Jurnal Ekonomi, Manajemen, Bisnis dan Akuntansi Review Vol: 5, No 2, 2025, Page: 1-10

Quantum Computing dan Implikasinya Terhadap Keamanan Sistem Akuntansi: Kajian Literatur

Aprita Ravenna Ginting*, Cindy Aulia Rusli, Riska Harianingsih, Jufri Darma

Universitas Negeri Medan

Abstrak: Tujuan penelitian ini adalah untuk menilai dampak komputasi kuantum terhadap perlindungan data akuntansi yang selama ini bergantung pada kriptografi konvensional seperti RSA dan ECC. Penelitian ini menggunakan pendekatan studi literatur yang mencakup jurnal ilmiah, white paper, dan standar internasional yang relevan dengan post-quantum cryptography. Analisis yang dilakukan mengungkapkan bahwa algoritma kuantum, seperti Shor dan Grover, dapat melemahkan kekuatan enkripsi digital yang digunakan dalam sistem akuntansi saat ini, yang berisiko merusak integritas serta kerahasiaan data akuntansi. Sebagai solusi terhadap ancaman tersebut, disarankan untuk menerapkan kriptografi pasca-kuantum berbasis lattice dan hash, serta mengintegrasikan quantum blockchain untuk memastikan perlindungan data dalam jangka panjang. Penelitian ini juga menekankan pentingnya kesiapan organisasi akuntansi dan lembaga regulator dalam menghadapi potensi risiko keamanan yang dapat muncul akibat kemajuan pesat dalam teknologi komputasi kuantum.

Kata Kunci: Komputasi Kuantum, Sistem Akuntansi, Keamanan Informasi, Kriptografi Konvensional, *Post-Quantum Cryptography*, *Quantum Blockchain*

DOI: https://doi.org/10.53697/emba.v5i2.3080
*Correspondence: Aprita Ravenna Ginting
Email: apritarvnginting06@gmail.com

Received: 23-10-2025
Accepted: 23-11-2025
Published: 23-12-2025

Abstract: *The purpose of this study is to assess the impact of quantum computing on accounting data protection, which has traditionally relied on conventional cryptography such as RSA and ECC. This study uses a literature review approach that includes scientific journals, white papers, and international standards relevant to post-quantum cryptography. The analysis reveals that quantum algorithms, such as Shor and Grover, can weaken the strength of digital encryption used in current accounting systems, which risks compromising the integrity and confidentiality of accounting data. As a solution to this threat, it is recommended to implement lattice-based and hash-based post-quantum cryptography, as well as integrate quantum blockchain to ensure long-term data protection. This research also emphasizes the importance of accounting organizations and regulatory agencies being prepared to face potential security risks that may arise due to rapid advances in quantum computing technology.*

Keywords: *Quantum Computing, Accounting Systems, Information Security, Conventional Cryptography, Post-Quantum Cryptography, Quantum Blockchain*

Pendahuluan

Perkembangan teknologi digital telah membawa perubahan besar dalam sistem informasi akuntansi, terutama dalam pengelolaan data transaksi, pelaporan keuangan, dan keamanan informasi. Di tengah pesatnya perkembangan ini, muncul teknologi komputasi kuantum yang diyakini mampu merevolusi berbagai aspek pemrosesan data. Berbasis pada prinsip superposisi dan entanglement, komputer kuantum dapat memproses informasi

secara paralel dengan kecepatan eksponensial dibandingkan komputer klasik (Lazirko, 2023; Kurniawan et al., 2023; Shadan & Islam, 2025).

Hal ini berimplikasi pada meningkatnya kerentanan terhadap kebocoran data akuntansi, manipulasi laporan keuangan, serta hilangnya kepercayaan terhadap sistem digital perusahaan. Untuk mengantisipasi hal tersebut, berbagai penelitian mulai mengarahkan perhatian pada penerapan post-quantum cryptography yang mencakup algoritma tahan-kuantum, seperti *lattice-based cryptography*, *hash-based cryptography*, dan integrasi dengan *quantum blockchain*. Pendekatan ini dipandang sebagai solusi potensial dalam menjaga kerahasiaan, integritas, dan keaslian data akuntansi di era komputasi kuantum (Fernández-Caramés & Fraga-Lamas, 2024). Selain itu, kesiapan organisasi akuntansi dan regulator dalam mengadopsi standar keamanan baru menjadi krusial agar sistem informasi akuntansi tetap andal dan terpercaya di masa depan (Shadan & Islam, 2025).

