

Indonesia's Digital Insights into Quantum Security Technology

Rudy Agus Gemilang Gultom^{1*}, Joko Waluyo Saputro², Heribertus Aprodito Danang Rimbawa³, Nur Aima Shafie⁴, Siti Nur Atika Shahari⁵

¹Nurtanio University Bandung, Indonesia

²ASEAN HPC Task Force, Co-Chair, & Republic of Indonesia Defense University, Indonesia

³Republic of Indonesia Defense University, Indonesia,

⁴Accounting Research Institute, Universiti Teknologi MARA, Malaysia,

⁵Faculty of Information Science, Universiti Teknologi MARA, Malaysia

*Corresponding Author

DOI: <https://dx.doi.org/10.47772/IJRISS.2025.909000815>

Received: 28 September 2025; Accepted: 04 October 2025; Published: 31 October 2025

ABSTRACT

Quantum computing promises transformative advances in optimisation, data-intensive research, and scientific discovery, yet it simultaneously threatens the foundations of classical cryptography that protect global digital infrastructures. This conceptual study examines Indonesia's readiness for quantum security by analysing literature, global best practices, and policy frameworks. The study highlights the urgency of transitioning to post-quantum cryptography (PQC), adopting quantum key distribution (QKD), and strengthening national governance capacities to mitigate risks such as the "store now, decrypt later" threat. Findings reveal that Indonesia's growing digital dependence in government services, e-commerce, and financial technology magnifies exposure to future quantum breaches. National readiness requires integrated policies, capacity building, and regional cooperation to align with emerging international standards. Quantum security is shown not merely as a defensive response but as a strategic enabler of resilience, innovation, and competitiveness. Early action will position Indonesia to safeguard its digital sovereignty and contribute to global quantum-safe ecosystems.

Keywords: Quantum Computing, Quantum Security, Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), Quantum Computing Threat, Cryptography and Cybersecurity

INTRODUCTION

In recent years, quantum computing technology has been rapidly advancing in the global technological landscape and has increasingly become one of the most discussed topics in the technology industry. This is primarily because quantum computing promises the ability to solve problems that are far more complex, larger in scale, and beyond the reach of current conventional computers. The impact of such technology is expected to be transformative, not only in computing itself but also across a wide range of domains including cybersecurity, medicine, finance, and national security. The rapid acceleration of research and investment in this field by leading technology companies, research institutes, and governments worldwide signals its potential as one of the defining technologies of the twenty-first century.

In conventional computing, the bit is the smallest unit of information used in data processing. A bit can only represent one of two states, namely 0 or 1. These binary states serve as the foundation of all digital computation in modern-day systems. In contrast, quantum computing introduces a fundamentally different paradigm. At its core lies the qubit (quantum bit), a unit of information that can exist not only as 0 or 1 but also in a superposition of both states simultaneously. This unique characteristic is rooted in the principles of quantum mechanics,

particularly the phenomena of superposition and entanglement. Through superposition, qubits can represent and process multiple possibilities at once, while entanglement allows qubits that are correlated to maintain interconnected states even when physically separated. By harnessing these properties, quantum computers have the potential to perform certain types of calculations exponentially faster and more efficiently than conventional systems. (see Fig.1)

Over the past decade, quantum computing has demonstrated immense promise in addressing highly complex and large-scale problems. Early research and prototypes developed by companies such as IBM, Google, and D-Wave, along with initiatives from government agencies and academic institutions, have showcased preliminary evidence of quantum advantage in selected areas. For example, optimization problems that involve identifying the most efficient solution from an exponentially large set of possibilities can be tackled much faster with quantum algorithms. Similarly, simulations of molecular interactions in drug discovery, which are computationally infeasible for classical supercomputers, can potentially be accelerated through quantum computational models. These advances suggest that industries, governments, and societies need to prepare for a technological paradigm shift that could disrupt traditional practices.

Potential Benefits of Quantum Computing

There are several benefits that can be obtained from the adoption and application of quantum computing, many of which extend into critical sectors of the economy and national security. Quantum computing offers transformative advantages for optimisation, data analysis, and cybersecurity. It excels at solving complex optimisation problems such as improving supply chain routes, reducing energy use in smart grids, and maximising investment returns far faster than classical computers.

Its power in data processing can accelerate pattern recognition, machine learning, and big data analytics. In healthcare, it could revolutionise drug discovery and enhance diagnostic imaging. In climate science, quantum simulations promise better modelling of weather patterns and climate change.

However, quantum computing also poses significant cybersecurity risks. Quantum algorithms like Shor's and Grover's could break widely used cryptographic systems, threatening the foundations of modern digital security and necessitating new post-quantum encryption standards.

As quantum computers continue to advance, it is increasingly evident that they will eventually gain the capacity to break the security protocols that underpin most digital communication, financial transactions, and data storage systems in the world today. The projected timeline for achieving such "cryptographically relevant quantum computers" (CRQCs) varies among experts, with estimates ranging from the next 10 to 30 years. Nonetheless, the uncertainty itself underscores the urgency of proactive preparation. Waiting until such capabilities are realized would expose critical infrastructures, governments, and societies to catastrophic risks, including massive data breaches, compromised national security, and erosion of public trust in digital systems.

