Jurnal Komputer, Informasi dan Teknologi Vol: 4, No 2, 2024, Page: 1-11

Enhancing Data Security and Integrity with Post-Quantum and AES Digital Signatures

Rayasa Puringgar Prasadha Putra[1*], H. A. Danang Rimbawa[2], Bisyron Wahyudi[3]

[123] Cyber Defense Engineering, Faculty of Defense Science and Technology, Universitas Pertahanan, Bogor, Indonesia

DOI: https://doi.org 10.53697/jkomitek.v4i2.2081/
*Correspondence: Rayasa Puringgar Prasadha Putra
Email: rayasa.putra@tp.idu.ac.id

Received: 03-10-2024
Accepted: 11-11-2024
Published: 23-12-2024

Abstract: Data security and integrity are crucial issues in contemporary information systems, since the emergence of quantum computing presents substantial risks to traditional cryptographic techniques such as RSA and ECC. This work suggests a hybrid technique that combines the Advanced Encryption Standard (AES) for symmetric encryption with Post-Quantum Cryptography (PQC) digital signatures to mitigate these issues. The framework seeks to safeguard sensitive documents, including PDFs, against unauthorized alterations and Man-in-the-Middle (MiTM) attacks. A simulation is executed to illustrate the threats associated with Man-in-the-Middle (MiTM) attacks, whereby the encrypted document and digital signatures are intercepted, altered, and re-encrypted. The technology guarantees data integrity by signature verification and hash comparisons, efficiently identifying and preventing tampering. The findings indicate that the suggested PQC-AES hybrid system not only fortifies defenses against conventional threats but also improves resistance to quantum-based assaults, offering a scalable and safe approach for contemporary data security. The research emphasizes the need of implementing quantum-resistant algorithms to safeguard digital security systems for the future, while preserving the efficacy of existing encryption techniques. The progression of quantum computing presents substantial threats to traditional cryptography methods, including RSA and ECC. These cryptosystems depend on mathematical issues that can be effectively resolved using quantum algorithms, especially Shor's algorithm. Post-Quantum Cryptography (PQC) has emerged as a viable way to mitigate this issue.

Keywords: Post – Quantum Cryptography, Digital Signature, Data Security, Data Integrity, Advanced Encryption Standard

Introduction

In an era marked by heightened susceptibility to cyberattacks, the security and integrity of data are paramount in the advancement of information systems. Quantum computers possess the capability to dismantle traditional asymmetric cryptography schemes, as demonstrated by Shor's and Grover's algorithms. Consequently, there is a necessity for more resilient and durable responses to quantum threats (Shim, 2022). The rapid advancement of quantum computing has posed significant challenges to conventional cryptographic systems. Algorithms such as RSA, ECC, and other public-key cryptographic schemes rely on the computational complexity of mathematical problems like integer factorization and discrete logarithms. However, Shor's quantum algorithm can efficiently solve these problems, threatening the security of existing encryption methods (Liu et al., 2022). Data integrity and security are crucial aspects in the administration of information systems, especially in the constantly changing field of cybersecurity. Specifically, the legal

framework for the use of e-Signatures in Indonesia includes provisions for digital signatures. This is outlined in Article 1 Verse (12) of Law (UU) Number 11 of 2008 regulating Electronic Information and Transactions (ITE). In the past, classical cryptography has been extensively employed for data and communication security. However, it has been shown that certain classical cryptographic algorithms could be susceptible to assaults carried out by upcoming quantum computers. Digital signatures are a crucial cryptographic tool used to verify the validity of documents and ensure the integrity of data. Quantum computing has given rise to the concept of digital signatures based on quantum cryptography, offering a better level of security compared to prior technologies. Quantum cryptography utilises ideas from quantum mechanics, which provide a fundamentally distinct and more challenging method to breach compared to classical cryptography techniques.