Selama beberapa dekade terakhir, kriptografi konvensional seperti RSA (Rivest–Shamir–Adleman) dan ECC (Elliptic Curve Cryptography) telah menjadi standar utama dalam melindungi data digital, termasuk data akuntansi. Kedua algoritma ini berbasis pada permasalahan matematika kompleks, yakni faktorisasi bilangan prima besar (RSA) dan logaritma diskrit (ECC). Dengan komputer klasik, proses pemecahan kode enkripsi ini membutuhkan waktu yang sangat lama sehingga dianggap aman.

Komputasi kuantum menghadirkan tantangan besar bagi kriptografi konvensional, yang memiliki sejumlah kelemahan utama, di antaranya:

1. Kehilangan Keamanan terhadap Algoritma Kuantum

Algoritma kuantum seperti Shor's Algorithm dapat memecahkan masalah faktorisasi bilangan besar dan logaritma diskrit dalam waktu yang sangat singkat. Hal ini menyebabkan kunci enkripsi RSA dan ECC, yang sebelumnya membutuhkan waktu bertahun-tahun untuk dipecahkan, kini dapat dibongkar dalam hitungan jam atau bahkan menit menggunakan komputer kuantum.

2. Keterbatasan Penggunaan Panjang Kunci

Kriptografi konvensional sering menggunakan kunci panjang (misalnya 2048-bit atau 4096-bit) untuk meningkatkan keamanan. Namun, pendekatan ini menjadi tidak efektif dalam menghadapi kemampuan komputasi kuantum yang dapat memproses data secara eksponensial, sehingga tidak ada peningkatan yang signifikan dengan memperpanjang panjang kunci.

3. Risiko Kebocoran Data Sensitif

Sistem akuntansi yang bergantung pada RSA atau ECC memiliki potensi besar untuk kebocoran data, termasuk informasi transaksi, laporan keuangan, dan dokumen audit digital, yang dapat dengan mudah diakses oleh pihak yang tidak berwenang. Hal ini membuka peluang manipulasi laporan dan mengurangi transparansi serta kepercayaan pada perusahaan.

Ketidakmampuan Menyesuaikan dengan Perkembangan Teknologi

Kriptografi konvensional dikembangkan untuk melawan serangan dari komputer klasik, bukan komputer kuantum. Akibatnya, metode ini tidak cocok lagi untuk tantangan keamanan yang akan datang, mengingat kemajuan teknologi yang terus berkembang Berdasarkan hal tersebut, penelitian ini bertujuan untuk mengeksplorasi dampak komputasi kuantum terhadap keamanan sistem akuntansi melalui kajian literatur. Dengan menganalisis jurnal, *white paper*, dan standar internasional terkait, penelitian ini diharapkan dapat memberikan wawasan yang lebih dalam mengenai risiko yang ada serta strategi mitigasi yang dapat diterapkan untuk memperkuat keamanan sistem akuntansi di masa depan."

Metodologi

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kepustakaan *(library research)*. Data penelitian ini bersumber dari data sekunder yang diperoleh melalui jurnal internasional, artikel penelitian, buku teks, laporan standar internasional, serta whitepaper teknologi yang dipublikasikan oleh lembaga-lembaga resmi seperti National Institute of Standards and Technology (NIST) dan IEEE. Pengumpulan data dilakukan dengan menelaah, mengidentifikasi, serta mendokumentasikan hasil penelitian terdahulu mengenai topik yang berkaitan. Literatur yang dipilih difokuskan pada publikasi terbaru dalam rentang waktu 2020–2025 untuk memastikan relevansi dengan perkembangan komputasi kuantum dan kriptografi pasca-kuantum.

Hasil Kajian Literatur

1. Ancaman Komputasi Kuantum terhadap Kriptografi Konvensional

Sistem akuntansi digital saat ini sangat bergantung pada enkripsi untuk menjaga kerahasiaan, keaslian, dan integritas data. Algoritma RSA dan Elliptic Curve Cryptography (ECC) telah lama dianggap sebagai standar keamanan yang mumpuni karena tingkat kesulitannya dalam pemecahan bilangan prima besar dan logaritma diskrit menggunakan komputer klasik.

