Information Technology Studies Journal (ITECH)
Vol 2 (3) 2025 : 207-217

QUANTUM INSPIRED ALGORITHMS FOR ENHANCING CRYPTOGRAPHIC SECURITY

ALGORITMA TERINSPIRASI KUANTUM UNTUK MENINGKATKAN KEAMANAN KRIPTOGRAFI

Mepa Kurniasih
Universitas Budi Luhur
*mepa.kurnia@gmail.com

**Corresponding Author*

ABSTRACT
The escalation of computing capabilities and the threats posed by quantum algorithms, such as Shor's and Grover's algorithms, have triggered an urgent need to re-evaluate the resilience of classical cryptographic architectures. The primary issue lies in the vulnerability of traditional key spaces to advanced heuristic attacks and the limitations of conventional evolutionary algorithms that frequently get trapped in local optima. This article provides an in-depth review of the potential integration of Quantum-Inspired Evolutionary Algorithms (QIEA) as a hybrid solution to strengthen cryptographic security. Using a narrative review method covering literature from the Scopus and Web of Science databases (2021–2026), this study analyzes the mechanisms of Q-bit representation and Quantum Rotation Gates in the key search process. The analysis results indicate that the application of superposition principles allows for the simultaneous exploration of vast key spaces without a linear increase in computational burden. This study proposes an adaptive cryptographic system framework encompassing four integration pillars: Q-bit-based key space exploration , parameter optimization in Elliptic Curve Cryptography (ECC) , S-Box strengthening in the Advanced Encryption Standard (AES) , and evolutionary proactive detection of key weaknesses. As a theoretical contribution, this model offers a transformation from static security to adaptive defense systems that are robust against various future cyberattack scenarios.
Keywords: Quantum-Inspired Evolutionary Algorithms, Cryptographic Security, Key Space, Q-bit Representation, Adaptive Cryptography.

ABSTRAK
Eskalasi kapabilitas komputasi dan ancaman dari algoritma kuantum, seperti algoritma Shor dan Grover, telah memicu urgensi untuk mengevaluasi kembali ketahanan arsitektur kriptografi klasik. Permasalahan utama terletak pada kerentanan ruang kunci (key space) tradisional terhadap serangan heuristik serta keterbatasan algoritma evolusioner konvensional yang sering terjebak dalam optimum lokal. Artikel ini bertujuan untuk meninjau secara mendalam potensi integrasi Quantum-Inspired Evolutionary Algorithms (QIEA) sebagai solusi hibrida dalam memperkuat keamanan kriptografi. Melalui metode tinjauan naratif terhadap literatur dari pangkalan data Scopus dan Web of Science (2021-2026), studi ini menganalisis mekanisme representasi Q-bit dan Quantum Rotation Gates dalam proses pencarian kunci. Hasil analisis menunjukkan bahwa penggunaan prinsip superposisi memungkinkan eksplorasi ruang kunci yang luas secara simultan tanpa peningkatan beban komputasi secara linear. Studi ini mengusulkan sebuah kerangka kerja sistem kriptografi adaptif yang mencakup empat pilar integrasi: eksplorasi ruang kunci berbasis Q-bit, optimasi parameter pada Elliptic Curve Cryptography (ECC), penguatan S-Box pada Advanced Encryption Standard (AES), serta deteksi dini kelemahan kunci secara evolusioner. Sebagai kontribusi teoritis, model ini menawarkan transformasi dari keamanan statis menuju sistem pertahanan yang adaptif dan tangguh terhadap berbagai skenario serangan siber di masa depan.
Keywords: Quantum-Inspired Evolutionary Algorithms, Cryptographic Security, Key Space, Q-bit Representation, Adaptive Cryptography.

1. PENDAHULUAN

Kemajuan kemampuan komputasi dalam dekade terakhir telah mengantarkan paradigma baru dalam bidang keamanan siber. Transformasi ini ditandai dengan meningkatnya ancaman yang ditimbulkan oleh komputasi kuantum, yang menantang arsitektur kriptografi tradisional. Metode kriptografi klasik sangat bergantung pada kompleksitas matematika, seperti faktorisasi prima besar dan logaritma diskrit, yang rentan terhadap algoritma kuantum seperti algoritma Shor dan Grover (Yang dkk., 2024). Karena ancaman ini semakin nyata, ada kebutuhan mendesak bagi pengembang sistem informasi untuk menilai kembali ketahanan infrastruktur keamanan mereka. Transisi ke era pasca-kuantum bukan hanya dugaan teoritis, tetapi persyaratan penting untuk menjaga integritas dan kerahasiaan data di tingkat global.

Salah satu kekhawatiran utama muncul dari kerentanan dalam ruang kunci konvensional ketika dihadapkan dengan serangan heuristik tingkat lanjut dan teknik kriptanalisis yang canggih. Ketergantungan pada peningkatan panjang kunci sebagai tindakan defensif sering dianggap sebagai solusi prematur. Memperpanjang panjang kunci memang dapat meningkatkan keamanan sampai batas tertentu, tetapi juga mengakibatkan peningkatan beban komputasi dan latensi sistem. Ketidakefisienan ini sangat bermasalah dalam skenario yang melibatkan sumber daya terbatas, seperti perangkat Internet of Things (IoT) dan platform seluler (Olaniyan dkk., 2023; Dolly, 2015).Selain masalah-masalah tersebut, algoritma evolusi tradisional untuk optimasi kunci sering kali konvergen pada optimasi lokal, yang menyebabkan kurangnya keragaman kunci. Homogenitas ini memberikan peluang lebih besar bagi penyerang untuk mengeksploitasi pola yang dapat diprediksi melalui analisis statistik atau serangan brute-force yang dioptimalkan (Singh et al., 2018; Annalakshmi & Jayanthi, 2024).