In addition, symmetric encryption methods like the Advanced Encryption Standard (AES) remain resilient against quantum threats, provided sufficient key lengths are used (Alagic et al., 2022). Advanced Encryption Standard (AES) is one of the symmetric encryption algorithms that has been widely used in various applications due to its speed and efficiency.When a file or document goes through the encryption process, the contents of the file will be turned into unreadable symbols. Then, when the encryption result goes through the decryption process by entering the key used in the encryption process, the contents of the file will return to normal (Olivia Putri Irine Irawan et al., 2023). With the rapid advancements in quantum computing, traditional cryptographic algorithms such as RSA, ECC, and other public-key systems are increasingly at risk of becoming obsolete. As a result, the National Institute of Standards and Technology (NIST) has called for the development of post-quantum cryptography (PQC), which can withstand quantum-based attacks (Chen et al., 2016). The main application of quantum communication is QKD, which uses the properties of qubits to establish a secure key between two parties. Well-known protocols, such as BB84, are examples of this technique. The security of QKD is based on quantum mechanics, so it is essentially impossible for an eavesdropper to intercept the communication without disrupting the qubits and alerting the parties involved (Liu et al., 2022).

Data transmission has become a prime target for attackers in modern digital systems, particularly with sensitive documents such as PDFs. In a Man-in-the-Middle (MiTM) attack, an adversary intercepts and modifies the transmitted data, compromising both its confidentiality and integrity. Traditional cryptographic systems, while effective against classical attacks, may fail under quantum-based threats due to their reliance on computational hardness assumptions (Khan et al., 2024). Therefore, developing robust security frameworks that combine quantum-resistant digital signatures and proven encryption methods like AES is critical for ensuring data security in a post-quantum era. This study introduces a hybrid system that integrates AES encryption with PQC-based digital signatures to provide confidentiality, authenticity, and integrity for sensitive document transmission. The framework not only addresses the vulnerabilities of traditional systems but also strengthens defenses against emerging quantum-based attacks. By simulating a MiTM attack on PDF documents, the study demonstrates the effectiveness of this hybrid approach in detecting unauthorized modifications and ensuring data integrity.

Methodology

This study employs a methodology that combines Post-Quantum Cryptography (PQC) digital signatures with the Advanced Encryption Standard (AES) to ensure secure and tamper-proof document transmission. This hybrid framework guarantees the confidentiality, authenticity, and integrity of sensitive data in the face of both classical and quantum attacks. The proposed methodology consists of three primary phases: key generation, encryption and signing, and transmission with verification.

This step involves the generation of the AES encryption key and post-quantum digital signature keys. The AES key is symmetric and is produced using a secure random number generator to guarantee anonymity (Stallings, 2017). During the key generation phase, a pair of post-quantum public and private keys is produced utilizing a PQC algorithm like CRYSTALS-Dilithium, identified as a robust candidate for quantum-resistant digital signatures (Peikert, 2016). A symmetric key is generated concurrently for AES-256 encryption, which guarantees both high security and computational efficiency (Chen et al., 2016) The sensitive document, specifically a PDF file, is encrypted using the AES-128 method in Cipher Block Chaining (CBC) mode to provide secrecy and protection against block-based attacks (Menezes et al., 2018).

The encryption and signing phase commences with the application of the AES-256 encryption algorithm to the plaintext document. AES is chosen for its established resilience against quantum-based Grover's algorithm, attributed to its limited key search space (Khan et al., 2024). After encryption, the system generates a hash of the encrypted document with SHA-256 and signs the hash utilizing the PQC private key. This measure guarantees the authenticity of documents and inhibits unauthorized alterations during transmission (Aggarwal et al., 2018).

During the transmission and verification phase, the encrypted document along with the digital signature is sent to the receiver. Upon receipt of the document, the recipient decrypts it with the AES symmetric key and verifies the digital signature utilizing the PQC public key. The integrity of the decrypted document is verified by comparing its hash with the signed hash. Any discrepancy suggests a possible tampering attempt, as observed in a MiTM attack (Bernstein & Lange, 2017).

To validate the framework, MiTM attacks are simulated where encrypted documents and digital signatures are intercepted, modified, and re-encrypted. The system's ability to detect these modifications through signature verification and hash comparisons demonstrates the effectiveness of the hybrid approach (Chen et al., 2016; Preskill, 2018). We conduct a simulation of MiTM attacks on PDF documents to assess the effectiveness of the proposed framework. The attacker intercepts, decrypts, alters, and re-encrypts the document prior to sending it to the intended recipient. The proposed system effectively detects unauthorized modifications via signature verification and hash comparisons, illustrating its resilience to tampering and quantum threats.