Namun, perkembangan komputasi kuantum menghadirkan tantangan baru. Dengan algoritma kuantum seperti *Shor's Algorithm*, masalah matematika yang sebelumnya membutuhkan waktu jutaan tahun untuk diselesaikan oleh komputer klasik dapat dipecahkan dalam waktu relatif singkat oleh komputer kuantum (Kurniawan et al., 2023).

Jika kondisi ini terwujud, maka berbagai risiko akan muncul, di antaranya:

1. Kebocoran data sensitif, misalnya informasi transaksi nasabah dan arsip keuangan.
2. Manipulasi laporan keuangan, yang berpotensi merusak transparansi perusahaan.
3. Akses ilegal ke sistem akuntansi, sehingga pihak luar dapat mengubah data tanpa jejak.
4. Hilangnya integritas audit, karena bukti digital dapat dipalsukan.

Dengan demikian, kriptografi klasik tidak lagi dapat dipandang sebagai solusi keamanan jangka panjang. Dunia akuntansi perlu memikirkan langkah alternatif untuk menjaga kepercayaan publik.

2. Post-Quantum Cryptography sebagai Solusi Mitigatif

Sebagai jawaban atas ancaman kuantum, lahirlah konsep Post-Quantum Cryptography (PQC), yaitu algoritma kriptografi yang dirancang agar tetap aman walaupun komputer kuantum berkembang pesat.

Tidak seperti RSA dan ECC yang bertumpu pada pemecahan faktorisasi bilangan besar, PQC menggunakan struktur matematika yang lebih kompleks, misalnya:

I. Lattice-based Crytography

Memanfaatkan kompleksitas perhitungan dalam ruang kisi, dengan contoh algoritma seperti NTRU dan Kyber.

II. Hash-based Crytography

Menggunakan kekuatan fungsi hash untuk menghasilkan tanda tangan digital yang aman terhadap serangan kuantum.

III. Code-based Crytography

Contohnya algoritma McEliece, yang menggunakan teori kode koreksi kesalahan untuk menjaga keamanan.

Dalam bidang akuntansi, PQC penting diterapkan karena dapat menjaga kerahasiaan data transaksi, laporan keuangan, dan catatan digital dari ancaman pencurian maupun pemalsuan data di era kuantum (Fernández-Caramés & Fraga-Lamas, 2024).

3. Integrasi Blockchain Kuantum dalam Sistem Akuntansi

Selain PQC, teknologi lain yang dipandang menjanjikan adalah blockchain kuantum. Blockchain tradisional sudah banyak dipakai untuk mencatat transaksi secara terdistribusi dan transparan, namun masih rawan terhadap ancaman kuantum karena sistem enkripsinya juga berbasis algoritma klasik.

Integrasi blockchain dengan Quantum Key Distribution (QKD) dapat menambah lapisan keamanan. QKD memungkinkan pertukaran kunci kriptografi dengan prinsip fisika kuantum, sehingga setiap upaya penyadapan akan langsung terdeteksi.

Dalam praktik akuntansi, blockchain kuantum dapat dimanfaatkan untuk:

1. Menjamin audit digital yang lebih aman dan akurat.
2. Menyediakan laporan keuangan yang transparan bagi pemegang saham dan regulator.
3. Memperkuat pelaporan real-time dengan dukungan *Distributed Ledger Technology (DLT)* (Shadan & Islam, 2025).

Hal ini menunjukkan bahwa blockchain kuantum bukan sekadar konsep teoritis, tetapi juga memiliki potensi nyata dalam mendukung keamanan sistem akuntansi di masa depan.

4. Peran Regulator dan Organisasi Akuntansi

Peningkatan keamanan sistem akuntansi tidak hanya menjadi tanggung jawab teknis perusahaan, melainkan juga menuntut peran aktif dari regulator dan organisasi profesi.

Sejak tahun 2017, NIST (National Institute of Standards and Technology) telah menjalankan program standarisasi kriptografi pasca-kuantum untuk memilih algoritma yang tahan terhadap komputer kuantum. Upaya serupa perlu diadopsi oleh regulator di Indonesia.

