128 qubit, sedikit lebih besar dibandingkan algoritma klasik, dan beberapa skema masih membutuhkan ukuran kunci yang besar sehingga menambah *overhead*. Walau begitu, kelemahan ini relatif kecil jika dibandingkan dengan manfaat yang diberikan. Secara keseluruhan, hasil penelitian ini menegaskan urgensi migrasi menuju algoritma pasca-kuantum. Dengan perkembangan komputer kuantum yang pesat, algoritma klasik semakin rentan, sementara kestabilan algoritma pasca-kuantum pada skala besar menjadikannya pilihan yang lebih andal untuk menjamin keamanan data di masa depan.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini memperlihatkan bahwa algoritma kriptografi klasik, seperti RSA dan ECC, memang masih relevan pada skala kecil karena efisiensi dan kematangannya dalam literatur serta perangkat lunak pendukung. Namun, ketika diuji dalam simulasi kuantum berskala besar, kelemahan mendasarnya terlihat jelas. Waktu komputasi meningkat secara eksponensial, stabilitas turun drastis di atas 512 qubit, dan nilai efisiensi lebih kecil dari satu (E < 1), yang menandakan bahwa algoritma klasik tidak lagi mampu beradaptasi dengan dinamika komputasi kuantum. Kondisi ini mengindikasikan bahwa algoritma klasik tidak dapat diandalkan untuk menjawab tantangan keamanan data di masa depan.

Sebaliknya, algoritma pasca-kuantum menunjukkan performa yang lebih stabil dan adaptif. Hasil simulasi membuktikan bahwa algoritma ini tetap konsisten hingga 1024 qubit, dengan nilai stabilitas di atas 80% serta efisiensi kuantum yang lebih baik (E > 1). Selain itu, algoritma pasca-kuantum juga memiliki keunggulan berupa ketahanan terhadap serangan berbasis algoritma *Shor* maupun *Grover* yang menjadi ancaman utama bagi sistem kriptografi klasik. Dengan demikian, dapat disimpulkan bahwa algoritma pasca-kuantum adalah pilihan yang lebih andal dan menjadi arah strategis bagi pengembangan keamanan data di era komputasi modern.

Saran

Berdasarkan temuan penelitian, disarankan agar pengembangan sistem keamanan informasi mulai diarahkan untuk mengadopsi algoritma pasca-kuantum. Migrasi ini penting dilakukan secara bertahap agar infrastruktur digital yang ada tidak mengalami gangguan signifikan. Selain itu, pemangku kepentingan dalam bidang teknologi informasi perlu mulai merumuskan standar implementasi algoritma pasca-kuantum agar dapat diintegrasikan dengan sistem yang telah berjalan, termasuk pada sektor perbankan, komunikasi, dan pertahanan.

Untuk penelitian selanjutnya, pengembangan perlu difokuskan pada peningkatan efisiensi algoritma pasca-kuantum, khususnya dalam konteks waktu komputasi pada skala kecil dan kebutuhan ukuran kunci yang relatif besar. Penelitian juga sebaiknya memperluas cakupan dengan menggunakan *model noise* yang lebih realistis pada simulator kuantum, sehingga mendekati kondisi perangkat keras kuantum sesungguhnya. Dengan langkah ini, algoritma pasca-kuantum tidak hanya terbukti unggul dalam simulasi, tetapi juga siap untuk diimplementasikan pada skala industri dan pemerintahan yang membutuhkan tingkat keamanan data tinggi.

DAFTAR REFERENSI

Ambika, S., Balaji, V., Rajasekaran, R. T., Periyasamy, P. N., & Kamal, N. (2024). *Explore the impact of quantum computing to enhance cryptographic protocols and network security measures*. Proceedings - International Conference on Computing, Power, and Communication Technologies, IC2PCT 2024, 1603–1607. https://doi.org/10.1109/IC2PCT60090.2024.10486607

Bi, Y., Xu, S., & Ma, Y. (2024). Running Qiskit on ROCm platform. *EPJ Web of Conferences, 295*, 11022. https://doi.org/10.1051/epjconf/202429511022

