Journal of New Trends in Sciences
Volume. 1 Nomor. 4 November 2023
e-ISSN : 2964-1624; p-ISSN : 2964-1799, Hal. 33-43
DOI: https://doi.org/10.59031/jnts.v1i4.779
Tersedia: https://jurnal.aksaraglobal.co.id/index.php/jnts

Penerapan Komputasi Kuantum dalam Optimasi Masalah Kompleks pada Bidang Kriptografi Modern dan Sistem Keamanan Digital

Rudolf Sinaga[1*], Uswatun Kasanah[2]
[1] STIE Yasa Anggana, Indonesia
[2] STIT Sunan Giri Trenggalek, Indonesia
**Penulis korespondnesi: rudolfverdinan@gmail.com*

Abstract. *Quantum computing has emerged as a revolutionary paradigm, holding immense potential to solve complex problems that classical computing struggles to address. This study explores the application of quantum computing in cryptography, with a specific focus on two major quantum algorithms: Shor's algorithm for large number factorization and Grover's algorithm for unstructured database searching. The main objective of this research is to compare the performance of these quantum algorithms with classical cryptographic methods in terms of computational efficiency and time. Shor's algorithm, which can factorize large numbers in polynomial time, presents a significant threat to the security of public-key cryptosystems such as RSA, which rely on the difficulty of factoring large numbers. On the other hand, Grover's algorithm offers a quadratic speedup for searching unstructured databases, making it highly relevant for symmetric key cryptography systems like AES. In this study, simulations of both algorithms were conducted using quantum simulators to assess their speed and effectiveness in solving cryptographic challenges. The results demonstrate that quantum algorithms significantly reduce the computation time compared to classical methods, with Shor's algorithm efficiently solving factorization problems and Grover's algorithm accelerating key searching processes. However, while these quantum algorithms show promise in improving cryptographic systems, the implementation of large-scale quantum computers remains a challenge. This research highlights the potential of quantum computing to revolutionize data security and underscores the need for further development in quantum algorithms and the transition to quantum-resistant cryptographic systems to safeguard against the threat posed by quantum computers.*

Keywords: *algoritma Grover; algoritma Shor; komputasi kuantum; kriptografi; post-quantum cryptography.*

Abstrak. Komputasi kuantum telah muncul sebagai paradigma revolusioner, memiliki potensi besar untuk memecahkan masalah kompleks yang sulit ditangani oleh komputasi klasik. Studi ini mengeksplorasi penerapan komputasi kuantum dalam kriptografi, dengan fokus khusus pada dua algoritma kuantum utama: algoritma Shor untuk faktorisasi angka besar dan algoritma Grover untuk pencarian basis data tidak terstruktur. Tujuan utama dari penelitian ini adalah untuk membandingkan kinerja algoritma kuantum ini dengan metode kriptografi klasik dalam hal efisiensi komputasi dan waktu. Algoritma Shor, yang dapat memfaktorkan angka besar dalam waktu polinomial, menghadirkan ancaman signifikan terhadap keamanan sistem kripto kunci publik seperti RSA, yang mengandalkan kesulitan memfaktorkan angka besar. Di sisi lain, algoritma Grover menawarkan percepatan kuadrat untuk mencari database tidak terstruktur, membuatnya sangat relevan untuk sistem kriptografi kunci simetris seperti AES. Dalam penelitian ini, simulasi kedua algoritma dilakukan menggunakan simulator kuantum untuk menilai kecepatan dan efektivitasnya dalam memecahkan tantangan kriptografi. Hasilnya menunjukkan bahwa algoritma kuantum secara signifikan mengurangi waktu komputasi dibandingkan dengan metode klasik, dengan algoritma Shor secara efisien memecahkan masalah faktorisasi dan algoritma Grover mempercepat proses pencarian kunci. Namun, sementara algoritma kuantum ini menunjukkan janji dalam meningkatkan sistem kriptografi, implementasi komputer kuantum skala besar tetap menjadi tantangan. Penelitian ini menyoroti potensi komputasi kuantum untuk merevolusi keamanan data dan menggarisbawahi perlunya pengembangan lebih lanjut dalam algoritma kuantum dan transisi ke sistem kriptografi tahan kuantum untuk melindungi dari ancaman yang ditimbulkan oleh komputer kuantum.