Recognizing these risks, researchers and policymakers have begun to focus on post-quantum cryptography (PQC) and quantum security technologies. PQC involves developing cryptographic algorithms that are resistant to quantum attacks, ensuring that data and communications remain secure even in the presence of powerful quantum adversaries. The U.S. National Institute of Standards and Technology (NIST), for example, has initiated a multi-year standardization process to identify and adopt quantum-resistant algorithms. Similarly, international collaborations and regional efforts are underway to prepare digital ecosystems for the quantum era.

For Indonesia, a rapidly digitizing nation with growing reliance on digital platforms, e-commerce, financial technology, and e-governance, the challenges and opportunities of quantum computing are particularly significant. The protection of sensitive national data, critical infrastructures such as energy and transportation, and the privacy of citizens depends on robust cybersecurity measures. Without early preparation, Indonesia risks being vulnerable to future quantum threats that could undermine its digital sovereignty and economic stability.

To address this, it is essential for Indonesia to leverage expertise across multiple domains, including cryptography, quantum computing, and infrastructure resilience. A collaborative approach involving government

institutions, academic research, industry stakeholders, and international partners is necessary to ensure readiness. The development of a national quantum security strategy would allow Indonesia not only to defend against future threats but also to position itself as a proactive player in the global quantum security landscape.

Quantum security technology encompasses a wide range of strategies and solutions aimed at mitigating the risks posed by quantum computing. These include the adoption of post-quantum cryptographic algorithms, the exploration of quantum key distribution (QKD) for secure communications, and the integration of quantum-resistant protocols into existing digital infrastructures. While technical solutions are central, non-technical aspects such as regulatory frameworks, capacity building, and public awareness are equally crucial.

In this regard, Indonesia's journey toward quantum readiness should not be viewed solely as a defensive measure but also as an opportunity. By investing in research, fostering talent, and engaging in international collaborations, Indonesia can contribute to the development of innovative solutions and strengthen its role in the global digital economy. This proactive stance can enhance national resilience, protect sovereignty, and build trust among citizens and international partners alike.

In summary, quantum computing is no longer a distant theoretical concept but a rapidly emerging technology with profound implications for the future. Its benefits in optimization, data processing, and scientific discovery are balanced by its disruptive potential in cryptography and cybersecurity. For nations like Indonesia, recognizing both sides of this technological transformation is crucial. Preparing for the quantum era requires not only technological adoption but also strategic foresight, policy innovation, and multi-stakeholder collaboration. By implementing and developing quantum security technologies today, Indonesia can secure its digital future and establish itself as a resilient and forward-looking digital nation.

The aim of this paper is to conceptually examine Indonesia's readiness for quantum security by identifying the vulnerabilities of existing cryptographic systems, assessing the urgency for adopting post-quantum cryptography and quantum key distribution, and exploring governance and policy measures that integrate technical innovation with institutional preparedness, with the objective of highlighting that a proactive, multidimensional approach combining technological adoption, national policy coordination, capacity building, and international cooperation is essential for Indonesia to mitigate the disruptive risks of quantum computing while leveraging its transformative potential as a strategic enabler of resilience, digital sovereignty, and global competitiveness.

Problem Statement

Quantum computing is emerging as one of the most disruptive technologies of the twenty-first century. While it promises transformative breakthroughs in optimization, artificial intelligence, and scientific discovery, it also poses serious risks to digital security. Existing cryptographic systems such as RSA and elliptic curve cryptography rely on mathematical problems that are difficult for classical computers to solve. However, with the development of quantum algorithms such as Shor's and Grover's, these systems are at risk of being broken within seconds once large-scale quantum computers become practical. This creates a looming threat to the confidentiality, integrity, and authenticity of sensitive data worldwide.

For Indonesia, the challenge is particularly urgent. As the nation advances its digital transformation in government services, e-commerce, financial technology, and critical infrastructure, the reliance on vulnerable encryption methods could lead to catastrophic consequences. A lack of preparedness would expose the country to risks including data breaches, compromised national security, and erosion of public trust in digital systems. While global efforts to standardize post-quantum cryptography and explore quantum key distribution are underway, Indonesia has yet to establish a comprehensive strategy that integrates government policy, industry readiness, academic research, and international collaboration.

The uncertainty surrounding national awareness, the slow pace of adoption of quantum-resistant solutions, and the varying levels of digital infrastructure maturity across sectors further complicate Indonesia's readiness. Without urgent intervention, adversaries could exploit the "store now, decrypt later" approach, where sensitive data collected today could be decrypted once quantum computers mature. This scenario highlights the need for

systematic research that empirically examines the factors shaping Indonesia's preparedness for quantum security. Such an investigation is essential for guiding the development of policies and frameworks that can protect digital sovereignty, ensure resilience, and position Indonesia as a proactive participant in global quantum security.

LITERATURE REVIEW

Quantum computing is an emerging field that leverages the principles of quantum mechanics to perform computations in ways fundamentally different from classical computing. Unlike classical bits that exist in a state of 0 or 1, quantum bits or qubits can exist in a superposition of both states simultaneously. This unique property enables quantum computers to explore multiple possibilities at once, potentially solving certain problems exponentially faster than classical computers.