Efektivitas manajemen kunci kriptografi sangat penting dalam lingkungan yang semakin rentan terhadap ancaman kuantum. Algoritma evolusioner, seperti Algoritma Genetika (GA) dan Optimasi Swarm Partikel (PSO), dapat meningkatkan keacakan dan efektivitas proses pembangkitan kunci (Kusyk dkk., 2018; Farhadi, 2022). Namun, metode-metode ini secara inheren kesulitan dengan optimasi lokal. Teknik standar seringkali gagal untuk menghindari jebakan ini kecuali dimodifikasi untuk menggabungkan mekanisme yang mendorong eksplorasi ruang solusi (Bewoor dkk., 2017; Wang dkk., 2007; Friedl & Kuczmann, 2014). Pendekatan baru telah diusulkan untuk meningkatkan algoritma ini, seperti menggabungkan PSO dengan operator genetika untuk meningkatkan kinerja dan mencegah konvergensi prematur (Kangah dkk., 2021; Arunkumar, 2020; Donghui dkk., 2016).

Untuk mengatasi ancaman komputasi kuantum yang semakin nyata, para peneliti menganjurkan pengembangan metode kriptografi pasca-kuantum yang mampu menahan serangan kuantum. Sistem tersebut memanfaatkan algoritma kriptografi yang tetap aman terhadap algoritma kuantum seperti algoritma Shor dan Grover. Dua strategi utama yang diusulkan adalah adaptasi algoritma kriptografi klasik untuk meningkatkan ketahanannya dan eksplorasi algoritma baru yang sepenuhnya aman terhadap kuantum (Yang dkk., 2024).

Kesimpulannya, peningkatan kemampuan komputasi dan kedatangan komputasi kuantum yang akan segera terjadi menuntut evaluasi ulang yang signifikan terhadap paradigma keamanan siber saat ini. Kerentanan yang melekat pada sistem kriptografi tradisional menyoroti kebutuhan akan pendekatan inovatif yang memanfaatkan algoritma evolusioner untuk pembangkitan kunci yang kuat. Seiring para peneliti terus mengeksplorasi solusi kriptografi pasca-kuantum, urgensi untuk mengimplementasikan kemajuan ini ke dalam infrastruktur saat ini menjadi semakin mendesak untuk memastikan integritas dan kerahasiaan data dalam skala global. Transisi ke kerangka kerja pasca-kuantum merupakan elemen penting dalam menjaga masa depan keamanan siber.

Artikel ini bertujuan untuk meninjau secara mendalam potensi integrasi Algoritma Evolusi yang Terinspirasi Kuantum (QIEA) sebagai solusi hibrida dalam memperkuat arsitektur kriptografi. Dengan mengadopsi prinsip-prinsip mekanika kuantum seperti superposisi dan interferensi dalam kerangka kerja algoritma evolusioner klasik, QIEA menawarkan metodologi

baru untuk eksplorasi ruang pencarian kunci yang jauh lebih luas dan dinamis. Fokus utama tinjauan ini adalah bagaimana representasi bit kuantum (Q-bit) dapat meningkatkan diversitas populasi dalam pencarian kunci, sehingga menciptakan lapisan pertahanan yang lebih tangguh tanpa harus bergantung sepenuhnya pada perangkat keras kuantum murni yang saat ini masih dalam tahap pengembangan.

Kebaruan dari tinjauan ini terletak pada penekanan spesifik terhadap mekanisme integrasi prinsip kuantum ke dalam algoritma evolusioner untuk optimalisasi keamanan struktural, bukan sekadar mengejar kecepatan komputasi. Berbeda dengan studi terdahulu yang seringkali mengedepankan efisiensi waktu, analisis ini membedah bagaimana gerbang rotasi kuantum dan konsep probabilitas kuantum dapat memperumit entropi sistem kriptografi. Dengan demikian, penelitian ini memberikan kontribusi teoritis bagi pengembangan skema kriptografi yang tidak hanya efisien secara algoritmik, tetapi juga memiliki ketahanan yang lebih tinggi terhadap berbagai skenario serangan siber di masa depan.

2. METODE

Metodologi penulisan tinjauan naratif ini didasarkan pada pemilihan literatur primer yang ketat untuk menjamin validitas dan relevansi akademik. Data dikumpulkan melalui pencarian sistematis pada pangkalan data bereputasi internasional, yaitu Scopus dan Web of Science (WoS), dengan fokus pada publikasi jurnal dalam rentang waktu lima tahun terakhir (2021–2026). Strategi pencarian menggunakan kombinasi kata kunci spesifik seperti "Algoritma Evolusi yang Terinspirasi Kuantum","Keamanan Kriptografi","Optimasi Ruang Kunci", dan "Sistem Informasi Pasca Kuantum". Kriteria inklusi diprioritaskan pada artikel penelitian yang menyajikan model integrasi teoritis maupun empiris dari algoritma QIEA dalam skema enkripsi, guna memastikan bahwa sintesis yang dihasilkan mencerminkan perkembangan terkini dalam keamanan siber.