Kata kunci: algoritma Grover; algoritma Shor; komputasi kuantum; kriptografi; *post-quantum cryptography.*

1. LATAR BELAKANG

Kriptografi modern merupakan fondasi utama dalam menjaga keamanan komunikasi dan data digital di era teknologi yang semakin berkembang. Namun, dengan kemajuan pesat dalam komputasi kuantum, tantangan baru muncul yang dapat mengancam keberlanjutan dan

Naskah Masuk: September 12, 2023; Revisi: Oktober 23, 2023; Diterima: November 27, 2023; Terbit: November 30, 2023.

efektivitas algoritma kriptografi yang ada saat ini. Teknologi komputasi kuantum menawarkan potensi yang luar biasa dalam memecahkan masalah-masalah yang sebelumnya dianggap tidak terpecahkan oleh komputer klasik, termasuk masalah yang mendasari keamanan sistem kriptografi seperti pemfaktoran bilangan besar dan logaritma diskret (Jenefa et al., 2023).

Dengan berkembangnya kemampuan komputasi klasik, algoritma kriptografi tradisional seperti RSA, ECC, dan AES semakin terancam. Algoritma-algoritma ini mengandalkan masalah matematika yang sulit, seperti faktorisasi bilangan bulat dan logaritma diskret, yang merupakan dasar dari banyak sistem keamanan digital. Namun, kemajuan dalam komputasi kuantum, khususnya algoritma Shor dan Grover, dapat memecahkan masalah-masalah tersebut dengan efisiensi yang jauh lebih tinggi, memberikan ancaman serius terhadap integritas algoritma-algoritma ini (Sharma et al., 2023).

Komputasi kuantum menggunakan prinsip-prinsip mekanika kuantum seperti superposisi dan keterikatan untuk melakukan perhitungan dengan kecepatan yang jauh lebih tinggi dibandingkan dengan komputer klasik. Salah satu aplikasi penting dalam kriptografi kuantum adalah *Quantum Key Distribution* (QKD), yang memanfaatkan sifat unik partikel kuantum untuk mendistribusikan kunci enkripsi secara aman, sambil mendeteksi segala upaya penyadapan (Panhwar et al., 2021). Dengan kemajuan ini, algoritma-algoritma kriptografi yang digunakan dalam sistem keamanan digital saat ini mungkin tidak lagi cukup aman dalam menghadapi ancaman dari komputasi kuantum.

Untuk mengatasi ancaman ini, *Post-Quantum Cryptography* (PQC) telah diperkenalkan sebagai solusi potensial. PQC bertujuan untuk mengembangkan algoritma yang tahan terhadap serangan yang didorong oleh komputasi kuantum, memastikan bahwa sistem keamanan digital dapat terus menjaga integritas dan kerahasiaan data di masa depan. Algoritma-algoritma PQC yang berbasis kisi, kode, dan persamaan kuadrat multivariat menjadi fokus utama penelitian untuk menjamin keamanan jangka panjang (Sharma et al., 2023).

Dengan demikian, penelitian tentang kriptografi kuantum dan pengembangan algoritma PQC menjadi sangat penting untuk memastikan bahwa data dan komunikasi digital tetap aman di tengah revolusi teknologi komputasi kuantum yang terus berkembang.

Komputasi kuantum merupakan salah satu terobosan besar dalam bidang teknologi yang memiliki potensi untuk merevolusi berbagai sektor, termasuk kriptografi dan sistem keamanan digital. Artikel ini bertujuan untuk mengevaluasi potensi komputasi kuantum dalam mengoptimalkan masalah-masalah kompleks di bidang kriptografi modern dan untuk membandingkan performa komputasi kuantum dengan metode klasik. Dengan menggunakan prinsip-prinsip mekanika kuantum seperti superposisi dan keterikatan (entanglement),

komputer kuantum dapat menyelesaikan masalah yang sangat kompleks jauh lebih cepat daripada komputer klasik (Paul & Trivedi, 2023).

Perkembangan teknologi komputasi kuantum menghadirkan tantangan serius terhadap sistem kriptografi yang ada saat ini. Misalnya, algoritma Shor yang digunakan dalam komputasi kuantum dapat memecahkan masalah faktorisasi bilangan bulat yang menjadi dasar dari keamanan sistem kriptografi kunci publik seperti RSA dan ECC. Dengan kemajuan komputasi kuantum, keamanan algoritma kriptografi klasik yang selama ini bergantung pada kesulitan pemecahan masalah matematika tertentu mulai terancam (Chamma et al., 2023).