Peran organisasi seperti Ikatan Akuntan Indonesia (IAI) dan lembaga pengawas seperti Otoritas Jasa Keuangan (OJK) sangat krusial, antara lain dengan:

- Mendorong riset dan edukasi tentang PQC di bidang akuntansi.
- Menyusun kebijakan dan standar audit berbasis kriptografi pasca-kuantum.
- Membuat roadmap regulasi agar perusahaan publik mulai mengadopsi teknologi mitigatif secara bertahap (Lazirko, 2023).

Tanpa adanya regulasi dan standar yang jelas, implementasi PQC dan blockchain kuantum berisiko berjalan lambat, sehingga sistem akuntansi rentan ketika komputer kuantum sudah tersedia secara luas.

5. Implikasi Praktis bagi Sistem Akuntansi

Dari kajian literatur, terdapat beberapa pelajaran penting bagi dunia akuntansi:

1. Kriptografi klasik tidak lagi memadai. RSA dan ECC, yang selama ini jadi andalan, berpotensi usang di era kuantum.
2. Migrasi ke PQC mendesak dilakukan. Perusahaan harus mulai menguji coba algoritma pasca-kuantum untuk melindungi arsip digital.
3. Blockchain kuantum menjanjikan transparansi baru. Teknologi ini dapat meningkatkan kualitas audit dan mengurangi potensi manipulasi laporan keuangan.
4. Regulasi menjadi kunci keberhasilan transisi. Tanpa aturan dan kesiapan organisasi, adaptasi teknologi baru akan terhambat.

Diskusi

Kemajuan komputasi kuantum merupakan salah satu revolusi terbesar dalam dunia teknologi informasi. Berbeda dengan komputer klasik yang bekerja berdasarkan bit biner (0 atau 1), komputer kuantum menggunakan qubit yang dapat berada dalam keadaan superposisi, serta memiliki kemampuan entanglement yang memungkinkan pemrosesan data secara paralel dalam jumlah sangat besar. Keunggulan ini membuat komputer kuantum mampu menyelesaikan persoalan matematis kompleks, seperti faktorisasi bilangan prima dan logaritma diskrit, dalam waktu yang jauh lebih cepat dibandingkan komputer klasik.

Kemajuan komputasi kuantum membawa implikasi besar terhadap sistem akuntansi digital yang selama ini bergantung pada kriptografi konvensional. Dalam era kuantum, algoritma seperti Shor's Algorithm dapat merusak keamanan RSA dan ECC dalam waktu singkat. Oleh karena itu, penerapan PQC dalam sistem akuntansi sangat mendesak untuk melindungi data keuangan dan transaksi yang sangat sensitif. Selain itu, integrasi

blockchain kuantum dapat meningkatkan integritas dan transparansi sistem akuntansi. Saran untuk penelitian selanjutnya adalah untuk menguji implementasi PQC dalam lingkungan operasional akuntansi dan mengevaluasi dampaknya terhadap efektivitas dan efisiensi sistem keuangan.

Perkembangan ini menghadirkan peluang di berbagai bidang, namun sekaligus menimbulkan ancaman serius bagi keamanan informasi, khususnya pada sistem akuntansi digital yang semakin bergantung pada infrastruktur teknologi. Sistem akuntansi modern menyimpan dan mengolah data yang sangat sensitif, mulai dari transaksi keuangan harian, laporan keuangan tahunan, hingga catatan audit. Seluruh informasi tersebut selama ini dilindungi dengan kriptografi konvensional berbasis algoritma RSA atau Elliptic Curve Cryptography (ECC).

Sayangnya, algoritma kriptografi konvensional ini memiliki titik lemah yang dapat dieksploitasi oleh komputer kuantum. Dengan adanya Shor's Algorithm, komputer kuantum mampu memecahkan masalah faktorisasi dan logaritma diskrit secara eksponensial lebih cepat. Hal ini berarti bahwa kunci enkripsi RSA dan ECC yang dianggap aman dengan panjang ratusan hingga ribuan bit sekalipun, dapat dipecahkan dalam waktu singkat. Konsekuensinya, sistem akuntansi berisiko menghadapi berbagai ancaman: kebocoran data keuangan, manipulasi laporan, pencurian identitas digital, hingga hilangnya kepercayaan publik terhadap integritas informasi akuntansi.