An exploration of quantum computing concepts and the associated threats will set the stage for appreciating the necessity of quantum security. In fact, Quantum computing is an emerging field that leverages the principles of quantum mechanics to perform computations in ways fundamentally different from classical computing. Unlike classical bits that exist in a state of 0 or 1, quantum bits or qubits can exist in a superposition of both states simultaneously. This unique property enables quantum computers to explore multiple possibilities at once, potentially solving certain problems exponentially faster than classical computers.

One of the key concepts in quantum computing is entanglement, where qubits become correlated in such a way that the state of one qubit is directly related to the state of another, regardless of the physical distance between them. This entanglement property allows quantum computers to perform complex computations more efficiently than classical computers for specific tasks. The potential applications of quantum computing are vast and varied. Quantum computers have the potential to revolutionize fields such as cryptography, optimization, drug discovery, and artificial intelligence. For instance, they could break widely-used encryption algorithms, threatening the security of sensitive data.

On the flip side, they could also help design more secure encryption methods, creating a dual-edge sword in the realm of cybersecurity. Despite their immense potential, quantum computers are still in their infancy, facing challenges related to error correction, stability, and scalability. As researchers work towards overcoming these hurdles, the world is waking up to both the promises and threats posed by quantum computing. Quantum computing poses a significant threat to classical cryptographic systems that currently safeguard our digital communication and transactions. The most notable risk comes from Shor's algorithm, a quantum algorithm that can efficiently factor large numbers, breaking widely-used public-key cryptosystems such as RSA. Once a practical quantum computer is developed, it could compromise the security of confidential information, financial transactions, and even the integrity of digital signatures.

Post-quantum cryptography is an active area of research aimed at developing cryptographic algorithms that are secure against quantum attacks. Transitioning to these new cryptographic standards is essential to maintaining the confidentiality and integrity of information in the quantum era. The urgency to develop and adopt post-quantum cryptography is underscored by the looming threat of quantum computers rendering existing cryptographic systems obsolete. The realization of quantum computing's potential and the concurrent threats to classical cryptography emphasize the urgent need for quantum security measures. Quantum key distribution (QKD) is a promising solution that leverages the principles of quantum mechanics to secure communication channels against quantum attacks. QKD uses the quantum properties of particles to enable secure key exchange, making it theoretically immune to eavesdropping attempts by quantum computers.

As quantum technologies advance, the integration of quantum-resistant cryptographic algorithms and the implementation of quantum-safe communication protocols become imperative. Governments, industries, and researchers must collaborate to develop and standardize quantum-resistant cryptographic solutions, ensuring the long-term security of sensitive information in the face of the quantum threat. The concepts of quantum computing bring both unparalleled opportunities and unprecedented threats. Understanding the potential applications, grappling with the challenges, and actively pursuing quantum-safe security measures are essential steps in preparing for the quantum era. As quantum technologies continue to evolve, a proactive approach to quantum security will be crucial in safeguarding the integrity and confidentiality of our digital world.

Importance of Quantum Security

As the world advances into the quantum era, the need for stronger, future-proof digital security is more urgent than ever. Quantum computers, once fully realized, will possess the power to solve complex mathematical problems far faster than classical computers. While this brings significant potential in science and technology, it also poses a serious threat to current encryption systems that protect sensitive data worldwide. Today's widely-used cryptographic algorithms, such as RSA and ECC, rely on the computational difficulty of specific problems, like factoring large numbers. These methods have kept digital communications safe for decades. However, quantum algorithms, such as Shor's algorithm, could easily break these codes, rendering current systems obsolete almost overnight.

This threat affects national defense systems, banking infrastructure, medical records, intellectual property, and personal communications. Even more concerning is the strategy known as "store now, decrypt later," where attackers collect encrypted data today to decrypt it in the future with quantum technology. To address this challenge, researchers and cybersecurity experts are developing quantum-resistant algorithms under the umbrella of post-quantum cryptography (PQC), as well as leveraging quantum key distribution (QKD) to create unbreakable encryption based on the laws of quantum mechanics. Quantum security is not merely a technical upgrade, it is a foundational step toward maintaining global trust in digital systems. Governments, industries, and academia must act together to transition to quantum-safe infrastructure before the threat becomes a reality. Quantum computing is coming. The time to secure our future is now.

Security solution with quantum encryption

In this digital era, quantum technology and the cyber domain have a very close relationship, as can be seen in the following picture (see Fig. 3). Cybersecurity has become very important to protect information and communications from threats and attacks. However, technological advances also bring new challenges, especially with the emergence of quantum computers capable of breaking the classical encryption used today. Therefore, new approaches are needed that utilize quantum properties to improve cyber security. One approach used is quantum computing, which uses qubits as units of information. Qubits can be in two states at once, so they can perform calculations more quickly and efficiently than classical bits. Quantum computing can be used for cryptanalysis, which allows breaking public encryption and authenticating messages.

Quantum computing can also be used to improve cyber operations through artificial intelligence and machine learning, which can automate tasks such as software, gaming and threat detection. Another approach is post-quantum cryptography, which uses new classical algorithms based on problems that are difficult enough even for quantum computers. Post-quantum cryptography provides opportunities for new approaches, such as position-based cryptography, which allows verifying a person's location without revealing their identity. Post-quantum cryptography could also reduce reliance on trust authorities, such as digital certificates, which can be hacked or forged.