The methodology is executed utilizing Python alongside the subsequent libraries:

- AES-256 encryption and decryption in cryptography.
- CRYSTALS-Dilithium is a post-quantum cryptography algorithm designed for digital signatures.

- PyPDF2 facilitates PDF management, encompassing reading, modification, and rewriting tasks.
- Hashlib is utilized for the computation of SHA-256 hashes.
-

This methodology leverages the computational efficiency of AES for encryption while integrating post-quantum digital signatures to ensure integrity and authenticity, making it suitable for securing data transmissions in both classical and quantum threat models. The proposed methodology integrates AES-128 with quantum-resistant digital signatures, offering a scalable and efficient approach to securing sensitive documents in a post-quantum context. Quantum communication represents a revolutionary method for safe information transmission. Utilizing qubits and quantum phenomena like entanglement, it has the potential to revolutionize encryption and enable long-distance communication, providing unmatched security and efficiency (Liu et al., 2022). These advancements have generated new prospects for the commercialization of quantum communications, which are expected to significantly influence the evolution of secure communications in the future (Mehic et al., 2020).

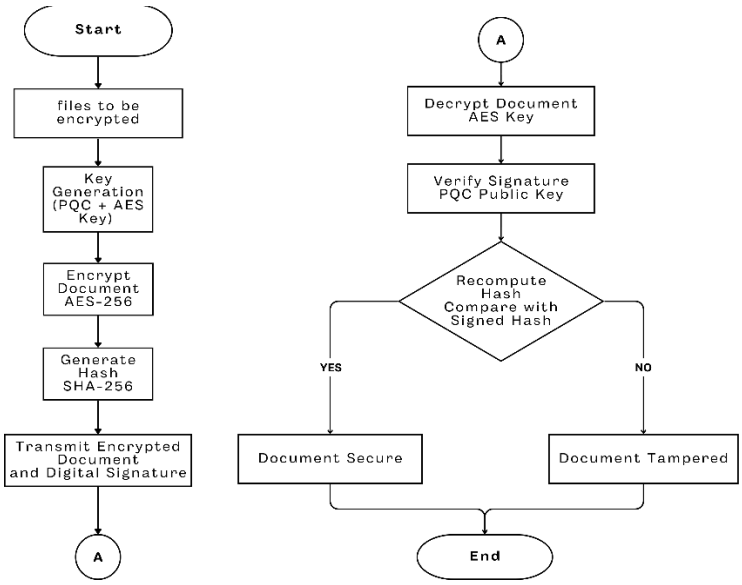

Figure 1. Research Methodology

Figure 1 Researh Methodology illustrates the stages of the methodology used in this research to integrate AES-256 encryption with Post-Quantum Cryptography (PQC) digital signatures. The process begins with Key Generation, where a PQC public-private key pair and an AES-256 symmetric key are generated. This key will be used in the encryption and signature process. Next, at the Encrypt Document stage, the document (e.g. PDF) is encrypted using the AES-256 algorithm to ensure data confidentiality. After that, at the Generate Hash stage, a hash of the encrypted document is generated using the SHA-256 algorithm. This hash is then signed at the Sign Hash stage using the PQC private key, which ensures the authenticity and integrity of the document.

The next stage is Transmit Encrypted Document and Digital Signature, where the encrypted document along with the digital signature is sent to the recipient. At the receiving end, the document is decrypted using the AES key at the Decrypt Document stage. After decryption, the verification process starts with Verify Signature using the PQC public key. In the Yes condition (valid signature), the system proceeds to the Recompute Hash and Compare with Signed Hash stage. If the hash comparison result matches (Yes), the document is considered secure and Document Secure is marked. However, if the hash comparison result does not match (No), the document is declared modified and Document Tampered is marked. In case of No at the Verify Signature stage (invalid signature), the process immediately declares that the document has been manipulated and is marked as Document Tampered. This flowchart clearly shows the steps to detect Man-in-the-Middle (MiTM) attacks and ensure confidentiality, authenticity and integrity of data using a combination of AES-256 and PQC digital signatures. The 'Yes' and 'No' conditions help identify if the validation process was successful or if there are indications of an attack on the document.