Pendekatan sintesis temuan dilakukan melalui analisis komparatif dan integratif untuk menjawab bagaimana mekanisme QIEA diaplikasikan pada sistem kriptografi simetris dan asimetris. Proses ini melibatkan identifikasi komponen inti kuantum—seperti representasi Q-bitdan menggunakangerbang rotasi kuantum serta bagaimana komponen tersebut memengaruhi parameter keamanan pada algoritma seperti AES (simetris) dan Kriptografi Kurva Elips (asimetris). Dengan mengkategorikan literatur berdasarkan arsitektur enkripsi yang digunakan, tinjauan ini mampu memetakan pola integrasi yang paling efektif untuk meningkatkan kompleksitas ruang kunci. Pendekatan ini memastikan bahwa argumen yang dibangun dalam artikel ini didukung oleh bukti lintas disiplin antara teori informasi kuantum dan sistem keamanan informasi klasik.

3. HASIL DAN PEMBAHASAN

3.1. *QIEA Integration Mechanism: Analysis of Q-bit Representation and Quantum Rotation Gates in Key Search Process*

Algoritma evolusi yang terinspirasi kuantum (QIEA) memanfaatkan prinsip-prinsip dari komputasi kuantum, khususnya penggunaan representasi Q-bit dan gerbang kuantum, untuk meningkatkan kinerja dalam tugas optimasi, seperti pencarian kunci dalam kriptografi. Analisis ini mengeksplorasi bagaimana mekanisme ini memfasilitasi pemulihan kunci yang efisien, terutama melalui algoritma Grover dan adaptasinya dalam konteks kriptografi.

Q-bit Representation in QIEAs

Representasi Q-bit berfungsi sebagai tulang punggung Algoritma Evolusi yang Terinspirasi Kuantum. Representasi unik ini memungkinkan solusi individual untuk dikodekan bukan sebagai string biner, tetapi sebagai model probabilistik di mana setiap Q-bit dapat mewakili banyak keadaan secara bersamaan.(Khan, 2010;,Li dkk., 2010) Karakteristik ini meningkatkan kemampuan algoritma untuk menjelajahi ruang pencarian yang besar, karena

dapat mempertahankan populasi solusi potensial yang beragam. Dalam konteks seperti optimasi kombinatorial, Q-bit memfasilitasi eksplorasi kemungkinan yang sulit dilakukan oleh metode klasik, memberikan QIEA keunggulan dibandingkan algoritma genetika tradisional dalam skenario seperti masalah knapsack 0/1 dan penjadwalan pekerjaan.(Patvardhan dkk., 2015;,Li & Wang, 2007;,(Moriyama dkk., 2015). Selain itu, representasi Q-bit secara inheren mendukung pemilihan solusi secara probabilistik, sehingga memungkinkan QIEA untuk mengeksplorasi ruang solusi yang lebih luas secara efisien. Dengan menggunakan representasi ini, QIEA berhasil menyeimbangkan eksplorasi dan eksploitasi secara efektif.(Moriyama dkk., 2015;,Takata dkk., 2011).

Quantum Rotation Gates and Their Application

Penerapan gerbang rotasi kuantum (Q-gate) adalah fitur penting lain yang membedakan QIEA dari algoritma evolusi klasik. Q-gate berfungsi secara analog dengan operator variasi klasik, memodifikasi keadaan Q-bit untuk mendorong keragaman dan konvergensi menuju solusi optimal.(Khan, 2010;,(Pavithr & Gursaran, 2013)Gerbang-gerbang ini memungkinkan algoritma untuk menavigasi lanskap kompleks secara efektif, menerapkan prinsip-prinsip kuantum seperti interferensi dan superposisi untuk meningkatkan proses pencarian.

Sebagai contoh, Algoritma Kuantum Genetik (GQA) menggabungkan gerbang rotasi kuantum untuk memanipulasi Q-bit selama evolusi, yang secara signifikan mempengaruhi proses pencarian genetik (Pavithr & Gursaran, 2013)Studi menunjukkan bahwa penggabungan gerbang-Q sebagai operator genetik dapat secara signifikan meningkatkan kinerja QIEA dalam memecahkan masalah optimasi.(Jeong dkk., 2010;,Takata dkk., 2011)Hal ini sangat relevan dalam skenario pemulihan kunci kriptografi, dimana ruang pencarian sangat luas, dan metode tradisional tidak mampu mengatasinya.Jang dkk., 2021),(Grassl dkk., 2016;.

Key Search Process and Cryptographic Applications

Dalam kriptografi, integrasi QIEA dengan representasi Q-bit dan gerbang Q menghadirkan kemajuan signifikan, khususnya dalam proses pencarian kunci. Algoritma Grover, yang secara teoritis menawarkan percepatan kuadratik untuk pencarian basis data yang tidak terurut, adalah contoh utama bagaimana prinsip kuantum dapat diterapkan.Jang dkk., 2021)Ketika diadaptasi untuk kriptanalisis, seperti pencarian kunci dalam cipher blok seperti AES, QIEA berpotensi mengurangi kompleksitas komputasi dari O(2^n) menjadi O(2^(n/2)), sehingga menjadikannya sangat ampuh terhadap panjang kunci simetris.(Davenport & Pring, 2021;,(Grassl dkk., 2016)

Studi telah memvalidasi kelayakan penggunaan QIEA untuk pemulihan kunci, menunjukkan bahwa biaya tambahan yang terkait dengan implementasi oracle kuantum dapat diminimalkan, sehingga meningkatkan efisiensi.(Davenport & Pring, 2021;,Jang dkk., 2021)Metodologi ini memungkinkan penyerang untuk melakukan pencarian kunci secara menyeluruh dengan lebih cepat daripada algoritma klasik, menandai pergeseran paradigma dalam pertimbangan keamanan di bidang kriptografi.(Grassl dkk., 2016;,Ranea & Rijmen, 2022).