A third approach is quantum communication, which uses photons as information carriers. Photons have unique quantum properties, such as overlap and entanglement, that can be used to transmit information in a secure and confidential manner. Quantum communication includes quantum key distribution, which allows two parties to share a secret key that cannot be intercepted or forged. Quantum communications also include quantum digital signatures, which allow senders to sign messages in a way that cannot be forged or refuted.

The fourth approach is Quantum RNG, which stands for Quantum Random Number Generator. Quantum RNG is a device that generates true random numbers, which differ from the pseudo-random numbers generated by classical algorithms. True random numbers are essential for strong cryptography, because they can be used as a key, salt, or nonce. Quantum RNG can also be used for certification and verification, such as random selection, auditing, or voting. Some of these quantum technology approaches can provide benefits and solutions for the cyber world, which is increasingly complex and dynamic. Quantum technology can increase speed, efficiency and cybersecurity, and open up new opportunities for innovation and collaboration.

Analyzing Limitations of Existing Security Systems

Existing security systems, such as RSA, ECC, and AES, have formed the backbone of digital protection for decades. These cryptographic methods rely heavily on mathematical problems that are difficult to solve with classical computers. However, as technology evolves, so do the limitations of these systems. One of the most critical threats comes from the advent of quantum computing. Algorithms like Shor's and Grover's have the potential to break widely-used encryption methods, rendering today's secure systems highly vulnerable. Even before quantum threats fully materialize, current systems face challenges such as poor key management, vulnerabilities in software implementation, social engineering attacks, and limited resilience to large-scale distributed denial-of-service (DDoS) attacks.

Moreover, traditional security architectures were not designed with today's decentralized, cloud-based, and highly mobile environments in mind. As a result, legacy systems often struggle to maintain data confidentiality, integrity, and availability across complex infrastructures. In addition, the increasing reliance on Internet of Things (IoT) devices, many of which lack robust security protocols, creates new attack surfaces. These limitations highlight the urgent need for security models that are adaptable, scalable, and resistant to future threats, especially quantum threats. To maintain digital trust, security systems must be reimagined for the future.

Threats of Quantum Attacks

Quantum computing holds the promise of revolutionizing fields such as medicine, logistics, and material science. However, alongside these opportunities lies a major cybersecurity concern: quantum attacks. These refer to the ability of quantum computers to break cryptographic systems that currently protect digital communications, financial transactions, and national infrastructure. The most significant threat stems from Shor's algorithm, which allows quantum computers to efficiently factor large integers, the very foundation of RSA and ECC encryption. Once quantum computers become sufficiently powerful, they can decrypt encrypted data in seconds, rendering widely-used security systems obsolete. This poses an existential threat to the confidentiality of everything from bank accounts to classified government communications.

Even more concerning is the "harvest now, decrypt later" tactic, where adversaries intercept and store encrypted data today with the intent to decrypt it once quantum capabilities mature. This endangers long-term sensitive data such as medical records, diplomatic archives, and intellectual property. Other areas at risk include blockchain systems, secure messaging platforms, and cloud infrastructures. Without proactive defenses, quantum attacks could trigger global-scale disruptions in trust, finance, and digital governance. To mitigate these threats, organizations must transition to quantum-safe cryptography, including post-quantum algorithms and quantum key distribution (QKD). Global cooperation among governments, academia, and industry is essential to accelerate research, develop standards, and deploy resilient solutions. The quantum threat is not a distant problem. It is a growing reality that demands immediate attention, investment, and innovation. Failure to prepare now could result in irreversible consequences in the near future.

Delving into the principles and advantages of quantum communication will elucidate its role in securing sensitive information. Quantum communication is a cutting-edge field that exploits the principles of quantum mechanics to enable secure and efficient information exchange. Unlike classical communication, which relies on classical bits, quantum communication utilizes quantum bits or qubits, offering unique properties such as superposition, entanglement, and uncertainty.

The underlying principle is to leverage these quantum phenomena to achieve secure transmission of information, presenting a paradigm shift in the realm of secure communication. At the core of quantum communication are the principles of superposition and entanglement. Superposition allows qubits to exist in multiple states simultaneously, enabling the encoding of more information than classical bits. This property enhances the data-carrying capacity of quantum communication systems, paving the way for more efficient and information-dense communication channels.

Entanglement-based Quantum Key Distribution (QKD) is a secure communication protocol that leverages the quantum phenomenon of entanglement. It is a unique quantum correlation between particles where the state of

one particle is dependent on the state of its entangled partner, regardless of the distance between them. This phenomenon is harnessed in quantum communication to establish secure connections. Attempts to intercept or measure entangled particles inevitably disturb their states, providing a means to detect eavesdropping and ensuring the security of quantum communication.

In this method, a pair of entangled photons is generated and distributed to two parties, typically called Alice and Bob. Due to entanglement, measurements on one photon instantaneously determine the state of its pair, regardless of the distance. This correlation allows Alice and Bob to generate a shared cryptographic key. If an eavesdropper (Eve) tries to intercept or measure the photons, the entanglement is disturbed, revealing the intrusion. This makes entanglement-based QKD highly secure and a promising solution for future-proof encryption systems (see Fig. 1).