Result and Discussion

The results of this study are presented in the form of tables and figures to highlight the performance and effectiveness of the proposed PQC-AES framework.

a. Comparison of PDF file size before and after encryption

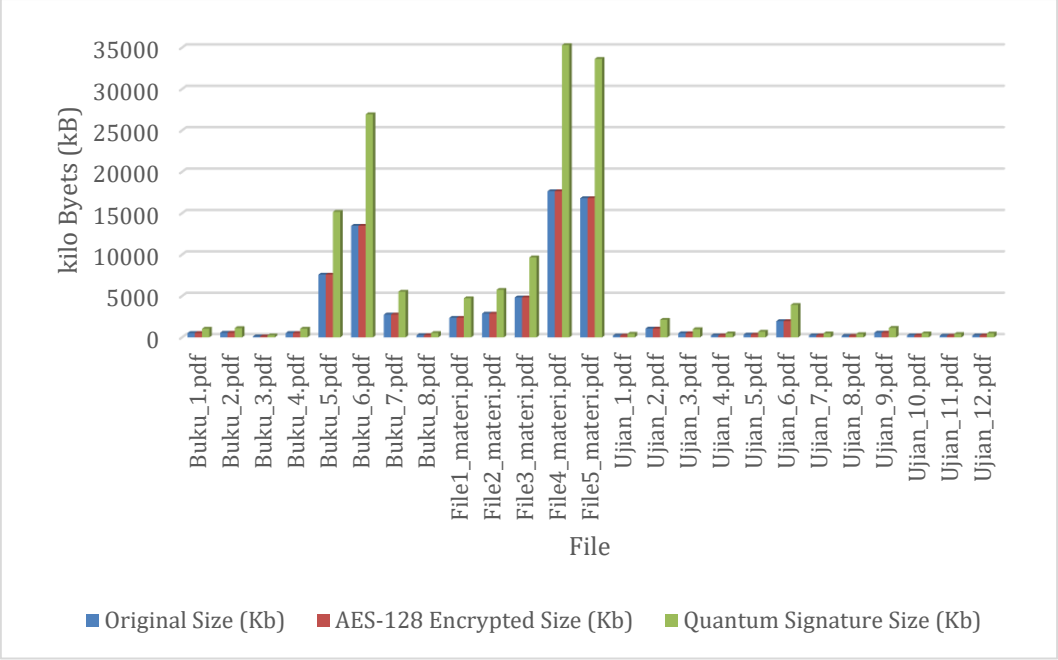

Figure 2. Comparison of PDF file size before and after encryption

In figure 2 this graph compares the size of the PDF file before to and after to encryption using AES-128, as well as the size of the digital signature generated by Quantum Signature. The investigation indicates that the file size post-AES-128 encryption is identical to the original file size. The characteristic of AES-128 symmetric encryption results in little overhead, rendering the original and encrypted file sizes equal. For instance, Book_1.pdf has an initial size of 525 KB, and the AES-128 size also stays 525 KB.

Table 1: Effect of Quantum Signature on File Size

File	Original Size (kB)	Quantum Signature Size (kB)	Change Ratio
Buku_1.pdf	525	1050	2.0x
File4_materi.pdf	17654	35308	2.0x
Ujian_9.pdf	575	1150	2.0x

In contrast, the size of digital signatures generated by Quantum Signature has increased markedly. This finding shows that the signature size is consistently equal to twice the size of the original file. For example, Book_1.pdf, which was originally 525 Kb in size, produced a signature of 1050 Kb, while File4_materials.pdf, with a size of 17654 Kb, produced a signature of 35308 Kb. This pattern uniformly holds for all the files in Table 1 Effect of Quantum Signature on File Size, showing that the Quantum Signature implementation offers better security guarantees in terms of integrity and authentication, even with a corresponding increase in file size.