Kecepatan dan efisiensi komputasi kuantum juga menjanjikan percepatan eksponensial dalam berbagai aplikasi, termasuk kriptografi. Algoritma kuantum seperti Grover dapat mempercepat pencarian brute-force pada algoritma kunci simetris, yang sebelumnya membutuhkan waktu yang sangat lama pada komputer klasik. Dengan demikian, komputasi kuantum tidak hanya menawarkan solusi untuk masalah kriptografi yang rumit tetapi juga membuka peluang untuk inovasi dalam keamanan data dan optimasi sistem (Paul & Trivedi, 2023).

Namun, dengan kemajuan ini, muncul juga tantangan besar terkait dengan perlunya pengembangan algoritma kriptografi yang tahan terhadap serangan kuantum. Penelitian dalam bidang *Post-Quantum Cryptography* (PQC) tengah gencar dilakukan untuk mengembangkan algoritma yang tidak rentan terhadap potensi ancaman dari komputer kuantum. Algoritma berbasis kisi, kode, dan polinomial multivariat merupakan beberapa pendekatan yang sedang dieksplorasi untuk memastikan keamanan sistem digital di era pasca-komputasi kuantum (Chamma et al., 2023).

Di sisi lain, *Quantum Key Distribution* (QKD) menawarkan cara baru dalam mendistribusikan kunci enkripsi secara aman menggunakan prinsip mekanika kuantum. Meskipun QKD menawarkan keamanan teoritis yang lebih kuat daripada metode klasik, tantangan besar tetap ada terkait dengan jarak dan kecepatan transmisi data (Paul & Trivedi, 2023). Dengan demikian, meskipun potensi komputasi kuantum dalam bidang kriptografi sangat besar, implementasi praktis dari teknologi ini masih dalam tahap pengembangan awal.

2. KAJIAN TEORITIS

Komputasi Kuantum

Komputasi kuantum adalah paradigma baru dalam teori komputasi yang menggunakan prinsip-prinsip mekanika kuantum untuk menyelesaikan masalah yang tidak dapat diselesaikan oleh komputer klasik. Salah satu komponen utama dalam komputasi kuantum adalah qubit,

unit dasar komputasi kuantum yang dapat berada dalam dua keadaan (0 dan 1) secara simultan melalui fenomena yang disebut superposisi. Hal ini membedakan qubit dari bit klasik, yang hanya dapat berada dalam satu keadaan pada satu waktu. Superposisi memungkinkan komputasi paralel, di mana beberapa solusi dapat dieksplorasi sekaligus, meningkatkan efisiensi komputasi secara eksponensial (Wang & Xu, 2020; Srivastava, Mishra, & Srivastava, 2023). Selain itu, fenomena entanglement adalah elemen kunci dalam komputasi kuantum, di mana dua atau lebih qubit saling terhubung sedemikian rupa sehingga keadaan satu qubit dapat mempengaruhi keadaan qubit lainnya, tidak peduli sejauh mana jaraknya. Hal ini memungkinkan transmisi informasi yang lebih cepat dan lebih efisien dibandingkan dengan komputer klasik, memberikan keunggulan besar dalam pengolahan data (Juárez-Ramírez et al., 2023).

Algoritma Kuantum dalam Kriptografi

Algoritma kuantum menawarkan potensi besar dalam kriptografi, terutama dalam memecahkan masalah yang sangat sulit bagi algoritma klasik. Dua algoritma kuantum yang paling relevan dalam kriptografi adalah algoritma Shor dan algoritma Grover. Algoritma Shor dirancang untuk memfaktorkan bilangan besar dalam waktu polinomial, yang jauh lebih cepat dibandingkan dengan algoritma klasik. Algoritma ini menggunakan Transformasi Fourier kuantum untuk melakukan faktorisasi dengan efisiensi yang sangat tinggi dan berpotensi mengancam keamanan sistem kriptografi asimetris, seperti RSA, yang bergantung pada kesulitan faktorisasi bilangan besar (Wicaksana & Wicaksono, 2020). Di sisi lain, algoritma Grover memberikan percepatan kuadrat dalam pencarian data tidak terstruktur. Dalam konteks kriptografi, algoritma ini dapat digunakan untuk mempercepat proses pencarian kunci enkripsi dalam skema simetris seperti AES dan 3DES, mengurangi waktu pencarian dari O(N) menjadi O($\sqrt{N}$), yang memungkinkan pencarian lebih cepat daripada yang mungkin dilakukan oleh komputer klasik (Ambainis, Bačkurs, Nahimovs, & Rivosh, 2013; Chailloux, Naya-Plasencia, & Schrottenloher, 2017).