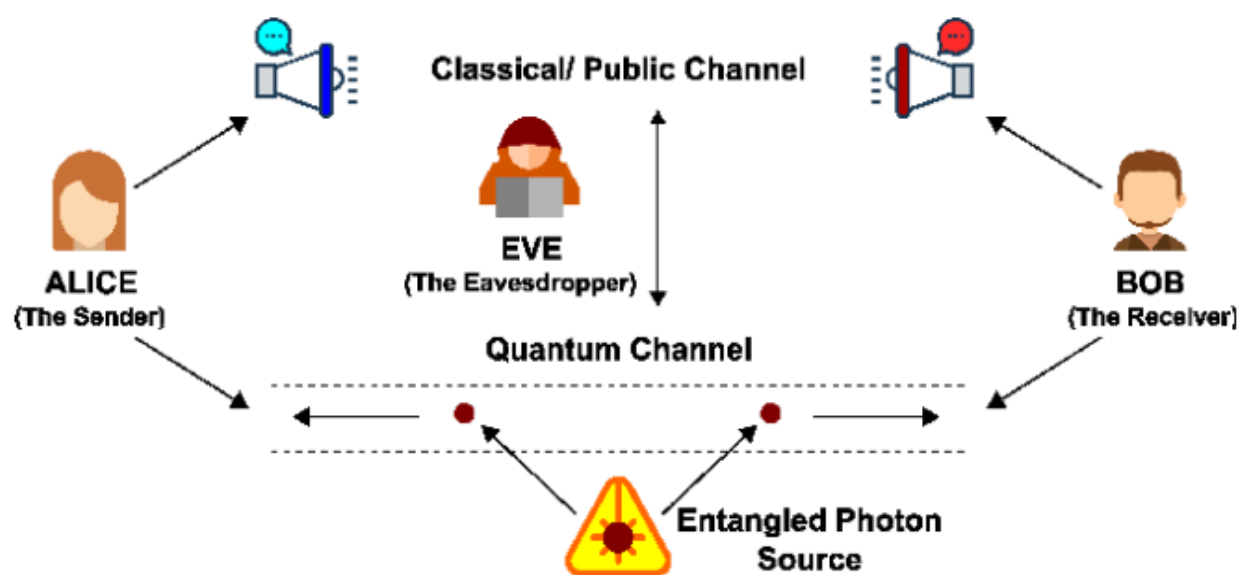


Figure 1. Basic Concept of Entanglement-Based QKD Protocol (source: <https://www.semanticscholar.org/paper/Quantum-Key-Distribution-%28QKD%29-Protocols%3A-A-Survey-Nurhadi-Syambas/858b2ca1a277ca343d3ca5ddeb9e7a60a622c4a7/figure/10>)

A cornerstone of quantum communication is QKD, a revolutionary cryptographic protocol that uses quantum principles to exchange secure keys between parties. QKD employs the transmission of quantum particles, typically photons, to create a shared secret key. The security of QKD lies in the fundamental principles of quantum mechanics: any attempt to intercept the quantum particles would disturb their states, alerting the legitimate parties to a potential security breach. QKD addresses a critical vulnerability in classical cryptographic systems, where the security relies on the difficulty of certain mathematical problems.

Quantum computers, with their potential to efficiently solve these problems, pose a threat to classical encryption. QKD provides a quantum-safe solution, ensuring the security of key exchange even in the face of quantum computational power. Quantum communication offers several advantages over classical communication, primarily centered around enhanced security and efficiency. One of the key advantages is the unconditional security provided by the quantum properties of superposition and entanglement. The ability to detect any attempt at eavesdropping ensures that quantum communication systems are inherently secure, providing a level of protection that classical systems cannot match.

Another advantage lies in the potential for quantum communication networks to establish ultra-secure channels for information exchange. Quantum key distribution and entanglement-based communication systems could pave the way for secure communication over long distances without compromising the confidentiality of the transmitted information. The development of quantum repeaters further enhances the advantages of quantum communication. Quantum repeaters leverage entanglement to extend the range of quantum communication, overcoming challenges associated with signal loss over long distances.

This opens the door to the creation of global quantum communication networks, enabling secure communication on a global scale. Looking ahead, the future of quantum communication holds promise for a range of applications beyond secure key exchange. Quantum communication networks could revolutionize secure data transmission in fields such as finance, healthcare, and government.

Additionally, quantum communication protocols may play a crucial role in the development of quantum internet, providing secure and efficient communication between quantum computers and other quantum devices. However, challenges remain on the path to widespread adoption of quantum communication. Overcoming issues related to noise, interference, and maintaining quantum coherence over long distances are key research areas.

Standardization of protocols and the development of practical quantum technologies are essential for the integration of quantum communication into existing communication infrastructure. The principles and advantages of quantum communication mark a transformative era in secure information exchange. By leveraging the unique properties of quantum mechanics, quantum communication systems offer unparalleled security and efficiency, positioning them as a crucial component in the evolving landscape of secure communication.

As research and development progress, the realization of practical quantum communication applications holds the promise of reshaping the way we transmit and secure information in the digital age.

