Jurnal Komputer, Informasi dan Teknologi Vol: 4, No 2, 2024, Page: 1-10

Quantum Entropy-Based Encryption for Securing Communication Devices in TNI AU Space Units

Lisdi Inu Kencana[1*], H.A Danang Rimbawa[2], Bisyron Wahyudi[3]

[123] Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology, Universitas Pertahanan

DOI: https://doi.org/10.53697/jkomitek.v4i2.2091
*Correspondence: Lisdi Inu Kencana
Email: lisdi.kencana@tp.idu.ac.id

Received: 11-11-2024
Accepted: 23-11-2024
Published: 27-12-2024

Abstract: The rising threat of cyber-attacks demands advanced encryption technologies to ensure secure communication. This study evaluates the performance and security of the Quantum Shieldz Cipher integrated with Quantum Entropy-Based Encryption (QEBE) to address the limitations of conventional encryption methods. The main objective is to test the system's ability to generate unpredictable encryption keys, detect interception attempts, and resist quantum-based cyber threats. Experiments were conducted under various operational scenarios, including standard conditions, high interference, and high bandwidth environments, with a focus on its implementation for strategic communication in the Indonesian Air Force (TNI AU).The results show that QEBE effectively generates highly secure encryption keys using the Quantum Random Number Generator (QRNG), significantly reducing the risk of brute-force attacks. The system successfully detects interception by identifying changes in qubit states during data transmission. The implementation within TNI AU demonstrates its effectiveness in securing critical communication systems that require robust protection. However, the system relies heavily on stable network infrastructure with high bandwidth to maintain optimal performance. Compared to conventional methods, QEBE provides superior security and resistance to quantum-based attacks, albeit with a slight trade-off in processing speed. In conclusion, the Quantum Shieldz Cipher integrated with QEBE shows significant potential for enhancing secure communication systems, particularly in critical operations within TNI AU. This technology is a promising solution to safeguard against evolving cyber threats and quantum-based attacks.

Keywords: Quantum Entropy-Based Encryption (QEBE), Military Communication Security, Quantum-Based Security Protocols

Introduction

The advancement of technology in the Industry 4.0 era transitioning to Industry 5.0 has integrated the Internet of Things (IoT), Artificial Intelligence (AI), and robotics with human expertise (Chen et al., 2024). This integration aims to create efficient, flexible, and sustainable production systems while enhancing human well-being. In a military context, communication technology becomes a crucial aspect for protecting sensitive data from increasingly complex cyber threats and supporting the success of military operations (Sahu et al., 2024).

The protection of military communication devices is becoming increasingly important as cyber-attacks targeting military infrastructure rise. Quantum-based encryption technology provides better security solutions compared to conventional methods. However, commercial satellite communication systems, which play a strategic

role in modern military operations, still face significant limitations (Wang et al., 2023). Traditional encryption methods struggle to counter sophisticated cyber threats, making the adoption of more advanced technologies an urgent necessity (Hazra et al., 2024).

Cyber threats have been emphasized in Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional (Presiden Republik Indonesia, 2023) and Keputusan Panglima TNI No. Kep/1355/XII/2018 tentang Doktrin Siber TNI. These regulations classify cyber threats as military threats that significantly impact TNI's core duties. As one of the main forces, the Indonesian Air Force (TNI AU) plays a strategic role in addressing these threats. One of the efforts involves DISPAMSANAU (Air Signal and Security Service), responsible for cybersecurity organization development, post-incident response, and coordination with related institutions (militer.udara, 2023).