Integrasi representasi Q-bit dan gerbang rotasi kuantum dalam QIEA secara signifikan meningkatkan kemampuan algoritma ini untuk tugas optimasi yang menantang, termasuk proses pencarian kunci kriptografi. Kemampuan untuk merepresentasikan solusi secara probabilistik dan memanfaatkan operasi yang terinspirasi kuantum memfasilitasi eksplorasi ruang pencarian yang luas secara efisien, menjadikan QIEA sebagai alat yang tangguh dalam analisis kriptografi kontemporer. Seiring penelitian yang terus dilakukan untuk menyempurnakan algoritma ini, implikasinya terhadap paradigma keamanan di masa depan tidak diragukan lagi akan sangat besar.

3.2.Peningkatan Kompleksitas Ruang Kunci

Eksplorasi ruang kunci yang lebih besar yang difasilitasi oleh prinsip-prinsip komputasi kuantum, khususnya melalui representasi superposisi, memiliki implikasi signifikan dalam bidang kriptografi dan keamanan data. Superposisi memungkinkan representasi beberapa keadaan secara simultan, memungkinkan sistem kuantum untuk mengeksplorasi ruang kunci yang jauh lebih besar secara eksponensial tanpa peningkatan sumber daya komputasi yang proporsional.

Quantum Superposition and Enhanced Key Space

Superposisi dalam mekanika kuantum memungkinkan sebuah bit quantum (qubit) untuk berada dalam banyak keadaan sekaligus. Fenomena ini merupakan dasar yang memungkinkan algoritma kuantum untuk memproses sejumlah besar informasi secara simultan. Untuk aplikasi kriptografi, seperti yang dibahas oleh Ige dkk., penggunaan keadaan kuantum (phi-bit) untuk mengkodekan informasi menunjukkan bagaimana sistem kriptografi tradisional menghadapi tantangan dari kemampuan kuantum.(Ige dkk., 2024)Bit-phi ini menunjukkan superposisi yang mirip dengan qubit, yang secara substansial meningkatkan kompleksitas kunci potensial yang digunakan dalam enkripsi.

Karya Farsana dan Gopakumar tentang enkripsi suara semakin mengilustrasikan poin ini, di mana bit klasik diubah menjadi keadaan kuantum nonortogonal, sehingga meningkatkan kesulitan akses tanpa izin (Farsana & Gopakumar, 2020). Penerapan gerbang Controlled-NOT dalam algoritma enkripsi mereka menunjukkan kegunaan fenomena kuantum dalam menciptakan konfigurasi kunci yang kompleks, yang secara bersamaan memanfaatkan sifat klasik dan kuantum untuk meningkatkan keamanan.

Computational Burden vs. Exponential Key Space Growth

Salah satu keunggulan paling menarik dari penggunaan superposisi dalam sistem enkripsi kuantum adalah pengurangan beban komputasi sambil tetap mencapai peningkatan ruang kunci yang signifikan. Eksplorasi Liu tentang enkripsi gambar kuantum menekankan bagaimana sistem kuantum dapat memanfaatkan paralelisme yang melekat pada strukturnya. Peta Baker, misalnya, memungkinkan proses pengacakan dan pengkodean yang efisien yang secara signifikan memperluas ruang kunci dengan biaya komputasi tambahan minimal.(Liu, 2023)Metode ini menunjukkan bahwa operasi kuantum dapat menyederhanakan proses yang biasanya membutuhkan sumber daya yang besar dalam sistem klasik.

Selain itu, Wu dkk. mengusulkan kerangka kerja hibrida kuantum-klasik untuk meningkatkan pelatihan model bahasa besar (LLM) dengan mengintegrasikan prinsip-prinsip kuantum seperti superposisi dan keterikatan. Integrasi ini memungkinkan pemodelan data yang lebih canggih, memanfaatkan ruang Hilbert berdimensi lebih tinggi untuk merepresentasikan informasi secara lebih kaya daripada pendekatan klasik.(Wu dkk., 2025)Kemampuan ini sangat relevan ketika mempertimbangkan skenario enkripsi data, karena menunjukkan bahwa superposisi dapat dimanfaatkan untuk mengeksplorasi kunci enkripsi yang membutuhkan banyak komputasi untuk dihitung melalui metode klasik.

Future Implications of Quantum Key Spaces

Implikasi dari pemanfaatan superposisi untuk ruang kunci yang luas meluas ke aplikasi masa depan komunikasi aman dan penyimpanan data. Seiring perkembangan bidang kriptografi kuantum, metode yang memanfaatkan prinsip superposisi kemungkinan akan menjadi sangat penting dalam merancang sistem yang tidak hanya aman terhadap musuh kuantum tetapi juga efisien dalam kebutuhan komputasinya. Kemajuan saat ini menunjukkan bahwa penggabungan algoritma tahan kuantum akan sangat penting seiring dengan kematangan teknologi komputasi kuantum.(Rosales & Martín, 2016).