Untuk mengantisipasi hal ini, berbagai penelitian merekomendasikan transisi ke Post-Quantum Cryptography (PQC). PQC mencakup algoritma yang dirancang khusus agar tetap aman meskipun diserang dengan kemampuan komputasi kuantum. Beberapa pendekatan utama yang banyak dibahas adalah:

1. Lattice-based cryptography – memanfaatkan kompleksitas perhitungan dalam ruang kisi (lattice) yang sulit dipecahkan bahkan oleh komputer kuantum. Contoh algoritma: NTRU, Kyber.
2. Hash-based cryptography – menggunakan kekuatan fungsi hash untuk membangun tanda tangan digital tahan-kuantum.
3. Code-based cryptography – seperti McEliece, yang mengandalkan teori kode koreksi kesalahan.
4. Multivariate polynomial cryptography – berbasis kesulitan dalam menyelesaikan sistem persamaan polinomial multivariat.

Dalam sistem akuntansi, adopsi PQC sangat penting untuk menjaga keamanan transaksi, validitas laporan keuangan, serta perlindungan data audit digital. Implementasi PQC tidak hanya memerlukan perubahan teknis, tetapi juga menuntut pelatihan, standar baru, dan integrasi dengan perangkat lunak akuntansi yang sudah ada.

Selain PQC, inovasi lain yang muncul adalah Quantum Blockchain. Blockchain tradisional memang sudah banyak digunakan untuk mendukung transparansi dan keamanan data akuntansi melalui buku besar terdistribusi (*distributed ledger*). Namun, blockchain klasik masih rentan terhadap serangan kuantum jika kunci enkripsinya dilemahkan. Oleh karena itu, integrasi blockchain dengan Quantum Key Distribution

(QKD) menjadi solusi baru. Dengan QKD, distribusi kunci enkripsi dilakukan melalui prinsip mekanika kuantum, sehingga setiap upaya penyadapan dapat terdeteksi.
Dalam konteks akuntansi, Quantum Blockchain dapat memberikan manfaat strategis, seperti:

- Menjamin integritas audit digital dengan catatan transaksi yang tidak dapat dimanipulasi.
- Meningkatkan transparansi laporan keuangan perusahaan publik.
- Memfasilitasi pelaporan keuangan real-time yang aman berbasis Distributed Ledger Technology (DLT).

Namun, diskusi literatur menekankan bahwa teknologi saja tidak cukup. Peran regulator dan organisasi akuntansi sangat krusial dalam mendorong kesiapan menghadapi ancaman kuantum. Misalnya, National Institute of Standards and Technology (NIST) telah meluncurkan program Post-Quantum Cryptography Standardization sejak 2017, dan pada tahun 2022 sudah memilih kandidat algoritma standar untuk masa depan. Hal ini dapat menjadi acuan bagi regulator di Indonesia, seperti Otoritas Jasa Keuangan (OJK) dan Ikatan Akuntan Indonesia (IAI), untuk merumuskan kebijakan transisi menuju standar keamanan baru.

Kesiapan regulasi akan menentukan kecepatan adopsi teknologi mitigatif. Beberapa langkah yang dapat dilakukan adalah:

- Menetapkan roadmap adopsi PQC di perusahaan publik dan lembaga keuangan.
- Memberikan insentif penelitian terkait keamanan kuantum di bidang akuntansi.
- Mengintegrasikan kurikulum keamanan kuantum dalam pendidikan akuntansi dan auditing.
- Mendorong kolaborasi antara praktisi akuntansi, pakar teknologi, dan regulator.

Dengan demikian, implikasi praktis dari kajian literatur ini dapat dirangkum sebagai berikut:

1. Kriptografi klasik tidak lagi memadai untuk menjamin keamanan sistem akuntansi di era kuantum.
2. Adopsi Post-Quantum Cryptography menjadi kebutuhan mendesak untuk melindungi data akuntansi.
3. Integrasi Quantum Blockchain dapat memperkuat transparansi dan akuntabilitas audit.
4. Peran regulator dan organisasi akuntansi menjadi kunci untuk memastikan transisi yang aman dan terstandar.