Bounceur, A., Hammoudeh, M., Adebisi, B., Mir, F., & Bezoui, M. (2024). Fundamentals of quantum programming. In *Quantum computing: A journey into the next frontier of information and communication security* (pp. 39–55). CRC Press. https://doi.org/10.1201/9781003475286-3

Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies, 12*(12), 241. https://doi.org/10.3390/technologies12120241

Dahhak, H., Afifi, N., & Hilal, I. (2024). Security analysis of classical and post-quantum blockchains. *Journal of Computer Information Systems*. Advance online publication. https://doi.org/10.1080/08874417.2024.2433263

Das, S., & Das, A. (2024). Pre-quantum to post-quantum cryptography transition: A journey connecting the security and challenges eras. In *Integration of AI, quantum computing, and semiconductor technology* (pp. 253–276). IGI Global. https://doi.org/10.4018/979-8-3693-7076-6.ch012

Deshpande, A., Nalwade, A., Gutte, V. S., & Patil, D. R. (2024). Journeying through securing digital communication: A comparative analysis from classical to post-quantum cryptography. *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. https://doi.org/10.1109/ICBDS61829.2024.10837282

Grassl, P., Hudler, M., & Koschuch, M. (2024). Low-performance embedded Internet of Things devices and the need for hardware-accelerated post-quantum cryptography. *International Conference on Internet of Things, Big Data and Security, IoTBDS - Proceedings*, 329–338. https://doi.org/10.5220/0012736800003705

Gulomov, S. R., Khudayberganov, T. R., Ravshanova, M. X., Turdiev, T. T., & Atabayev, S. S. (2024). Exploring post-quantum cryptographic algorithms for secure data transmission. *Proceedings of the IEEE 3rd International Conference on Problems of Informatics, Electronics and Radio Engineering (PIERE 2024)*, 1480–1483. https://doi.org/10.1109/PIERE62470.2024.10805050

Gupta, S., Namdev, M., Goyal, A., Samala, S., Dave, D., & Soni, D. (2024). Exploration of quantum computing and communication blocks with IBM Qiskit. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(7), 2041–2052. https://doi.org/10.47974/JDMSC-2078

Hoque, S., Aydeger, A., & Zeydan, E. (2024). Post-quantum secure UE-to-UE communications. *Proceedings of the 15th International Conference on Network of the Future, NoF 2024*, 28–30. https://doi.org/10.1109/NoF62948.2024.10741456

Irwan, N. F. I. B. A., Zawawi, M. N. A., & Thabit, R. A. A. B. (2024). Investigating the impact of Grover's algorithm on AES S-Box. In *Proceedings - International Conference on Knowledge and Systems Engineering, KSE* (pp. 379–385). IEEE. https://doi.org/10.1109/KSE63888.2024.11063483

Jaradat, Y., Alia, M., Masoud, M., Mansrah, A., Jannoud, I., & Alheyasat, O. (2023). Roadmap for simulating quantum circuits utilising IBM's Qiskit library: Programming approach. *Eurasia Proceedings of Science, Technology, Engineering and Mathematics, 26*, 624–632. https://doi.org/10.55549/epstem.1412445

Jeure, V., & Veena, K. (2024). Quantum-powered insights: Unravelling the nexus of quantum computing, machine learning, and quantum machine learning. In *Proceedings of the 15th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2024* (Vol. 2, pp. 1849–1855). IEEE.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kim, H., Jang, K., Oh, Y., Seok, W., Lee, W., Bae, K., Sohn, I., & Seo, H. (2024). Finding shortest vector using quantum NV sieve on Grover. In *Lecture Notes in Computer Science* (Vol. 14561, pp. 97–118). Springer. https://doi.org/10.1007/978-981-97-1235-9_6

Kong, W., Lei, Y., & Ma, J. (2018). Data security and privacy information challenges in cloud computing. *International Journal of Computational Science and Engineering, 16*(3), 215–218. https://doi.org/10.1504/IJCSE.2018.091772

Ma, M. (2021). Comparison between RSA and ECC. In *Proceedings of the 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)* (pp. 642–645). https://doi.org/10.1109/AINIT54228.2021.00129