RESEARCH METHODOLOGY

This study adopts a conceptual and exploratory qualitative approach designed to capture the multidimensional challenges and opportunities associated with Indonesia's readiness for quantum security. The methodology integrates a policy-oriented desk review, thematic synthesis of literature, and policy-focused analysis to address the dual realities of quantum computing as both a transformative enabler and a disruptive threat.

The research is primarily conceptual, drawing insights from published academic articles, technical reports, and policy documents. The design emphasises synthesising theoretical insights on quantum computing, cryptographic vulnerabilities, and post-quantum solutions, as well as analysing international best practices and their applicability to Indonesia's national context. The study also frames a forward-looking conceptual discussion to guide national policy and strategic preparedness for the quantum era.

The study relies exclusively on secondary data gathered from reputable academic journals, technical reports, and institutional policy documents. Key sources include guidelines and reports from international organisations such as the National Institute of Standards and Technology (NIST), the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), and the International Organization for Standardization (ISO), along with ASEAN initiatives and Indonesia's own national cybersecurity strategies. Case studies from early-adopter countries such as the United States, Germany, Japan, and Singapore are also examined to highlight transferable lessons relevant to Indonesia's national priorities.

A desk-based literature review was undertaken to compile evidence on the emerging risks posed by quantum computing to classical cryptographic systems and to examine progress in the development of post-quantum cryptographic (PQC) algorithms, quantum key distribution (QKD), and quantum communication networks. The review further explored governance and institutional frameworks for implementing quantum-safe infrastructures in both developed and developing countries and identified gaps and opportunities within Indonesia's cybersecurity ecosystem, particularly in relation to public sector readiness, research capacity, and industry participation.

The study employed a thematic analysis approach to identify recurring patterns and concepts across the reviewed sources. Technological themes were drawn from the literature on the benefits of quantum computing, cryptographic vulnerabilities, and the development of PQC and QKD solutions. Governance themes included the assessment of policy gaps, institutional readiness, and the role of multi-stakeholder collaboration in advancing national preparedness. The analysis also examined regional and global dimensions such as participation in international standard-setting initiatives, the interoperability of security solutions, and the importance of shared resilience.

The thematic mapping provided a basis for integrating both technical and policy dimensions into a coherent narrative about Indonesia's preparedness for the quantum era. By comparing these patterns with Indonesia's existing digital security and transformation priorities, the study was able to propose a structured yet flexible approach for strengthening national readiness for quantum security. This methodology allows for the development of insights that are rooted in both the current realities of Indonesia's digital ecosystem and in the broader global movement towards quantum-safe technologies.

FINDINGS DISCUSSION

The analysis highlights a dual reality surrounding the rise of quantum computing. On one hand, the technology's transformative potential for optimisation, data-intensive research, and scientific discovery positions it as a strategic enabler for future innovation in healthcare, finance, logistics, and climate modelling. On the other, its disruptive implications for cryptographic systems signal unprecedented risks to the integrity, confidentiality, and authenticity of digital communications and critical infrastructures. This paradox illustrates the need for a proactive and balanced approach to quantum readiness.

A key finding is the urgency of addressing the vulnerability of existing encryption systems. Current cryptographic protocols such as RSA and elliptic curve cryptography, which underpin most secure digital communication, are potentially obsolete in the face of algorithms like Shor's and Grover's. This threat is not merely theoretical. The "store now, decrypt later" strategy, whereby malicious actors collect encrypted data today for future decryption using quantum machines, intensifies the need for immediate mitigation strategies. This insight underscores that the timeline for preparation cannot be tied solely to the commercial availability of large-scale quantum computers.

The Indonesian context reflects both opportunity and risk. Rapid digitalisation in government services, e-commerce, and financial technology has created a digitally dependent society whose security relies on the resilience of encryption methods. While these advancements support economic growth and improved service delivery, they also magnify the potential consequences of quantum-driven breaches. The lack of a unified national quantum security strategy further accentuates this vulnerability and indicates a pressing need for an integrated policy framework that brings together government, industry, academia, and international collaborators.

Another significant observation is that quantum readiness requires more than technical upgrades. Beyond adopting post-quantum cryptography and exploring quantum key distribution for secure communications, attention must also be paid to regulatory reform, capacity building, and coordinated investments in research and talent development. Indonesia's readiness will be strengthened by the establishment of a dedicated national centre for quantum security, functioning as both a research hub and a policy advisory platform. Such an institution could help bridge the gap between emerging science and policy implementation, fostering innovation while safeguarding national interests.

Moreover, findings from this conceptual exploration suggest that quantum readiness has important implications for global competitiveness. Nations that act early to develop and deploy quantum-resistant infrastructure are likely to gain first-mover advantages in the digital economy. For Indonesia, leveraging its growing technology ecosystem and aligning it with quantum security priorities can attract international partnerships, enhance investor confidence, and stimulate domestic innovation. Building local expertise through collaboration with universities and encouraging the participation of small and medium enterprises in the quantum supply chain will be critical in establishing an inclusive national response.