Namun, sangat penting untuk mendekati perkembangan ini dengan pemahaman tentang keterbatasan yang ada dan tantangan potensial terkait tingkat kesalahan dan implementasi praktis pada perangkat kuantum. Eksplorasi teknik untuk mengoptimalkan simulasi sirkuit kuantum dan menyempurnakan algoritma untuk pengkodean data akan terus menjadi vital untuk mewujudkan janji sistem kriptografi yang ditingkatkan secara kuantum.(Liu dkk., 2024;,Karimi dkk., 2025).

Kesimpulannya, representasi superposisi dalam komputasi kuantum menghadirkan pendekatan transformatif untuk menjelajahi ruang kunci yang lebih besar dalam enkripsi, dan mencapai hal ini dengan beban komputasi yang lebih rendah daripada yang dibutuhkan dalam sistem klasik. Perpaduan yang berkembang antara teori kuantum dan keamanan informasi menjanjikan paradigma baru untuk melindungi data sensitif di dunia yang semakin digital.

3.3.Komparasi Arsitektur

Dalam ranah sistem kriptografi, pilihan arsitektur algoritma enkripsi simetris dan asimetris menghadirkan keunggulan dan tantangan operasional yang berbeda. Sintesis ini mengeksplorasi efektivitas integrasi dalam algoritma simetris, khususnya berfokus pada penguatan S-Box dalam Advanced Encryption Standard (AES), dan membandingkannya dengan optimasi parameter dalam algoritma asimetris, terutama kriptografi kurva eliptik (ECC).

Symmetric Algorithms: S-Box Strengthening in AES

Algoritma kriptografi simetris, seperti AES, menggunakan satu kunci untuk enkripsi dan dekripsi, yang memungkinkan pemrosesan yang efisien dan beban komputasi yang lebih rendah. Inti dari keamanan AES adalah S-Box-nya, yang meningkatkan non-linearitas dan difusi, sehingga membuatnya tahan terhadap berbagai bentuk kriptanalisis, termasuk serangan diferensial dan linier. Desain dan optimasi S-Box secara signifikan mempengaruhi kekuatan dan kinerja AES. Peningkatan terbaru bertujuan untuk meningkatkan konstruksi S-Box guna memastikan efek longsoran yang lebih baik dan ketahanan terhadap serangan saluran samping, yang menunjukkan peran penting arsitektur S-Box dalam menjaga standar keamanan.(Baig dkk., 2024; Aydın & Özkaynak, 2023).

Penggunaan akselerasi perangkat keras dalam implementasi AES semakin memposisikan algoritma simetris secara menguntungkan di lingkungan yang membutuhkan operasi enkripsi dan dekripsi berkecepatan tinggi (misalnya, transfer data jaringan).(Uzuner & Kavun, 2024; Kumar dkk., 2021)Selain itu, efisiensi kinerja pada algoritma simetris sangat signifikan, terutama di lingkungan terbatas di mana keterbatasan sumber daya menjadi perhatian, seperti pada jaringan sensor nirkabel (WSN) dan aplikasi Internet of Things (IoT).(Wang dkk., 2011; Maqsood dkk., 2017).

Asymmetric Algorithms: Parameter Optimization in ECC

Sebaliknya, algoritma asimetris seperti ECC menggunakan sepasang kunci (publik dan privat), yang menyederhanakan manajemen kunci tetapi menimbulkan biaya komputasi yang lebih tinggi karena operasi matematika kompleks yang terlibat dalam menghasilkan dan menggunakan kunci. ECC, khususnya, telah mendapatkan popularitas karena kemampuannya untuk menawarkan keamanan yang setara dengan skema tradisional (seperti RSA) menggunakan panjang kunci yang jauh lebih pendek, sehingga mengurangi biaya tambahan.(Rezai dkk., 2016; (Tuo, 2023;Optimalisasi dalam pemilihan parameter—seperti pemilihan kurva eliptik—telah terbukti secara signifikan mempengaruhi efisiensi dan tingkat keamanan algoritma, menjadikan ECC sebagai pilihan yang lebih disukai di lingkungan yang membutuhkan langkah-langkah keamanan yang kuat dengan daya komputasi yang terbatas.

Skema berbasis ECC tidak hanya meningkatkan efisiensi komputasi tetapi juga menyederhanakan proses kesepakatan kunci dan tanda tangan digital, yang sangat penting dalam berbagai aplikasi keamanan, termasuk WSN.(Chandra dkk., 2014; Singh & Jain,

2021)Meskipun memiliki keunggulan, algoritma asimetris tetap menunjukkan masalah latensi karena kerumitan matematisnya, sehingga menimbulkan kekhawatiran tentang kesesuaiannya di lingkungan berkinerja tinggi di mana algoritma simetris lebih unggul.(Subedar & Ashwini, 2020; Horsch dkk., 2016).