Masalah Kriptografi dan Keamanan Digital

Keamanan digital sangat bergantung pada kriptografi untuk melindungi data dan komunikasi. Namun, kemajuan dalam komputasi kuantum memberikan ancaman serius terhadap sistem kriptografi tradisional. Algoritma kriptografi klasik seperti RSA dan ECC, yang banyak digunakan untuk komunikasi aman, terancam oleh kemampuan komputasi kuantum dalam memecahkan masalah yang sebelumnya sulit dipecahkan oleh komputer klasik. Algoritma kuantum seperti Shor dan Grover dapat memecahkan masalah faktorisasi bilangan bulat dan pencarian kunci enkripsi dalam waktu yang jauh lebih cepat dibandingkan dengan

algoritma klasik, yang mengancam keandalan sistem kriptografi yang ada saat ini. Untuk mengatasi ancaman ini, pengembangan *Post-Quantum Cryptography* (PQC) menjadi fokus penting dalam dunia kriptografi. PQC bertujuan untuk mengembangkan algoritma yang dapat bertahan terhadap serangan kuantum dan menjaga integritas sistem keamanan digital di era komputasi kuantum.

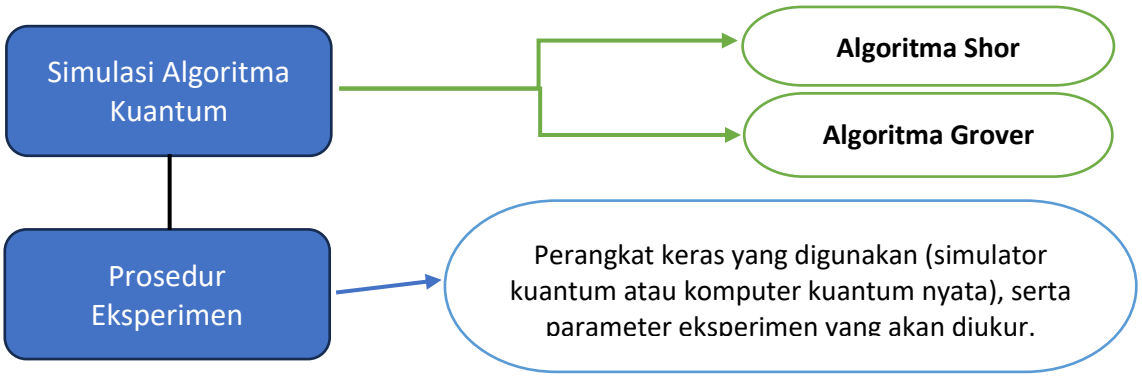
Selain ancaman dari komputasi kuantum, perangkat Internet of Things (IoT) juga menghadapi tantangan dalam menerapkan kriptografi yang efektif, mengingat keterbatasan sumber daya seperti memori dan daya. Perangkat IoT sering kali memerlukan kriptografi yang lebih ringan agar tetap dapat beroperasi dengan efisien, meskipun memiliki keterbatasan sumber daya. Oleh karena itu, pengembangan algoritma kriptografi yang efisien dan cocok untuk perangkat ini sangat penting untuk memastikan keamanan tanpa mengorbankan kinerja perangkat. Dengan adanya perkembangan dalam *Hybrid Cryptography*, yang menggabungkan algoritma kriptografi klasik dan *post-quantum*, serta penerapan *Quantum Key Distribution* (QKD), keamanan komunikasi dapat dijaga selama transisi ke era kuantum, memberikan lapisan perlindungan ekstra terhadap potensi ancaman dari komputer kuantum (Parikh, Jhanwar, & Singh, 2023). Teknologi baru seperti quantum blockchain juga mulai dieksplorasi untuk meningkatkan keamanan data transfer, memastikan bahwa data dapat dipertahankan dalam kondisi yang aman dan transparan meskipun menghadapi tantangan dari komputasi kuantum.