This finding indicates that although AES-128 efficiently maintains file size, the implementation of Quantum Signature must account for storage capacity and bandwidth, particularly for big files. Consequently, using a combination of AES-128 and Quantum Signature ensures a high degree of security; nevertheless, the trade-off regarding the enlargement of the digital signature necessitates optimisation in system implementation.

b. AES-128 encryption time and Quantum Signature

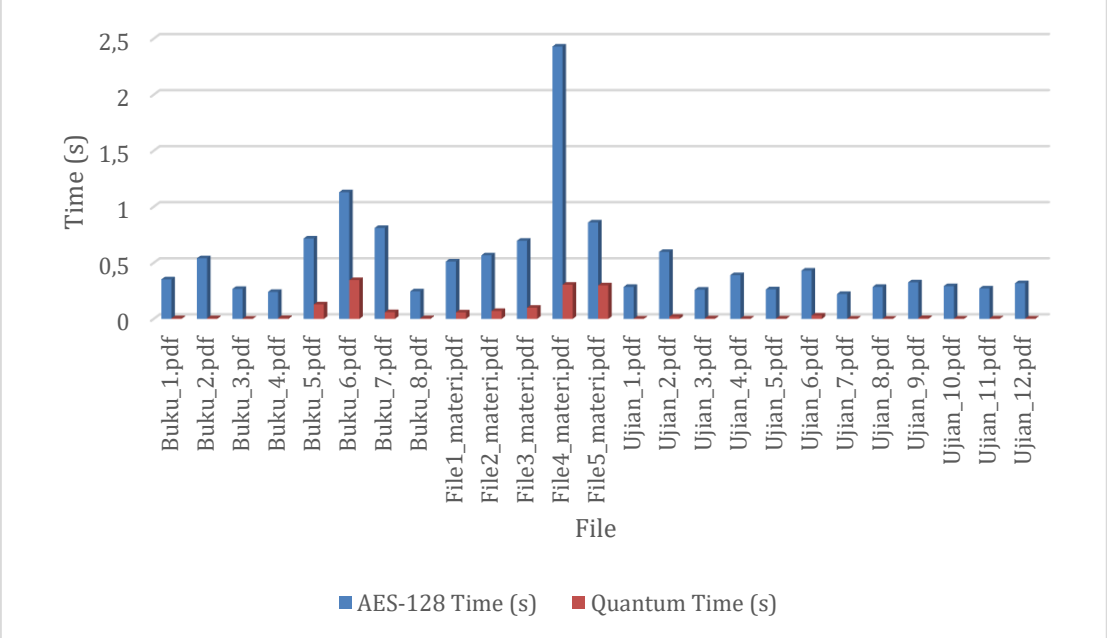

Figure 3. Encryption time comparison

Figure 3 illustrates the comparative execution times of AES-128 encryption and Quantum Signature creation for digital signatures across different PDF file sizes. The

investigation reveals a substantial disparity in the performance of the two approaches, with Quantum Signature exhibiting markedly quicker execution times than AES-128 across all file size categories. The encryption duration for AES-128 varies between 0.22 seconds and 2.42 seconds, but the signature creation time for Quantum Signature spans from 0.0016 seconds to 0.3458 seconds. The disparity is particularly obvious with tiny data, since Quantum Signature may complete the process in milliseconds, significantly outpacing AES-128.

Table 2: Time Comparison of AES-128 and Quantum Signature

File Category	Average AES-128 Time (s)	Average Quantum Time (s)	Comparison Ratio
Small Files (<1 MB)	0.28	0.003	98x faster
Medium Files (1-10 MB)	0.58	0.07	8x faster
Large Files (> 10 MB)	1.70	0.28	6x faster

It can be seen from Table 2 that this result verifies that the execution duration of AES-128 generally escalates linearly with the rise in file size. Conversely, Quantum Signature exhibits a more efficient and more stable performance despite the increase in file size. This is attributable to the characteristics of digital signature production, which relies only on the hash size of the data, rather than the whole file size. Consequently, Quantum Signature is appropriate for situations necessitating rapid signature validation, such as real-time document security or systems managing numerous files simultaneously.