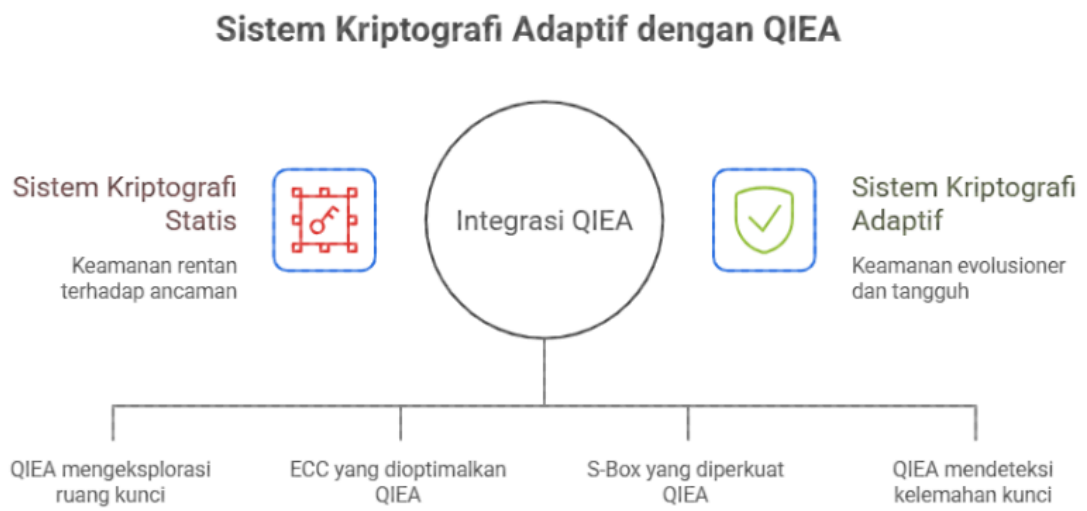
Comparative Analysis: Integration and Effectiveness

Perbedaan arsitektur antara algoritma simetris dan asimetris menghadirkan implikasi yang lebih kompleks terhadap integrasinya dalam solusi kriptografi. Algoritma simetris, khususnya dengan optimasi seperti peningkatan S-Box pada AES, menunjukkan metrik kinerja yang unggul terkait kecepatan pemrosesan dan pemanfaatan sumber daya di lingkungan di mana enkripsi/dekripsi cepat sangat penting.(Mandal dkk., 2014; Kumar dkk., 2021)Sebaliknya, kekuatan ECC terletak pada kemampuannya untuk mempertahankan tingkat keamanan yang tinggi dengan ukuran kunci yang diminimalkan dan manajemen yang lebih sederhana dibandingkan dengan sistem kriptografi kunci publik tradisional.(Tuo, 2023; Chandre dkk., 2023).

Sistem hibrida, yang mengintegrasikan pendekatan simetris dan asimetris, telah muncul untuk memanfaatkan kekuatan masing-masing metode sekaligus mengurangi kelemahannya. Misalnya, penggunaan metode asimetris untuk pertukaran kunci diikuti dengan enkripsi simetris untuk transmisi data menawarkan arsitektur keamanan yang seimbang yang dapat beradaptasi dengan berbagai lingkungan dan persyaratan.(Subedar & Ashwini, 2020; Maqsood et al., 2017).

Singkatnya, meskipun penguatan S-Box dalam algoritma simetris seperti AES memfasilitasi kinerja kriptografi berkecepatan tinggi, algoritma asimetris seperti ECC menawarkan keunggulan yang menarik dalam skenario yang membutuhkan keamanan yang kuat dengan manajemen kunci yang efisien. Memahami perbedaan arsitektur ini dapat membantu dalam pemilihan skema kriptografi dalam implementasi praktis, meningkatkan protokol keamanan di berbagai aplikasi. Perkembangan di masa mendatang di kedua domain ini kemungkinan akan terus menyempurnakan integrasinya, dengan tujuan meningkatkan keamanan dan kinerja di dunia yang semakin saling terhubung.

3.4.Framework Konseptual:



Implementasi model sistem kriptografi adaptif berbasis Quantum Inspired Evolutionary Algorithms (QIEA) merepresentasikan pergeseran paradigma dari arsitektur keamanan statis menuju sistem pertahanan yang evolusioner. Pada model konvensional, sistem kriptografi statis

sangat rentan terhadap eskalasi ancaman siber karena ketergantungan pada kompleksitas matematis yang kaku dan ruang kunci (key space) yang terbatas. Integrasi QIEA hadir sebagai mesin penggerak utama yang mentransformasi kerentanan tersebut melalui pemanfaatan prinsip mekanika kuantum dalam struktur algoritma evolusioner. Strategi ini memungkinkan sistem untuk tidak hanya mengoptimalkan efisiensi komputasi, tetapi juga memperkuat ketahanan struktural terhadap berbagai teknik cryptanalysis modern.

Secara teknis, kerangka kerja ini bekerja melalui empat pilar integrasi utama yang mencakup aspek hibrida dari sistem keamanan informasi. Pertama, QIEA melakukan eksplorasi ruang kunci secara masif dengan memanfaatkan representasi Q-bit dan prinsip superposisi, yang memungkinkan representasi berbagai kemungkinan kunci secara simultan untuk mencapai entropi maksimal. Kedua, pada ranah algoritma asimetris, QIEA digunakan untuk optimasi parameter pada Elliptic Curve Cryptography (ECC), menjamin keamanan yang kokoh dengan panjang kunci yang lebih pendek dan efisien. Ketiga, pada algoritma simetris seperti AES, integrasi ini difokuskan pada penguatan struktur S-Box guna meningkatkan non-linearitas dan efek avalanche. Terakhir, sistem ini memiliki kemampuan proaktif untuk mendeteksi kelemahan kunci secara periodik, di mana quantum rotation gates memfasilitasi konvergensi cepat menuju konfigurasi kunci baru yang lebih optimal jika terdeteksi adanya risiko keamanan.