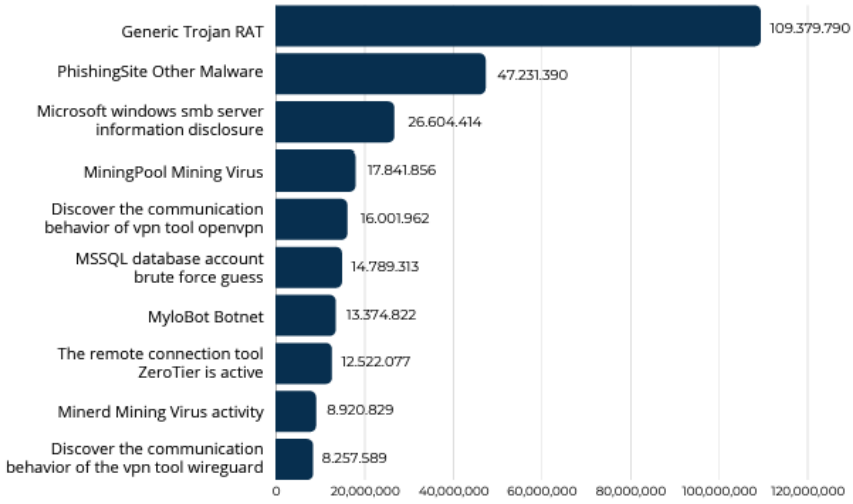

Figure 1. Anomali Serangan Siber di Indonesia Tahun 2023

The urgency of these threats is further underscored in Figure 1, which shows that the Generic Trojan RAT was the most prevalent attack in Indonesia in 2023 (BSSN, 2023). This attack creates dangerous traffic that can degrade network performance, steal sensitive data, and damage organizational reputation. This condition drives the adoption of more reliable security technologies, such as quantum entropy-based encryption, to protect military communications, particularly in the TNI AU environment.

Quantum entropy-based encryption technology leverages quantum mechanics principles to generate encryption keys that are hard to predict and breach. With the no-cloning theorem, quantum data cannot be copied without altering its characteristics, making it more secure. This technology can prevent eavesdropping and advanced cyber-attacks while ensuring the confidentiality of military communications (Lai et al., 2023). Therefore, adopting this technology becomes a crucial step in protecting TNI AU communications from modern cyber threats.

To address these challenges, several previous studies have explored the application of quantum technology for military communication security. Publications such as "Application of Quantum Technology in Military Communications" emphasize the use of

quantum cryptography to provide absolute secrecy and high communication capacity through the no-cloning theorem and quantum limitations (Wang et al., 2023). This technology overcomes the weaknesses of conventional encryption, which is vulnerable to advanced cyber-attacks. However, these studies are generalized and have not examined practical applications in specific military organizations.

Unlike previous research, this study focuses on developing Quantum Entropy-Based Encryption supported by Quantum Shieldz Cipher hardware. This technology is practically tested to prevent eavesdropping, enhance operational efficiency, and provide resilience against quantum computer threats. The focus of this research is its implementation in TNI AU Space Units, to improve military communication security in specific conditions and address modern cyber threats.

This research aims to evaluate the integration of quantum entropy-based encryption into the Quantum Shieldz Cipher and assess its effectiveness in enhancing TNI AU's communication security. The results of this study are expected to make a significant contribution to military security technology development. Furthermore, this research aims to provide practical guidelines for implementing the technology while identifying and resolving technical challenges that may arise in the field.

The integration of quantum entropy-based encryption technology through Quantum Shieldz Cipher is expected to protect TNI AU communications from increasingly sophisticated cyber threats. This technology has the potential to strengthen information security frameworks in the TNI AU environment and increase operational resilience. Thus, the adoption of quantum encryption technology becomes a strategic step in addressing cybersecurity challenges in the modern era.

Methodology

Quantum-based encryption utilizes the principles of quantum mechanics to protect information using Heisenberg's uncertainty principle and the no-cloning theorem (Elani, 2021). These principles ensure that any eavesdropping attempt will cause detectable changes in the quantum state. Quantum encryption uses qubits, the basic unit of information in a quantum system, which can exist in a superposition of two states, providing a higher level of security compared to classical encryption methods. The BB84 protocol, introduced by Bennett and Brassard in 1984, forms the foundation of modern quantum encryption (Abdullah & Jassem, 2019).

The primary advantage of quantum-based encryption is its ability to detect eavesdropping. Any attempt to measure a qubit during transmission will alter its state, which can be detected by the receiver (Abushgra, 2023). This technology also leverages quantum entanglement, where two qubits remain correlated even when separated by large distances. This phenomenon enables the generation of encryption keys that are highly secure, unpredictable, and resistant to eavesdropping attempts (Clemen & Teleron, 2023).

Quantum Entropy-Based Encryption (QEBE) harnesses natural entropy in quantum systems to produce truly random keys using a Quantum Random Number Generator (QRNG). This randomness is crucial for securing transmitted data, as the encryption keys generated are never identical in any communication session. QEBE plays a key role in

applications requiring high security, such as military communications, where unpredictable encryption keys are essential (Siswanto & Witjaksono, 2019).