Nevertheless, AES-128 encryption remains essential for preserving data secrecy via its robust and efficient symmetric encryption technique. Nonetheless, the extended execution duration relative to Quantum Signature must be considered, particularly in large-scale system deployments with constrained resources. The integration of AES-128 for data encryption with Quantum Signature for integrity verification may provide an ideal security solution, considering the equilibrium of secrecy, integrity, and temporal efficiency. Consequently, these findings provide a crucial basis for the development of more effective and robust data security solutions in the future, particularly in response to dangers posed by quantum computing technologies.

c. MiTM Attack results against AES-128 and QKD

Table 3: MiTM Attack results against aEs-128 and QKD

Trial	AES Attack Time (s)	QKD Attack Time (s)	QKD Attack Success
1	0.000062	0.000009	No
2	0.000039	0.000005	No
3	0.000032	0.000004	No
4	0.000033	0.000004	No
5	0.000033	0.000003	No
..	…	…	…
297	0.000031	0.000003	No

298	0.000034	0.000003	No
299	0.000032	0.000003	No
300	0.000031	0.000003	No

The data in Table 3 demonstrates that the outcomes of Man-in-the-Middle (MiTM) attacks on AES-128 and Quantum Key Distribution (QKD) throughout 300 trials indicate that both techniques effectively preserve their security. The attack duration for AES-128 varied between 0.000031 seconds and 0.000062 seconds, but the attack duration for QKD was more rapid, ranging from 0.000003 seconds to 0.000009 seconds. Despite the accelerated nature of the assault on QKD, the success rate for both methodologies remains at 0%, as seen by the 'No' outcome in the QKD attack success column. This indicates that QKD has an effective system for detecting tampering or manipulation attempts, allowing for the quick identification and prevention of assaults.

The reduced execution time of QKD relative to AES-128 signifies superior key validation efficiency. Nonetheless, despite the prolonged duration of attacks on AES-128, the inherent complexity of its symmetric algorithm renders it resistant to simple brute-force assaults. Consequently, both approaches demonstrated their efficacy in thwarting MiTM assaults, with QKD excelling in rapid attack detection and AES-128 effectively preserving data secrecy.

The findings affirm that the use of QKD as a major communication security measure offers enhanced protection against manipulation or interception attempts. AES-128 is still pertinent and safe for conventional data encryption; nevertheless, the impending danger posed by quantum technology underscores the need of integrating QKD to enhance security resilience. The integration of these two methodologies may provide a resilient and effective security system, adept at addressing diverse attack scenarios with enhanced performance and superior dependability.

```
AES Avg Attack Time (s): 3.462e-05
QKD Avg Attack Time (s): 3.54e-06
QKD Success Rate: 0.00%
```

Figure 4 Attack Summary

From Figure 4, the analysis results show significant differences between AES and QKD in terms of average attack time as well as attack success rate. The average attack time against AES was recorded at 3.462 × 10-⁵ seconds, while the average attack time against QKD was faster at 3.54 × 10-⁶ seconds. so that to get this value, calculations can be made with the formula Calculation of Average Attack Time The average value of attack time is calculated using the arithmetic average formula as follows:

$$Avarage = \frac{\sum_{i=1}^{n} T_i}{n}$$

Where:

T_i = Attack time on the i-th trial (in seconds).

n = Total number of trials.

$\sum_{i=1}^{n} T_i$ = Total attack time of all trials.

Value Calculation, suppose the total attack time resulting from 300 trials is as follows

AES Total Time = 0.010386 seconds (accumulated from all AES attack times)

QKD Total Time = 0.001062 seconds (accunulated from all QKD attack times)

To get the average attack time :

AES Average Time :

$$AES\ Avg\ Attack\ Time = \frac{QKD\ Total\ Time}{Number\ of\ Attempts} = \frac{0.010386}{300} = 3.462 \times 10^{-5}\ seconds$$

QKD Average Time :

$$QKD\ Avg\ Attack\ Time = \frac{QKD\ Total\ Time}{Number\ of\ Attempts} = \frac{0.001062}{300} = 3.54 \times 10^{-6}\ seconds$$

This disparity indicates that assaults on QKD can be conducted more rapidly than those against AES. It is crucial to acknowledge that the attack speed does not influence the success rate, since QKD maintains a 0% attack success rate. This signifies that the security measures of QKD are very proficient in identifying and preventing attack attempts. Conversely, while assaults on AES exhibit a comparatively brief execution duration, the intricacy of the AES symmetric encryption key continues to provide a substantial obstacle to successful attacks. The extended average attack duration relative to QKD suggests that AES-128 has a robust degree of protection against basic MiTM-based assaults.