A further theme emerging from the analysis is the importance of regional and international cooperation. Cybersecurity challenges transcend national borders, and the quantum threat is no exception. Collaboration with ASEAN neighbours and international standardisation bodies, including active participation in the development of post-quantum cryptographic standards, can help Indonesia ensure interoperability of systems and contribute to global resilience. Shared research initiatives and knowledge exchange can accelerate the transition to secure quantum-era systems while reducing duplication of effort and cost.

The findings suggest that quantum security readiness should be conceptualised as a multidimensional challenge. Technological preparedness must be coupled with robust governance mechanisms and a culture of innovation.

International cooperation will also be vital in establishing interoperable standards, sharing threat intelligence, and strengthening regional digital trust. This interconnected approach aligns with the principles of anticipatory governance, which emphasises foresight, multi-stakeholder engagement, and adaptive policy instruments.

Ultimately, the discussion points to a paradigm shift in national security thinking. Preparing for quantum threats cannot be relegated to technical domains alone. It calls for a broader rethinking of cybersecurity as a pillar of economic competitiveness, public trust, and sovereignty in the digital era. By embedding quantum readiness in national strategy today, Indonesia can not only defend its critical digital infrastructure but also position itself as an active contributor to shaping global norms and solutions in the emerging quantum landscape. The evidence suggests that those countries which take a proactive and collaborative approach will be better placed to protect their digital economies and foster trust among their citizens and partners. This foresight-driven readiness will define the competitive and secure digital nations of the future.

Table 1: Thematic Summarization

Theme	Key Insights	Supporting Evidence (Intro & LR)	Implications (Findings & Discussion)
Transformative Potential of Quantum Computing	Quantum computing enables exponential gains in optimisation, big data analytics, and scientific modelling (e.g., drug discovery, climate simulations).	Introduction highlights IBM, Google, D-Wave prototypes demonstrating quantum advantage in optimisation and molecular simulations.	Suggests a paradigm shift in technology; Indonesia can leverage these advances to improve national R&D and innovation capacity.
Disruptive Cybersecurity Risks	Shor's and Grover's algorithms threaten the resilience of RSA/ECC encryption, risking data confidentiality and digital sovereignty.	LR emphasises dual-edge nature of quantum computing—power for innovation vs. capacity to break classical cryptosystems.	Immediate need for post-quantum cryptography and QKD adoption to mitigate “store-now-decrypt-later” risks.
Urgency of Quantum-Safe Transition	Quantum threats may become real within 10-30 years; waiting until maturity of large-scale quantum computers exposes nations to catastrophic breaches.	Introduction notes uncertainty of timeline but stresses urgency; LR underlines looming risks to digital infrastructure.	National readiness must start now; early adopters gain resilience and international competitiveness.
National Policy & Strategic Readiness	Security is not only a technical issue but also a governance challenge requiring policy coordination, institutional capacity, and multi-stakeholder collaboration.	LR calls for integration of policy, industry, academia, and international partnerships; highlights gaps in Indonesia's readiness.	Development of a National Centre for Quantum Security and coordinated investments in talent, research, and public awareness.
International Cooperation & Standards	Regional and global partnerships essential for developing interoperable PQC standards, sharing threat intelligence, and building digital trust.	LR mentions NIST's PQC standardisation efforts and global collaborations.	ASEAN-level and cross-border cooperation can reduce costs, accelerate secure adoption, and enhance Indonesia's strategic positioning.
Technological Governance Duality	Addressing quantum risks requires both technical tools (PQC, QKD, quantum RNG) and enabling policy frameworks including regulation, incentives, and long-term R&D strategies.	LR outlines advances in QKD, RNG, and PQC alongside need for regulatory frameworks.	A multidimensional approach aligns with anticipatory governance—coupling foresight, multi-stakeholder engagement, and adaptive policy.

Theme	Key Insights	Supporting Evidence (Intro & LR)	Implications (Findings & Discussion)
Opportunities for National Competitiveness	Early investment in quantum readiness can enhance Indonesia's role in the global digital economy and attract innovation-driven partnerships.	LR stresses that quantum-secure infrastructure boosts trust and long-term competitiveness.	A proactive stance in research, education, and industry development can turn a defensive necessity into a competitive advantage.
Paradigm Shift in Cybersecurity Thinking	Cybersecurity must be reframed as a national security and economic competitiveness issue in the quantum era.	Discussion underscores that technological disruption affects governance, trust, and sovereignty.	Policy innovation is crucial; quantum readiness becomes part of national resilience and technological sovereignty strategy.

Table 1 highlights the interconnected nature of technological, policy, and governance issues in preparing for the quantum era. The introduction emphasises the promise of quantum computing for optimisation and data-intensive applications, while the literature review reveals that the same capabilities create unprecedented risks for classical cryptographic systems. This dual nature underscores why preparedness cannot be delayed until large-scale quantum machines become commercially available.

The findings and discussion further show that quantum security readiness extends beyond technical upgrades. Effective transition to quantum-safe systems requires a whole-of-nation approach that integrates research, regulation, capacity building, and international cooperation. The themes demonstrate that secure adoption of post-quantum cryptography (PQC), quantum key distribution (QKD), and related innovations must be supported by strong governance and anticipatory policy instruments.