QRNG works by measuring quantum fluctuations, such as the intensity of light from lasers, to generate random numbers used as encryption keys. The security of QEBE lies in the impossibility of predicting the results of these quantum measurements, making it extremely difficult for intruders to predict or duplicate the encryption keys. QRNG also produces encryption keys at high speeds, reaching gigabits per second, sufficient for modern communication and military operational needs.

Quantum Shieldz Cipher combines quantum encryption methods and classical cryptography to provide dual-layer protection for transmitted data. The system uses random encryption keys generated by QRNG, ensuring unpredictability and strengthening communication resilience against cyber threats. Quantum Shieldz Cipher is designed to be compatible with various communication devices and equipped with verified cryptographic modules, guaranteeing robust protection against eavesdropping attempts (EYL Inc., 2023).

Factors such as bandwidth limitations, signal interference, and transmission delays are the main challenges in maintaining the effectiveness of operational communication in TNI AU Space Units. Additionally, increasingly complex cyber threats demand the adoption of advanced encryption technologies resistant to interception attempts. Quantum Entropy-Based Encryption (QEBE) and Quantum Shieldz Cipher provide a concrete solution to address these challenges by offering unpredictable and highly random encryption keys, thereby enhancing communication security and supporting TNI AU' military mission success.

The quantum-based encryption process used in this study consists of the following stages:

1. Message State: The message data is represented as qubits in a superposition state, as described by the following formula:

$$U|\psi\rangle = (\alpha\gamma - \beta\delta)|0\rangle + (\alpha\delta + \beta\gamma)|1\rangle \quad (1)$$

This state enables the message to be encrypted in a quantum form that is difficult to hack.

2. Key Generation: The encryption key is randomly generated using a Quantum Random Number Generator (QRNG). This process leverages quantum fluctuations, such as laser light intensity, to define random qubit states as follows:

$$|\phi\rangle = \gamma|0\rangle + \delta|1\rangle \quad (2)$$

The keys generated possess high entropy and are unpredictable.

3. Encryption: The qubit message is encrypted using a transformation dependent on the quantum key $|\phi\rangle$. This process is formulated as:

$$U|\psi\rangle = (\alpha\gamma - \beta\delta)|0\rangle + (\alpha\delta + \beta\gamma)|1\rangle \quad (3)$$

This ensures that the message can only be decrypted by a party possessing the correct encryption key.

4. Decryption: An inverse transformation $U^{\dagger}$ is applied to the encrypted message to recover the original state, as follows:

$$U^{\dagger}U|\psi\rangle = |\psi\rangle \quad (4)$$

5. Key Security: The security of this process is supported by Von Neumann entropy, defined as:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \quad (5)$$

High entropy ensures that the key cannot be predicted, and any interception attempt will alter the quantum state, which can be detected.

The integration of Quantum Entropy-Based Encryption (QEBE) with Quantum Shieldz Cipher provides significant improvements in military communication security. This combination ensures that encryption keys are always random and unpredictable, making them difficult to compromise by classical or quantum computers. This technology also maintains high compatibility with existing communication devices, offering a practical and easily implementable solution for various military communication scenarios.

The methodology of this research involves the following steps:

1. Test Environment Preparation: Installation of Quantum Shieldz Cipher hardware and supporting software in a laboratory simulation environment.
2. Technology Implementation: Integration of QEBE using random keys from QRNG into the communication module to generate quantum-based encryption keys.
3. Security Testing: Simulation of cyber-attacks, including Man-in-the-Middle (MitM) attacks and eavesdropping attempts, to evaluate the resilience of quantum encryption against conventional threats.
4. Performance Evaluation: Measurement of technology efficiency based on data transmission speed, resistance to eavesdropping, and the quality of encryption keys.

The results of this methodology provide an experimental evaluation of the effectiveness of integrating Quantum Shieldz Cipher with QEBE in enhancing military communication security. All steps and testing protocols are designed to ensure that this research is replicable and supports implementation in TNI AU communications, meeting the necessary security standards.

Result and Discussion

The results of this research were obtained by testing the Quantum Shieldz Cipher under various secure communication scenarios. The testing aimed to evaluate several key aspects, such as encryption time, resistance to cyber-attacks, and the eavesdropping detection capability that represents the primary advantage of this technology. The testing scenarios included standard environments, high interference, high bandwidth, and

eavesdropping threats that reflect real-world communication security conditions. This analysis demonstrates the performance and security of the developed technology compared to conventional encryption methods.