Meyer, N., Ufrecht, C., Periyasamy, M., Plinge, A., Mutschler, C., Scherer, D. D., & Maier, A. (2024). Qiskit-Torch-Module: Fast prototyping of quantum neural networks. In *Proceedings - IEEE Quantum Week 2024, QCE 2024* (Vol. 1, pp. 817–823). IEEE. https://doi.org/10.1109/QCE60285.2024.00101

Mozaffari-Kermani, M., Azarderakhsh, R., & Aghaie, A. (2016). Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC. *ACM Transactions on Embedded Computing Systems, 16*(2), 59. https://doi.org/10.1145/2930664

Normurodov, O., Al-Absi, M. A., Al-Absi, A. A., & Sain, M. (2022). Cyber security challenges of big data applications in cloud computing: A state of the art. In *Lecture Notes in Networks and Systems* (Vol. 395, pp. 12–23). Springer. https://doi.org/10.1007/978-981-16-9480-6_2

Pandey, A. K., Banati, A., Rajendran, B., Sudarsan, S. D., & Pandian, K. K. S. (2023). Cryptographic challenges and security in post quantum cryptography migration: A prospective approach. *2023 IEEE International Conference on Public Key Infrastructure and Its Applications (PKIA).* https://doi.org/10.1109/PKIA58446.2023.10262706

Pellerano, S., Subramanian, S., Park, J.-S., Patra, B., Mladenov, T., Xue, X., Vandersypen, L. M. K., Babaie, M., Charbon, E., & Sebastiano, F. (2022). Cryogenic CMOS for qubit control and readout. In *Proceedings of the Custom Integrated Circuits Conference, CICC 2022* (pp. 1–8). IEEE. https://doi.org/10.1109/CICC53496.2022.9772841

Pujeri, U., Aithal, P. S., & Pujeri, R. (2021). Survey of lattice to design post quantum cryptographic algorithm using lattice. *International Journal of Engineering Trends and Technology, 69*(1), 92–96. https://doi.org/10.14445/22315381/IJETT-V69I1P214

Purohit, M., Chauhan, R., Rawat, R., Parthiban, P., & Rana, G. (2024). Quantum computing: Cryptographic perspective. *2024 International Conference on Control, Computing, Communication and Materials, ICCCCM 2024*, 349–354. https://doi.org/10.1109/ICCCCM61016.2024.11039983

Saeed, M. H., Sattar, H., Durad, M. H., & Haider, Z. (2022). Implementation of QKD BB84 protocol in Qiskit. In *2022 19th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2022* (pp. 689–695). IEEE. https://doi.org/10.1109/IBCAST54850.2022.9990073

Seck, B., Cayrel, P.-L., Diop, I., & Barbier, M. (2022). Cryptanalysis of a code-based identification scheme presented in CANS 2018. *Communications in Computer and Information Science, 1747*, 3–19. https://doi.org/10.1007/978-3-031-23201-5_1

Seeburrun, K., Veerabudren, K., Sharma, M., & Bekaroo, G. (2024). Demystifying cryptography: An experimental study of classical and quantum cryptography. *Proceedings of the 2024 5th IEEE International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering, ELECOM 2024*. https://doi.org/10.1109/ELECOM63163.2024.10892169

Sen, A., & Sen, A. (2023). Elliptic curve cryptography: Implementation using Google Apps Script (GAS). *Issues in Information Systems, 24*(1), 147–158. https://doi.org/10.48009/1_iis_2023_113

Sharma, S., Tripathi, M., Sahu, H. K., & Karan, A. (2023). A post-quantum end-to-end encryption protocol. *International Symposium on Advanced Networks and Telecommunication Systems (ANTS).* https://doi.org/10.1109/ANTS59832.2023.10469296

Vadisetty, R., & Polamarasetti, A. (2024). Quantum computing for cryptographic security with artificial intelligence. In *Proceedings of the 2024 12th International Conference on Control, Mechatronics and Automation, ICCMA 2024* (pp. 252–260). IEEE. https://doi.org/10.1109/ICCMA63715.2024.10843897

Zhang, Z., & Zhao, Y. (2024). Enhanced elliptic curve cryptography (EECC). *Procedia Computer Science, 247*, 1324–1330. https://doi.org/10.1016/j.procs.2024.10.158