For Indonesia, the table illustrates that quantum readiness is both a defensive and an opportunity-driven agenda. Early investments in research and education, as well as collaboration with ASEAN partners and global standardisation initiatives, can strengthen resilience and enhance competitiveness. By addressing these themes in a coordinated manner, Indonesia can safeguard its digital infrastructure, build trust in its digital economy, and contribute meaningfully to the emerging global quantum security ecosystem.

FUTURE RESEARCH PROSPECTS AND KEY ROLES OF QUANTUM SECURITY

As the digital landscape continues to evolve, the future of cybersecurity will increasingly be shaped by the progress of quantum technologies. Quantum security, which encompasses both quantum-resistant algorithms and quantum-based encryption methods, is emerging as a critical foundation for safeguarding information in the post-quantum era. The future prospects of quantum security are vast. With the expected rise of practical quantum computers within the next decade, institutions across the globe, from governments to corporations, are accelerating their transition to quantum-safe infrastructures. Post-quantum cryptography (PQC) is being standardized by organizations such as NIST, while quantum key distribution (QKD) is gaining traction for ultra-secure communication networks.

In the near future, we can expect quantum-secure systems to be embedded into financial platforms, healthcare databases, defense networks, and even consumer-level applications. The key roles of quantum security extend beyond mere protection of data. It will enable digital trust in an era where current cryptographic systems are no longer reliable. Quantum security ensures the confidentiality, authenticity, and integrity of information despite the threat of quantum-enabled adversaries.

It also supports the resilience of emerging technologies, such as the Internet of Things (IoT), blockchain, and artificial intelligence, by reinforcing their cryptographic foundations. Moreover, quantum security plays a strategic role in national defense and economic competitiveness. Nations that lead in implementing quantum-safe systems will have a decisive edge in protecting their digital sovereignty.

In summary, quantum security is not only a defensive necessity but also a proactive enabler of innovation and global digital stability. Its advancement and integration will shape the future of secure communication and trusted digital ecosystems.

CONCLUSION

As Indonesia advances its digital transformation across government, industry, defense, and society, the importance of adopting future-ready cybersecurity measures cannot be overstated. Quantum security technology represents not only a response to emerging quantum threats but also a strategic investment in national resilience, technological sovereignty, and data protection. This overview has highlighted that while the full realization of quantum computing may still be several years away, the risks to current cryptographic systems are real and urgent. Traditional encryption methods will be rendered vulnerable by quantum algorithms, exposing critical infrastructures and sensitive information to potential breaches.

For Indonesia, now is the time to act. Building quantum readiness through research, education, policy development, and international collaboration is essential. Embracing post-quantum cryptography, exploring quantum key distribution, and supporting local innovation in quantum technologies will prepare Indonesia to face the challenges and seize the opportunities of the quantum era. Quantum security is not merely a technical upgrade, it is a national imperative. By proactively engaging with this technological frontier, Indonesia can ensure the confidentiality, integrity, availability and sovereignty of its digital future.

REFERENCES

1. Artikel IT, ITG.ID-IT Governance Indonesia, "Ancaman Siber Ultrascale: Mampukah Indonesia Hadapi Serangan Quantum Computing?", <https://itgid.org/insight/artikel-it/ancaman-siber-ultrascale-mampukah-indonesia-hadapi-serangan-quantum-computing/>, 30 Desember 2023.
2. Nurhadi, N. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey", published in 4th International Conference on Wireless and Telematics (ICWT), 1 July 2018, DOI:10.1109/ICWT.2018.8527822, CorpusID:53279739 <https://www.semanticscholar.org/paper/Quantum-KeyDistribution-%28QKD%29-Protocols%3A-A-Survey-Nurhadi-Syambas/858b2ca1a277ca343d3ca5ddeb9e7a60a622c4a7/figure/10>, 2018.
3. Bernstein, D. J., et al. (2020). "Post-Quantum Cryptography: New Horizons for Secure Communication." Journal of Cryptographic Engineering.
4. E-book: "An Introduction to Quantum Computing", Phillip Kaye Raymond Laflamme Michele Mosca, Oxford University Press Inc., New York, 2007.
5. IBM.com: "IBM Quantum is building a large-scale, fault tolerant quantum computer", <https://www.ibm.com/quantum>, 2025.
6. Journal, JAPCC, "Quantum Technology for Defense: What to Expect for the Air and Space Domains", Journal Edition 35. Transformation & Capabilities. Page 42.
7. Rita Puspita Sari, "Quantum Safe Networks: Solusi Keamanan Data di Era Kuantum", Artikel di Cyber Hub, <https://cyberhub.id/pengetahuan-dasar/quantum-safe-networks>, 15 Maret 2025.
8. Sadik Khan, P. Krishnamoorthy, Mrinal Goswami, Fayzieva Makhbuba Rakhimjonovna, Dr. Salman Arafath Mohammed, Dr.D.Menaga, "Quantum Computing And Its Implications For Cyber security: A Comprehensive Review Of Emerging Threats And Defenses", Nanotechnology Perceptions 20(13): 1232-1248, DOI:10.62441/nano-ntp.v20iS13.79, November 2024.
9. Thales, e-book: "Data Threat Report: AI, Quantum and the Evolving Data Threat scape", cpl.thalesgroup.com, Data Threat Report: Quick Glance at Key Findings, <https://cpl.thalesgroup.com/ppc/datathreatreport?>, 2025.