The results obtained from these tests are presented as a comparative analysis of encryption effectiveness and efficiency across various scenarios. Furthermore, these findings are discussed in-depth, linking them to relevant theories and practical implications for implementation within TNI AU environments. Thus, this research not only identifies the superior performance of Quantum Shieldz Cipher but also provides a comprehensive understanding of its potential to enhance communication security in military operations.

Comparison of Encryption Methods

The evaluation results in Table 1 highlight the performance differences between Quantum Entropy-Based Encryption (QEBE) and conventional encryption methods based on several key criteria. These tests measure aspects such as security level, key predictability, eavesdropping detection, resistance to quantum-based attacks, implementation complexity, and encryption speed.

QEBE outperforms conventional methods due to the utilization of the Quantum Random Number Generator (QRNG), which generates random and unpredictable keys. This effectively reduces the risk of brute-force attacks. QEBE's ability to detect eavesdropping through changes in qubits has also proven to be efficient during data transmission, maintaining information integrity in high-risk environments.

Additionally, this technology is designed with a structure that ensures each stage of the process operates optimally under various operational conditions. The utilization of quantum methods enables QEBE to function efficiently in complex communication environments, providing stronger protection against third-party intervention attempts.

Tabel 1: Perbandingan Metode Enkripsi

Criteria	Conventional Encryption	Quantum Entropy-Based Encryption (QEBE)
Security Level	Medium	High
Key Predictability	High (easily predictable)	Low (difficult to predict)
Eavesdropping Detection	Difficult	Easy (qubit state changes detected)
Resistance to Quantum Computers	Low	High

The results show that Quantum Entropy-Based Encryption (QEBE) has a higher security level compared to conventional methods. This is because QEBE uses a Quantum Random Number Generator (QRNG) to produce truly random and unpredictable keys, effectively minimizing the risk of brute-force attacks.

QEBE ability to detect eavesdropping through changes in qubit states during data transmission is also highly effective. In eavesdropping detection tests, the system successfully identified third-party interventions with high accuracy. However, testing also showed that QEBE has higher implementation complexity and requires stable bandwidth to maintain optimal performance.

Encryption speed tests demonstrated that conventional methods were superior in processing time due to the additional complexity in processing qubits within QEBE. Nevertheless, the superior security provided by QEBE makes it highly relevant for environments demanding robust security measures.

Strengths and Limitations of Quantum Shieldz Cipher

The test results and evaluation of Quantum Shieldz Cipher under various scenarios are presented in Table 2.

Table 2: Strengths and Limitations of Quantum Shieldz Cipher

Aspect	Strengths	Limitations
Key Security	Generates random keys via QRNG	Requires specialized QRNG hardware
Eavesdropping Detection	Effectively detects quantum state changes	Requires technical user competence
Operational Efficiency	Maintains security without significant latency	Relies on high-bandwidth environments
Resilience to Attacks	Resistant to quantum-based attacks	Requires support for complex technology

The evaluation results show that Quantum Shieldz Cipher performs optimally in generating secure encryption keys using QRNG. The system successfully detects eavesdropping attempts with high accuracy during simulations involving both active and passive interception.

However, significant limitations include the requirement for specialized hardware and the need for a high-bandwidth environment. In testing conducted under network interference, the system's performance significantly decreased, particularly during key authentication and encrypted data transmission stages.

Quantum Key Authentication Process

The secure and reliable Quantum Key Authentication process tested in this research is outlined in Table 3.

Table 3: Quantum Key Authentication Process

Stage	Description
Connection Initialization	The user initiates the connection with an authentication request.
Key Generation	QRNG generates a quantum-based random key.

Key Distribution	The key is securely transmitted over an encrypted channel.
Authentication	The system verifies the validity of the received key.
Data Encryption	Data is encrypted using the authenticated key.
Data Transmission	Encrypted data is transmitted through the public channel.
Decryption and Verification	The recipient decrypts the data and verifies its authenticity.

Testing results confirm that each authentication stage functions effectively to ensure secure communication. The keys generated using QRNG were proven to be random and unpredictable, providing a high level of security. During the key distribution stage, the system successfully prevented third-party intervention by detecting changes in qubit states caused by eavesdropping attempts.

However, the performance of the authentication process heavily relies on a stable bandwidth. In environments with network interference, authentication times increased, affecting overall operational efficiency.

Comparison of Eavesdropping Detection Techniques

The results of testing the eavesdropping detection capabilities of conventional methods and QEBE are presented in Table 4.