Sinergi dari mekanisme tersebut menghasilkan sebuah sistem kriptografi adaptif yang mampu merespons dinamika ancaman di era pasca-kuantum. Dengan memanfaatkan paralelisme inherent dari struktur kuantum, sistem dapat memperluas ruang kunci secara eksponensial tanpa memicu beban komputasi yang tidak proporsional. Hal ini sangat krusial bagi implementasi pada infrastruktur sistem informasi dengan sumber daya terbatas, seperti perangkat IoT atau komunikasi seluler. Melalui pendekatan evolusioner ini, keamanan informasi tidak lagi dipandang sebagai parameter statis, melainkan sebuah proses dinamis yang terus beradaptasi untuk menjaga integritas dan kerahasiaan data di tingkat global.

4. KESIMPULAN

Integrasi Algoritma Evolusi yang Terinspirasi Kuantum (QIEA) terbukti menjadi solusi transformatif dalam meningkatkan ketahanan sistem kriptografi menghadapi ancaman era pasca-kuantum. Temuan penelitian ini menunjukkan bahwa penggunaan representasi Q-bit memungkinkan eksplorasi ruang kunci yang jauh lebih luas melalui prinsip superposisi, yang secara signifikan meningkatkan entropi dan diversitas populasi solusi tanpa memicu peningkatan beban komputasi secara linear. Selain itu, mekanisme Gerbang Rotasi Kuantum memberikan keunggulan dalam proses pencarian kunci dan optimasi parameter algoritma, seperti penguatan Kotak S pada AES dan efisiensi manajemen parameter pada ECC, yang secara kolektif memperkuat pertahanan terhadap teknik pembacaan sandi modern.

Bagi praktisi Sistem Informasi, hasil tinjauan ini memberikan implikasi manajerial yang krusial dalam perancangan infrastruktur keamanan yang adaptif. Pengadopsian model integrasi QIEA memungkinkan organisasi untuk mempertahankan standar keamanan tingkat tinggi pada perangkat dengan sumber daya terbatas, seperti IoT dan komunikasi seluler, tanpa harus menunggu ketersediaan perangkat keras kuantum murni secara komersial. Implementasi kerangka kerja manajemen kunci yang berbasis algoritma evolusioner ini menawarkan fleksibilitas bagi para manajer TI untuk mengkonfigurasi ulang parameter keamanan secara dinamis sesuai dengan profil ancaman yang terus berkembang.

Penelitian masa depan harus diarahkan pada validasi empiris dari model QIEA yang diusulkan dalam skenario serangan siber dunia nyata untuk mengukur ketahanannya secara lebih presisi. Selain itu, eksplorasi terhadap reduksi tingkat kesalahan (tingkat kesalahan) dan optimalisasi sirkuit simulasi kuantum tetap menjadi tantangan vital yang perlu dipecahkan untuk merealisasikan potensi penuh sistem kriptografi yang diperkuat kuantum. Studi lebih lanjut juga disarankan untuk mengeksplorasi sistem hibrida yang menggabungkan QIEA dengan

kecerdasan buatan untuk menciptakan sistem keamanan yang tidak hanya tangguh secara matematis, tetapi juga cerdas dalam mendeteksi anomali secara waktu nyata.

6. DAFTAR PUSTAKA

Annalakshmi, D., & Jayanthi, C. (2024). An asymmetric key encryption and decryption model incorporating optimization techniques for enhanced security and efficiency. The Scientific Temper, 15(3), 2663–2671. https://doi.org/10.58414/scientifictemper.2024.15.3.34

Arunkumar, J. (2020). Chaotic African buffalo optimization based efficient key mechanism in categorized sensor networks. International Journal of Engineering and Advanced Technology, 9(3), 1232–1238. https://doi.org/10.35940/ijeat.c5351.029320

Bewoor, L., Prakash, V., & Sapkal, S. (2017). Evolutionary hybrid particle swarm optimization algorithm for solving NP-hard no-wait flow shop scheduling problems. Algorithms, 10(4), 121. https://doi.org/10.3390/a10040121

Davenport, J., & Pring, B. (2021). Improvements to quantum search techniques for block-ciphers, with applications to AES. In Lecture Notes in Computer Science (pp. 360–384). Springer. https://doi.org/10.1007/978-3-030-81652-0_14

Dolly, U. (2015). The particle swarm optimization based linear cryptanalysis of advanced encryption standard algorithm. International Journal on Recent and Innovation Trends in Computing and Communication, 3(4), 1767–1769. https://doi.org/10.17762/ijritcc2321-8169.150408

Donghui, Z., Lu, H., Hao, W., & Jin, D. (2016). Improving particle swarm optimization: Using neighbor heuristic and Gaussian cloud learning. Intelligent Data Analysis, 20(1), 167–182. https://doi.org/10.3233/ida-150799

Farhadi, S. (2022). A review on the impact of evolutionary optimization algorithms in enhancing learning processes. Journal of Social Innovation and Educational Development, 2(2), 10–18. https://doi.org/10.61838/jsied.2.2.2

Farsana, F., & Gopakumar, K. (2020). Speech encryption algorithm based on nonorthogonal quantum state with hyperchaotic keystreams. Advances in Mathematical Physics, 2020, 1–12. https://doi.org/10.1155/2020/8050934

Friedl, G., & Kuczmann, M. (2014). Population and gradient based optimization techniques: A theoretical overview. Acta Technica Jaurinensis, 7(4). https://doi.org/10.14513/actatechjaur.v7.n4.342