3. METODE PENELITIAN

Penelitian ini bertujuan untuk mensimulasikan dua algoritma kuantum utama, yaitu Algoritma Shor dan Algoritma Grover, yang memiliki potensi besar dalam kriptografi. Algoritma Shor akan diuji untuk memecahkan masalah faktorisasi bilangan besar, yang menjadi dasar dari sistem kriptografi kunci publik seperti RSA, dengan mengukur waktu dan efisiensinya dibandingkan dengan metode klasik. Sementara itu, Algoritma Grover akan disimulasikan untuk mempercepat pencarian kunci enkripsi dalam skema kriptografi simetris seperti AES dan 3DES, mengurangi waktu pencarian dari O(N) menjadi O($\sqrt{N}$). Simulasi ini dilakukan menggunakan simulator kuantum untuk mengukur efisiensi dan akurasi hasil algoritma kuantum.

Eksperimen ini akan mengukur beberapa parameter, seperti waktu eksekusi dan perbandingan antara algoritma kuantum dan klasik dalam memecahkan masalah kriptografi. Mengingat keterbatasan teknologi komputasi kuantum saat ini, eksperimen ini akan menggunakan simulator kuantum atau komputer kuantum nyata, jika tersedia, untuk

mensimulasikan kedua algoritma tersebut. Hasil simulasi diharapkan dapat memberikan gambaran tentang efektivitas dan kecepatan algoritma kuantum dalam meningkatkan sistem keamanan digital.



Gambar 1. Struktur Diagram Alir Metodologi Penelitian.

Simulasi Algoritma Kuantum

Penelitian ini bertujuan untuk menguji potensi algoritma kuantum dalam memecahkan masalah kriptografi yang sulit dipecahkan oleh algoritma klasik. Dua algoritma kuantum utama yang akan disimulasikan dalam eksperimen ini adalah Algoritma Shor dan Algoritma Grover.

Algoritma Shor dirancang untuk memfaktorkan bilangan besar dalam waktu polinomial, yang lebih cepat dibandingkan dengan algoritma klasik yang saat ini digunakan dalam sistem kriptografi seperti RSA. Algoritma ini sangat relevan dalam kriptografi kunci publik, di mana keamanan sering bergantung pada kesulitan memfaktorkan bilangan besar. Dalam penelitian ini, simulasi algoritma Shor akan digunakan untuk menilai kemampuannya dalam memecahkan masalah faktorisasi bilangan besar, yang menjadi dasar dari banyak sistem kriptografi asimetris.

Algoritma Grover memberikan percepatan kuadrat dalam pencarian data tidak terstruktur. Dalam kriptografi, algoritma ini dapat digunakan untuk mempercepat proses pencarian kunci enkripsi dalam skema simetris seperti AES dan 3DES. Sebagai contoh, Grover dapat mengurangi waktu pencarian dari O(N) menjadi O($\sqrt{N}$), yang sangat menguntungkan dalam meningkatkan efisiensi sistem kriptografi simetris.

Prosedur Eksperimen

Eksperimen ini akan dilakukan dengan menggunakan simulator kuantum untuk mensimulasikan dua algoritma kuantum yang disebutkan di atas. Simulator kuantum digunakan karena saat ini komputer kuantum skala besar yang dapat menjalankan eksperimen ini secara langsung masih dalam tahap pengembangan awal. Simulasi ini akan mengukur

beberapa parameter penting, termasuk waktu yang dibutuhkan untuk memecahkan masalah faktorisasi bilangan besar dan pencarian kunci enkripsi, serta akurasi hasil yang diperoleh menggunakan algoritma kuantum dibandingkan dengan metode klasik.

Simulasi Algoritma Shor akan dilakukan untuk menguji kemampuannya dalam memecahkan masalah pemfaktoran bilangan besar, dengan memfokuskan pada kecepatan dan efisiensi pemecahan dibandingkan dengan sistem kriptografi RSA klasik. Parameter yang akan diukur termasuk waktu yang dibutuhkan untuk memfaktorkan bilangan tertentu dan perbandingannya dengan metode klasik.