Secara keseluruhan, ancaman komputasi kuantum bukan lagi isu yang bersifat teoritis, melainkan realitas yang harus segera diantisipasi. Dunia akuntansi perlu menyiapkan diri dengan kombinasi teknologi mitigatif dan kebijakan kelembagaan agar tetap relevan dan terpercaya di era kuantum.

Simpulan

Perkembangan komputasi kuantum membawa implikasi signifikan bagi dunia akuntansi modern, khususnya dalam aspek keamanan informasi. Dengan kemampuan memecahkan persoalan matematis kompleks secara eksponensial lebih cepat dibandingkan komputer klasik, komputer kuantum mengancam keberlangsungan kriptografi konvensional seperti RSA dan ECC yang selama ini menjadi fondasi keamanan sistem akuntansi digital. Ancaman ini dapat berujung pada kebocoran data, manipulasi laporan keuangan, hingga hilangnya kepercayaan terhadap integritas sistem akuntansi. Sebagai solusi mitigatif, penerapan Post-Quantum Cryptography (PQC) menjadi kebutuhan mendesak. Algoritma berbasis lattice, hash, maupun code-based terbukti lebih tahan terhadap serangan kuantum dan dapat diimplementasikan untuk menjaga keamanan transaksi, arsip keuangan, serta proses audit digital. Selain itu, Quantum Blockchain dengan dukungan Quantum Key Distribution (QKD) dapat meningkatkan transparansi, akuntabilitas, dan integritas laporan keuangan melalui mekanisme buku besar terdistribusi yang lebih aman.

Namun, kesiapan teknologi saja tidak cukup. Regulator dan organisasi akuntansi perlu mengambil peran strategis dalam menetapkan standar, regulasi, serta roadmap transisi menuju keamanan pasca-kuantum. Tanpa dukungan regulasi yang kuat, adopsi teknologi mitigatif dikhawatirkan berjalan lambat sehingga sistem akuntansi semakin rentan terhadap risiko kuantum.

Perkembangan komputasi kuantum membawa ancaman serius terhadap keberlangsungan kriptografi konvensional dalam sistem akuntansi. Oleh karena itu, penerapan Post-Quantum Cryptography (PQC) sangat penting untuk menjaga keamanan data akuntansi di era kuantum. Selain itu, teknologi blockchain kuantum dengan Quantum Key Distribution dapat meningkatkan transparansi dan keamanan sistem akuntansi. Regulator dan organisasi akuntansi harus segera mempersiapkan regulasi dan kebijakan untuk mendukung transisi menuju sistem yang lebih aman ini.

Daftar Pustaka

Chen, D., & Qian, H. (2022). *Post-Quantum Security Challenges in Cloud-Based Accounting. IEEE Transactions on Information Forensics and Security*, 17(8), 5431–5442.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2024). A review on post-quantum cryptography for secure Industry 4.0: Algorithms, applications, and challenges. *Journal of Information Security and Applications, 76*, 103641. https://doi.org/10.1016/j.jisa.2023.103641

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2024). A Review on the Application of Post-Quantum Cryptography to IoT and Blockchain. *Future Internet, 16*(2), 52. https://doi.org/10.3390/fi16020052

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2024). *Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks*. arXiv preprint arXiv:2402.00922.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2024). *Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks.*

Kim, S., & Park, T. (2023). *Quantum Key Distribution in Accounting Information Systems. Journal of Emerging Financial Technologies*, 5(1), 12–28.

Kurniawan, A., Pratama, Y., & Sari, M. (2023). Tantangan Komputasi Kuantum terhadap Kriptografi Klasik dalam Sistem Informasi Akuntansi. *Jurnal Teknologi Informasi dan Akuntansi, 5*(2), 101–115.

Kurniawan, A., Pratama, Y., & Sari, M. (2023). *Tantangan Komputasi Kuantum terhadap Kriptografi Klasik dalam Sistem Informasi Akuntansi.* Jurnal Teknologi Informasi dan Akuntansi, 5(2), 101–115.