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In Post-Quantum Cryptography (pp. 29–43). Springer. https://doi.org/10.1007/978-3-319-29360-8_3

Ige, A., Cavalluzzi, D., Djordjević, I., Runge, K., & Deymier, P. (2024). Information encoding and encryption in acoustic analogues of qubits. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-65800-z

Jang, K., Song, G., Kim, H., Kwon, H., Kim, H., & Seo, H. (2021). Efficient implementation of PRESENT and GIFT on quantum computers. Applied Sciences, 11(11), 4776. https://doi.org/10.3390/app11114776

Jeong, Y., Park, J., Jang, S., & Lee, K. (2010). A new quantum-inspired binary PSO: Application to unit commitment problems for power systems. IEEE Transactions on Power Systems, 25(3), 1486–1495. https://doi.org/10.1109/tpwrs.2010.2042472

Kangah, J., Appati, J., Darkwah, K., & Soli, M. (2021). Implementation of an H-PSOGA optimization model for vehicle routing problem. International Journal of Applied Metaheuristic Computing, 12(3), 148–162. https://doi.org/10.4018/ijamc.2021070106

Karimi, A., Zadeh-Haghighi, H., Kora, Y., & Simon, C. (2025). The role of entanglement in quantum reservoir computing with coupled Kerr nonlinear oscillators. Proceedings of SPIE, 73. https://doi.org/10.1117/12.3066098

Khan, M. (2010). Influence of probability of variation operator on the performance of quantum-inspired evolutionary algorithm for 0/1 knapsack problem. The Open Artificial Intelligence Journal, 4(1), 37–48. https://doi.org/10.2174/1874061801004010037

Kusyk, J., Uyar, M., & Şahin, C. (2018). Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks. Evolutionary Intelligence, 10(3–4), 95–117. https://doi.org/10.1007/s12065-018-0154-4

Li, B., & Wang, L. (2007). A hybrid quantum-inspired genetic algorithm for multiobjective flow shop scheduling. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(3), 576–591. https://doi.org/10.1109/tsmcb.2006.887946

Li, H., Landa-Silva, D., & Gandibleux, X. (2010). Evolutionary multi-objective optimization algorithms with probabilistic representation based on pheromone trails. In Proceedings of the IEEE Congress on Evolutionary Computation (pp. 1–8). https://doi.org/10.1109/cec.2010.5585998

Liu, X., Chen, Q., Zhao, R., Liu, G., Guan, S., Wu, L., & Fan, X. (2024). Quantum image encryption algorithm based on four-dimensional chaos. Frontiers in Physics, 12. https://doi.org/10.3389/fphy.2024.1230294

Liu, X. (2023). Quantum image encryption based on Baker map and DNA circular shift operation. Physica Scripta, 98(11), 115112. https://doi.org/10.1088/1402-4896/ad0099

Moriyama, Y., Iimura, I., Ohno, T., & Nakayama, S. (2015). An experimental study on optimization in permutation spaces by quantum-inspired evolutionary algorithm using quantum bit representation. Journal of Signal Processing, 19(6), 227–234. https://doi.org/10.2299/jsp.19.227

Olaniyan, O., Olusesi, A., Omodunbi, B., Wahab, W., Adetunji, O., & Olukoya, B. (2023). A data security model for mobile ad hoc network using linear function mayfly advanced encryption standard. International Journal of Emerging Technology and Advanced Engineering, 13(3), 101–110. https://doi.org/10.46338/ijetae0323_10

Patvardhan, C., Bansal, S., & Srivastav, A. (2017). Towards the right amount of randomness in quantum-inspired evolutionary algorithms. Soft Computing, 21(7), 1765–1784. https://doi.org/10.1007/s00500-015-1880-5

Pavithr, R. (2013). A random search and greedy selection based genetic quantum algorithm for combinatorial optimization. In Proceedings of the IEEE Congress on Evolutionary Computation (pp. 2422–2427). https://doi.org/10.1109/cec.2013.6557859

Ranea, A., & Rijmen, V. (2022). Characteristic automated search of cryptographic algorithms for distinguishing attacks (CASCADA). IET Information Security, 16(6), 470–481. https://doi.org/10.1049/ise2.12077

Rosales, J., & Martín, V. (2016). Quantum simulation of the factorization problem. Physical Review Letters, 117(20). https://doi.org/10.1103/physrevlett.117.200502

Singh, N., Sb, S., & Singh, S. (2018). Solution of bio-medical problem by genetic algorithm. Journal of Biomedical Sciences, 7(1). https://doi.org/10.4172/2254-609x.100081

Takata, T., Isokawa, T., & Matsui, N. (2011). Performance analysis of quantum-inspired evolutionary algorithm. Journal of Advanced Computational Intelligence and Intelligent Informatics, 15(8), 1095–1102. https://doi.org/10.20965/jaciii.2011.p1095

Wang, H., Li, H., Liu, Y., Li, C., & Zeng, S. (2007). Opposition-based particle swarm algorithm with Cauchy mutation. In Proceedings of the IEEE Congress on Evolutionary Computation (pp. 4750–4756). https://doi.org/10.1109/cec.2007.4425095

Wu, N., Song, F., & Li, X. (2025). Quantum-enhanced training of large language models: A hybrid approach. Proceedings of SPIE, 14. https://doi.org/10.1117/12.3057017

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Pietro, R., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. IEEE Communications Surveys & Tutorials, 26(2), 967–1002. https://doi.org/10.1109/comst.2023.3325761