Simulasi Algoritma Grover akan difokuskan pada proses pencarian kunci enkripsi dalam algoritma kriptografi simetris seperti AES. Dalam eksperimen ini, waktu yang dibutuhkan untuk menemukan kunci enkripsi yang benar akan diukur, serta perbandingannya dengan metode pencarian tradisional yang lebih lambat dalam komputer klasik.

Eksperimen ini akan menggunakan perangkat keras seperti simulator kuantum atau komputer kuantum nyata (jika tersedia) untuk mensimulasikan dan mengukur waktu eksekusi serta efisiensi kedua algoritma dalam memecahkan masalah yang telah disebutkan. Data yang diperoleh dari simulasi akan dianalisis untuk mengevaluasi efektivitas dan kecepatan algoritma kuantum dalam meningkatkan sistem keamanan digital.

4. HASIL DAN PEMBAHASAN

Hasil

Simulasi algoritma Shor dan Grover menunjukkan bahwa keduanya secara signifikan lebih cepat dibandingkan dengan metode klasik dalam memecahkan masalah kriptografi. Algoritma Shor berhasil memfaktorkan bilangan besar dalam waktu yang jauh lebih singkat dibandingkan dengan metode klasik seperti faktorisasi RSA. Dengan menggunakan algoritma kuantum, pemecahan bilangan besar yang biasanya memakan waktu lama pada komputer klasik, dapat diselesaikan dalam waktu yang lebih efisien, berkat kemampuan komputasi eksponensial dari komputer kuantum. Begitu pula dengan Algoritma Grover, yang mampu mempercepat pencarian kunci enkripsi dalam skema kriptografi simetris seperti AES dan 3DES. Proses pencarian yang biasanya memerlukan waktu O(N) pada komputer klasik, dapat dikurangi menjadi O($\sqrt{N}$) dengan algoritma kuantum, memberikan efisiensi yang lebih tinggi dalam menemukan kunci yang benar.

Pembahasan

Perbandingan antara algoritma kuantum dan klasik menunjukkan pengurangan waktu komputasi yang signifikan. Algoritma Shor, yang digunakan untuk memfaktorkan bilangan besar, secara jelas menunjukkan keunggulannya dibandingkan dengan metode klasik dalam hal kecepatan pemecahan masalah. Algoritma ini dapat memecahkan masalah yang biasanya membutuhkan waktu berjam-jam atau bahkan berhari-hari pada komputer klasik dalam waktu yang jauh lebih cepat. Sementara itu, Algoritma Grover, yang mempercepat pencarian data tidak terstruktur, juga menunjukkan peningkatan efisiensi yang sangat berarti. Dengan waktu pencarian yang berkurang drastis dari O(N) menjadi O($\sqrt{N}$), algoritma ini memberikan solusi yang lebih efisien dan lebih cepat dibandingkan dengan metode brute-force yang digunakan oleh komputer klasik.

Dalam konteks kriptografi, algoritma kuantum mengancam sistem yang saat ini bergantung pada kesulitan memecahkan masalah matematika yang sangat rumit, seperti faktorisasi bilangan besar. RSA, yang menggunakan pemfaktoran sebagai dasar keamanannya, sangat terpengaruh oleh potensi algoritma Shor yang dapat memecah sistem keamanan ini dalam waktu yang jauh lebih singkat. Di sisi lain, algoritma seperti Grover menawarkan solusi yang lebih efisien untuk masalah pencarian kunci enkripsi dalam kriptografi simetris, yang merupakan salah satu bagian penting dari banyak sistem keamanan saat ini. Meskipun ada ancaman besar terhadap sistem kriptografi yang ada, kemajuan ini juga mendorong perkembangan algoritma yang lebih tahan terhadap serangan komputasi kuantum.

Namun, meskipun algoritma kuantum menunjukkan hasil yang menjanjikan, implementasi praktis dari komputasi kuantum dalam skala besar masih menghadapi tantangan besar. Komputer kuantum yang dapat menjalankan eksperimen dengan ukuran masalah yang lebih besar masih dalam tahap pengembangan awal. Stabilitas qubit dan integrasi sistem kuantum ke dalam infrastruktur teknologi yang ada masih menjadi masalah teknis yang harus diatasi. Oleh karena itu, meskipun algoritma kuantum menunjukkan potensi besar dalam meningkatkan efisiensi kriptografi, pengembangan praktis dari teknologi ini memerlukan waktu dan upaya yang signifikan.