Kurniawan, A., Sari, N. P., & Pratama, R. (2023). Quantum computing and its threats to classical cryptography: A systematic literature review. *Jurnal Teknologi dan Sistem Informasi, 9*(2), 87–96. https://doi.org/10.25077/teknosi.v9i2.2023

Kurniawan, D., Triyanto, D., Wahyudi, M., & Pujiastuti, L. (2023). *Quantum Computing in Cryptography: Exploring Vulnerabilities and Countermeasures*. Jurnal Teknik Informatika C.I.T Medicom, 15(4), 87–95.

Kurniawan, D., Triyanto, D., Wahyudi, M., & Pujiastuti, L. (2023*). Quantum Computing in Cryptography: Exploring Vulnerabilities and Countermeasures*. Jurnal Teknik Informatika C.I.T Medicom, 15(4), 87–95.

Lazirko, D. (2023). Post-Quantum Cryptography Standardization and Its Implications for Information Systems Security. *Journal of Cybersecurity Policy, 8*(1), 33–49.

Lazirko, M. (2023). Preparing for the post-quantum era: The role of regulators in adopting secure cryptographic standards. *Journal of Accounting and Information Systems, 19*(3), 145–158. https://doi.org/10.1080/1834765X.2023.001

Lazirko, M. (2023). *Quantum Computing Standards & Accounting Information Systems*. arXiv preprint arXiv:2311.11925.

Li, Y., & Han, J. (2024). *Quantum Blockchain for Financial Auditing and Transparency*. Future Finance Journal, 8(1), 22–39.

Liu, X., & Wang, Z. (2024). *Quantum Encryption for Accounting Systems: Challenges and Opportunities*. Journal of Accounting Technology Research, 12(1), 45–58.

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

National Institute of Standards and Technology (NIST). (2022). *Post-Quantum Cryptography Standardization: Status Report on Round 3 Submissions*. Gaithersburg, MD: U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8413'

Nielsen, M. A., & Chuang, I. L. (2020). *Quantum Computation and Quantum Information* (10th Anniversary Edition). Cambridge: Cambridge University Press.

Nugroho, D., & Lestari, I. (2024). *Mitigasi Risiko Kuantum pada Sistem Audit Digital. Jurnal Sistem Informasi Akuntansi Indonesia*, 3(1), 33–47.

Ong, C. L., & Tan, Y. (2023). *Quantum-Safe Standards in Financial Data Management. Asia-Pacific Journal of Accounting Technology*, 14(1), 67–82.

Rahman, F., & Sari, E. (2023). *Implementasi Kriptografi Pasca-Kuantum dalam Sistem Akuntansi Digital. Jurnal Akuntansi dan Teknologi Informasi*, 7(2), 210–225.

Rahman, M., & Aisyah, F. (2023). *Kebijakan Regulasi terhadap Teknologi Komputasi Kuantum di Sektor Akuntansi*. Jurnal Kebijakan Akuntansi Indonesia, 4(2), 55–70.

Romney, M. B., & Steinbart, P. J. (2022). *Accounting Information Systems* (15th ed.). Pearson.

Shadan, H. H., & Islam, S. (2025). *Quantum Computing and Cybersecurity in Accounting and Finance: Current and the Future Challenges and Opportunities for Securing Accounting and Finance Systems*.

Shadan, M., & Islam, M. S. (2025). Quantum blockchain: A new frontier for financial security and distributed accounting systems. *International Journal of Blockchain and Quantum Security, 4*(1), 25–41. https://doi.org/10.1145/iqbs.2025.004

Shadan, S., & Islam, M. S. (2025). Quantum Blockchain: A New Frontier for Financial Security and Distributed Accounting Systems. *International Journal of Blockchain and Quantum Security, 4*(1), 25–41.

Sun, P., & Kim, J. (2024). *Quantum-Safe Frameworks for Accounting Data Integrity. International Journal of Accounting Information Systems*, 24(3), 155–170.

Wibowo, R., & Hartono, D. (2024). *Evaluasi Penerapan PQC dalam Sistem Akuntansi Publik. Jurnal Akuntansi dan Keamanan Siber*, 6(2), 115–132.

Zhang, J., & Chen, W. (2022). Integrating Blockchain and PQC for Secure Financial Auditing. Journal of Finance & Information Technology, 10(2), 77–89.

Zhou, L., & Li, C. (2023). *Evaluating Post-Quantum Cryptographic Readiness in Financial Reporting Systems. Information Systems Frontiers*, 25(4), 993–1007.