Table 4: Comparison of Eavesdropping Detection Techniques

Detection Technique	Conventional Method	Quantum Entropy-Based Encryption (QEBE)
Man-in-the-Middle (MitM)	Difficult to detect	Detected through quantum state changes
Passive Eavesdropping	Difficult to detect	Detected with high accuracy
Active Eavesdropping	Requires constant monitoring	Easily detected via quantum interaction
Malware-Based Eavesdropping	Limited to conventional detection	Detected via QRNG changes

The testing results indicate that QEBE significantly outperforms conventional methods in detecting various types of eavesdropping. QEBE successfully identified quantum state changes caused by interception attempts with high accuracy.

Conclusion

The research results demonstrate that the Quantum Shieldz Cipher integrated with Quantum Entropy-Based Encryption (QEBE) provides a significant improvement in communication security, particularly for strategic operations within TNI AU Space Units. By utilizing the Quantum Random Number Generator (QRNG), the system generates truly random and unpredictable keys, effectively mitigating brute-force attacks and enabling real-time interception detection through changes in qubit states.

While the technology requires specialized hardware and stable high-bandwidth infrastructure, its ability to resist quantum-based cyber threats and secure critical communication systems makes it a promising solution for modern military operations. Future research and infrastructure optimization are essential to ensure seamless implementation and further enhance communication resilience in TNI AU.

References

Abdullah, A., & Jassem, Y. (2019). Enhancement of Quantum Key Distribution Protocol BB84. *Journal of Computational and Theoretical Nanoscience*, *16*, 1138–1154. https://doi.org/10.1166/jctn.2019.8009

Abushgra, A. A. (2023). How Quantum Computing Impacts Cyber Security. *2023 Intelligent Methods, Systems, and Applications (IMSA)*, 74–79. https://doi.org/10.1109/IMSA58542.2023.10217756

BSSN. (2023). *Lanskap Keamanan Siber Indonesia 2023*.

Chen, S.-C., Chen, H.-M., Chen, H.-K., & Li, C.-L. (2024). Multi-Objective Optimization in Industry 5.0: Human-Centric AI Integration for Sustainable and Intelligent Manufacturing. *Processes*, *12*(12). https://doi.org/10.3390/pr12122723

Clemen, J. M., & Teleron, J. (2023). Advancements in Encryption Techniques for Secure Data Communication. *International Journal of Advanced Research in Science, Communication and Technology*, 444–451. https://doi.org/10.48175/IJARSCT-13875

Elani, Z. (2021). Qubit, Quantum Entanglement and all that: Quantum Computing Made Simple. *American Research Journal of Physics*, *7*, 1–9. https://doi.org/10.21694/2380-5714.21002

EYL Inc. (2023). *Quantum Shieldz Cipher: Anti-Eavesdropping Solution Powered by Quantum Shieldz*.

Hazra, R., Chatterjee, P., Singh, Y., Podder, G., & Das, T. (2024). *Data Encryption and Secure Communication Protocols* (pp. 546–570). https://doi.org/10.4018/979-8-3693-6557-1.ch022

Lai, J., Yao, F., Wang, J., Zhang, M., Li, F., Zhao, W., & Zhang, H. (2023). Application and Development of QKD-Based Quantum Secure Communication. *Entropy*, *25*(4). https://doi.org/10.3390/e25040627

militer.udara. (2023). *TNI AU Perkuat Kewaspadaan Keamanan Siber: Dispamsanau Gelar Bimbingan Teknis Cyber Security*. https://www.instagram.com/militer.udara/p/CzWEbTZSdy3/

Presiden Republik Indonesia. (2023). *Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber*. Presiden Republik Indonesia.

Sahu, K., Kumar, R., Srivastava, R. K., & Singh, A. K. (2024). Military Computing Security: Insights and Implications. *Journal of The Institution of Engineers (India): Series B*. https://doi.org/10.1007/s40031-024-01136-6

Siswanto, M., & Witjaksono, G. (2019). Parallel Quantum Random Number Generator (p-QRNG) Design for Enhancing Data Rate. *International Journal of Advances in Soft Computing and Its Applications*.

Wang, H., Li, N., & Jiang, H. (2023). Application of Quantum Technology in Military Communications. *2023 International Conference on Networking, Informatics and Computing (ICNETIC)*, 59–62. https://doi.org/10.1109/ICNETIC59568.2023.00018