Dengan hasil yang telah dicapai, perbandingan antara komputasi kuantum dan klasik menunjukkan bahwa komputasi kuantum memiliki potensi untuk merevolusi cara kita memandang dan mengelola sistem keamanan digital. Efisiensi yang ditawarkan oleh algoritma seperti Shor dan Grover membuka jalan untuk pengembangan sistem kriptografi yang lebih cepat dan lebih aman. Namun, tantangan implementasi dalam skala besar dan penerapan praktis

tetap menjadi hambatan utama yang perlu diatasi sebelum komputasi kuantum dapat diterapkan secara luas dalam kriptografi dan keamanan digital.

5. KESIMPULAN DAN SARAN

Kesimpulan

Komputasi kuantum memiliki potensi besar untuk meningkatkan efisiensi dan keamanan sistem kriptografi modern. Hasil eksperimen menunjukkan bahwa algoritma kuantum, khususnya Algoritma Shor dan Algoritma Grover, dapat menyelesaikan masalah kriptografi dengan waktu yang jauh lebih singkat dibandingkan dengan metode klasik. Algoritma Shor mampu memfaktorkan bilangan besar dalam waktu polinomial, yang mengancam keamanan sistem kriptografi kunci publik seperti RSA, sementara algoritma Grover mempercepat pencarian kunci enkripsi dalam skema simetris seperti AES dan 3DES. Dengan demikian, komputasi kuantum membuka kemungkinan untuk mengoptimalkan sistem kriptografi dan memperkuat sistem keamanan digital yang ada.

Saran

Penelitian lebih lanjut sangat diperlukan untuk mengembangkan algoritma kuantum yang lebih efisien dan aplikasinya dalam dunia keamanan digital. Pengembangan ini harus mencakup peningkatan kemampuan untuk menangani masalah kriptografi yang lebih kompleks dengan lebih cepat, serta penerapan algoritma kuantum dalam sistem yang lebih besar dan lebih praktis. Selain itu, penting untuk mempersiapkan transisi ke sistem yang tahan terhadap ancaman komputasi kuantum, seperti *Post-Quantum Cryptography* (PQC), yang dapat melindungi data dan komunikasi dari potensi serangan oleh komputer kuantum di masa depan.

DAFTAR REFERENSI

Ambainis, A., Bačkurs, A., Nahimovs, N., & Rivosh, A. (2013). *Grover's algorithm with errors*. In *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7721 LNCS, 180–189. https://doi.org/10.1007/978-3-642-36046-6_17

Bavdekar, R., Chopde, E.J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). *Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations*. In *International Conference on Information Networking* (pp. 146–151). https://doi.org/10.1109/ICOIN56518.2023.10048976

Chailloux, A., Naya-Plasencia, M., & Schrottenloher, A. (2017). *An efficient quantum collision search algorithm and implications on symmetric cryptography*. In *Lecture Notes in*

Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10625 LNCS, 211–240. https://doi.org/10.1007/978-3-319-70697-9_8

Chamma, E., McGee, A., Gillmann, A., McNallan, I., & Mahmoud, M. (2023). *Feasible Applications of Quantum Computing in Varying Fields*. In *Proceedings - 2023 International Conference on Computational Science and Computational Intelligence, CSCI 2023* (pp. 454–459). https://doi.org/10.1109/CSCI62032.2023.00080

Claudio, M., & Fernando, F. (2024). *Current and Future Panorama of Quantum and Post-Quantum Cryptography*. In *2024 7th IEEE Biennial Congress of Argentina, ARGENCON 2024*. https://doi.org/10.1109/ARGENCON62399.2024.10735956

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*. In *2024 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2024*. https://doi.org/10.1109/ICBDS61829.2024.10837282

Firmansyah, B., & Bansal, R. (2024). *Standardization and Regulatory Challenges in Modern Cryptography*. In *Metaverse Security Paradigms* (pp. 145–183). https://doi.org/10.4018/979-8-3693-3824-7.ch006

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*. In *Proceedings of the IEEE 3rd International Conference on Problems of Informatics, Electronics and Radio Engineering, PIERE 2024* (pp. 1480–1483). https://doi.org/10.1109/PIERE62470.2024.10805050