Discussion

The findings validate that the amalgamation of AES-128 with QKD digital signatures offers a formidable safeguard against Man-in-the-Middle attacks and quantum-related vulnerabilities. AES provides rapid and safe encryption, but QKD-based signatures enhance security for data authenticity and integrity. The tampering detection technique effectively recognized unlawful alterations, showcasing the dependability of the suggested method. The results correspond with earlier research emphasizing the weaknesses of conventional cryptography systems against quantum assaults (Bernstein & Lange, 2017; Chen et al., 2016). The system attains efficiency and future-proof security by integrating symmetric encryption (AES) with quantum-resistant signatures (PQC).

Conclusion

This study demonstrates that the integration of AES-128 for data encryption and Quantum Key Distribution (QKD) for digital signatures offers a formidable security solution against Man-in-the-Middle (MiTM) attacks, including potential risks from future quantum technologies. The implementation findings demonstrate that AES-128 successfully preserves data secrecy with stable performance, however the time needed for attacks is comparatively greater than that of QKD. Conversely, QKD demonstrates superior efficacy in identifying and preventing attack attempts with much expedited validation times. In the 300 MiTM attack assessment, QKD achieved a 0% success rate for attacks, demonstrating its robustness as a prospective security system.

AES-128 incurs little cost regarding file size, but QKD produces digital signatures that may be up to double the size of the original file. Nevertheless, the substantial processing speed of QKD renders it optimal for applications necessitating real-time verification of data integrity. The integration of these two methodologies establishes equilibrium among secrecy, integrity, and temporal efficiency, making it an ideal option for safeguarding sensitive data from both traditional and quantum threats. This study validates the need of using post-quantum cryptography (PQC) and symmetric encryption algorithms like AES-128 to mitigate possible attack risks in the quantum computer future. Subsequent research may concentrate on enhancing performance and minimizing the overhead associated with digital signature size, hence facilitating more efficient implementation of these security systems on a broader scale.

References

Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2018). Quantum Attacks on Bitcoin, and How to Protect Against Them. Ledger, 3. https://doi.org/10.5195/ledger.2018.127

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST Post-Quantum Cryptography Standardization process. https://doi.org/10.6028/NIST.IR.8413-upd1

Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. Nature, 549, 188–194. https://doi.org/10.1038/nature23461

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/https://doi.org/10.6028/NIST.IR.8105

Khan, S., Palani, K., Goswami, M., Rakhimjonovna, F., Mohammed, S., & Menaga, D. (2024). Quantum Computing And Its Implications For Cyber security: A Comprehensive

Review Of Emerging Threats And Defenses. Nanotechnology Perceptions, 20, 1232–1248. https://doi.org/10.62441/nano-ntp.v20iS13.79

Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., & De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), 151–163. https://doi.org/10.1049/qtc2.12044

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., & Voznak, M. (2020). Quantum Key Distribution: A Networking Perspective. ACM Computing Surveys, 53(5). https://doi.org/10.1145/3402192

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Applied Cryptography.

Olivia Putri Irine Irawan, B., Tahir, M., Ayu Windrastuti, N., Yurina Cholili, D., Mulaikah, D., Batsul Mushofi Septian wachid, A., & Pendidikan Informatika, P. (2023). Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma Advance Encryption Standard (AES) Cryptographic Implementation In Data Security Using Advanced Encryption Standard (AES) Algorithm. 11(2).

Peikert, C. (2016). A Decade of Lattice Cryptography. Foundations and Trends® in Theoretical Computer Science, 10, 283–424. https://doi.org/10.1561/0400000074

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

Shim, K.-A. (2022). A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communications. IEEE Transactions on Intelligent Transportation Systems, 23(9), 14025–14042. https://doi.org/10.1109/TITS.2021.3131668

Stallings, William. (2017). Cryptography and network security : principles and practice. Pearson Education Limited.