Haddouti, S.E., Kettani, M.D.E.-C.E., & Chaoui, H. (2024). *Unveiling Blockchain Security and Resilience in the Quantum Age: An Analytical Study of Post-Quantum and Quantum Approaches*. In *Proceedings - 7th International Conference on Advanced Communication Technologies and Networking, CommNet 2024*. https://doi.org/10.1109/CommNet63022.2024.10793363

Jenefa, A., Josh, F.T., Taurshia, A., Kumar, K.R., Kowsega, S., & Naveen, E. (2023). *PQC Secure: Strategies for Defending Against Quantum Threats*. In 2nd International Conference on Automation, Computing and Renewable Systems, ICACRS 2023 - Proceedings (pp. 1799-1804). https://doi.org/10.1109/ICACRS58579.2023.10404525

Juárez-Ramírez, R., Navarro, C.X., Jiménez, S., Ramírez, A., Tapia-Ibarra, V., Guerra-García, C., Perez-Gonzalez, H.G., & Fernández-y-Fernández, C. (2023). *A Taxonomic View of the Fundamental Concepts of Quantum Computing–A Software Engineering Perspective*. *Programming and Computer Software, 49*(8), 682–704. https://doi.org/10.1134/S0361768823080108

Ladino, I., Gomez, C., Corredor, C., & Toro, L. (2024). *Low-Compute Cryptography for IoT: Challenges, Solutions, and Perspectives*. In *Congreso Internacional de Innovacion y Tendencias en Ingenieria, CONIITI 2024*. https://doi.org/10.1109/CONIITI64189.2024.10854855

Panhwar, M.A., Khuhro, S.A., Mazhar, T., ZhongLiang, D., & Qadir, N. (2021). *Quantum*

Cryptography: A way of Improving Security of Information. International Journal of Mathematics and Computer Science, 16(1), 9-21. https://doi.org/10.1109/ICACRS58579.2023.10404525

Parikh, S., Jhanwar, R., & Singh, A. (2023). *Hybridization of AES and RSA Algorithm in File Encryption Using Parallel Computing*. In *Communications in Computer and Information Science, 1749 CCIS* (pp. 281–291). https://doi.org/10.1007/978-3-031-25088-0_25

Paul, B., & Trivedi, G. (2023). *Post Quantum Cryptography Algorithms: A Review and Applications*. *Lecture Notes in Networks and Systems, 685 LNNS*, 3–17. https://doi.org/10.1007/978-981-99-1912-3_1

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, 2022-April*. https://doi.org/10.1109/CICC53496.2022.9772841

Shadaksharappa, B., & Ramkumar, P. (2024). *Analysis of Drop-In-Replaceability Applying Post-Quantum Cryptography Techniques*. In *Harnessing Quantum Cryptography for Next-Generation Security Solutions* (pp. 75–88). https://doi.org/10.4018/979-8-3693-9220-1.ch003

Sharma, S., Ramkumar, K.R., Kaur, A., Hasija, T., Mittal, S., & Singh, B. (2023). *Post-quantum Cryptography: A Solution to the Challenges of Classical Encryption Algorithms*. Lecture Notes in Electrical Engineering, 948, 23-38. https://doi.org/10.1007/978-981-19-6383-4_3

Srivastava, P., Mishra, A., & Srivastava, Y.K. (2023). *From Quantum Mechanics to Quantum Computing*. In *Studies in Computational Intelligence* (Vol. 1085, pp. 15–30). https://doi.org/10.1007/978-981-19-9530-9_2

Wang, Y., & Xu, Q. (2020). *Principle and Research Progress of Quantum Computation and Quantum Cryptography [量子计算与量子密码的原理及研究进展综述]*. *Jisuanji Yanjiu yu Fazhan/Computer Research and Development, 57*(10), 2015–2026. https://doi.org/10.7544/issn1000-1239.2020.20200615

Wicaksana, A., & Wicaksono, A.W. (2020). *Web-app realization of Shor's quantum factoring algorithm and Grover's quantum search algorithm*. *Telkomnika (Telecommunication Computing Electronics and Control), 18*(3), 1319–1330. https://doi.org/10.12928/TELKOMNIKA.v18i3.14755