International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 11, No. 3, 2024, pp. 1-4.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Integration of Key Distribution and Cryptographic Technique to Achieve Quantum-resistant Authenticated Key Exchange in Transport Layer Security

Dr. Linda Okoro [a], Carlos Gutierrez [b]

[a] *University of Lagos, Nigeria.*
[b] *University of Lagos, Nigeria.*

Abstract

The latest breakthroughs in quantum computing (QC) have made building secured and effective authorization systems against QC threats more imperative. Quantum key dissemination (KD) and post-quantum cryptographic techniques (PQCT) are pioneering security innovations that enable transmissions to withstand QC attacks. To realize quantum-resistant authenticated key exchange (QRAKE), the above-stated methods must be integrated into a Transport Layer Security (TLS). This study presented and implemented two innovative hybrid techniques integrating KD and PQCT inside TLS to achieve QRAKE: Concatenation and Exclusive-OR (XOR). The Integrated Quantum KD and PQCT-master concealment setup is the most time-consuming configuration, reaching 203 ms. This is mainly due to high times of Credential (40 ms), Server Key Transfer (12 ms), Client Key Transfer (10 ms) and End (120 ms). This serves as an indication of the trade-off present between the security of the cryptographic structure and the efficiency of the protocol.

Keywords: Quantum Computing, Key Dissemination, Cryptographic Techniques, Quantum-resistant, Authentication, Key Exchange, Transport Layer Security.

DOI: 10.71086/IAJSE/V11I3/IAJSE1151
Received: 10 June 2024/Revised: 15 July 2024/Accepted: 16 August 2024/Published: 30 September 2024

Introduction

Quantum-resistant (QR) connectivity has arisen as a countermeasure to the danger QC poses to public key cryptography (PKC) fundamentals. TLS is an online safety protocol that necessitates the shift to QR encryption. TLS is frequently employed as the predominant client-server protocol for protecting internet connections and is continuously recommended for safeguarding the network control and administration layers in future 6G networks (Ristov & Koceski, 2023).

TLS is a network privacy protocol that provides safe ways to communicate over the web between two interacting apps. TLS may be implemented atop any system, offering an encryption layer that enables clients and servers to interact while preventing spying, manipulation, or message forging, preserving privacy and data fidelity between the apps (Rescorla, 2018). TLS fundamentally operates atop a dependable protocol, the Transmission Control Protocol (TCP). The encrypted channel provided by TLS must deliver:

• Authentication: The identities for connecting peers must be validated before establishing communication. The server end of the communication must consistently undergo authentication. Client-side verification is discretionary.

• Privacy: Information sent over the safe channel has been secured and must be accessible to the authorized terminals of the connection.

• Integrity: Information sent across the channel, even when protected, cannot be altered or changed by an unauthorized intruder without detection by both ends, ensuring the data stays correct, whole, and reliable during transfer.

The TLS communication has two separate layers: the TLS Handshake and the TLS Session layers [3]. The recent development of PQCT raises worries about its development and the prospect of future cryptanalytic assaults that might compromise algorithms now deemed safe. Authors in (Paquin et al., 2020) introduced an integrated classical-PQ approach for protecting TLS transactions in a simulated network environment created using the Linux kernel. The combined PQ approach was executed using liboqs. Their research established that the finishing length of the TLS interaction was mostly influenced by the expenses associated with both conventional and PQCT.

Authors in (Giron et al., 2023) proposed a framework for combining several cryptographic approaches, namely conventional, PQCT, and quantum KD, to provide quantum-secure composite key transfers. This study emphasized the need to develop QR procedures to safeguard against serious errors and prospective cryptanalytic assaults. In contrast to the approach, Dowling et al. conducted tests using simulated Quantum KD devices and did not include their authorized key exchange concept into a network interface like TLS.

Authors in (Huang et al., 2020) elucidated a theoretical framework for amalgamating conventional and PQCT with KD inside an internet protocol, thus attaining hybridized 'triple-security.' The paper suggested using the IPsec or TLS approach to get QR communications. Nonetheless, there were no findings or analyses on handshake efficiency or transaction size, nor were any actual implementations of the abovementioned protocols disclosed.

Proposed method

Quantum KD and PQCT are cryptographic methods that tackle distinct difficulties. PQCT addresses authorization and key transfer with various QR algorithms, while Quantum KD is only designed for QR key transfer. This study, shown in Fig. 1, presents the following technique: Utilize PQCT for authorization and employ both PQCT and Quantum KD for the QRAKE. To enhance the mechanism against "generate now, decipher subsequent assaults," specifically concerning the transfer of keys, we suggest and examine an innovative method for integrating Quantum KD and PQCT during the TLS-QRAKE stage. The union method is used at the premaster concealed layer, and the XOR method is used at the uppermost concealed layer.

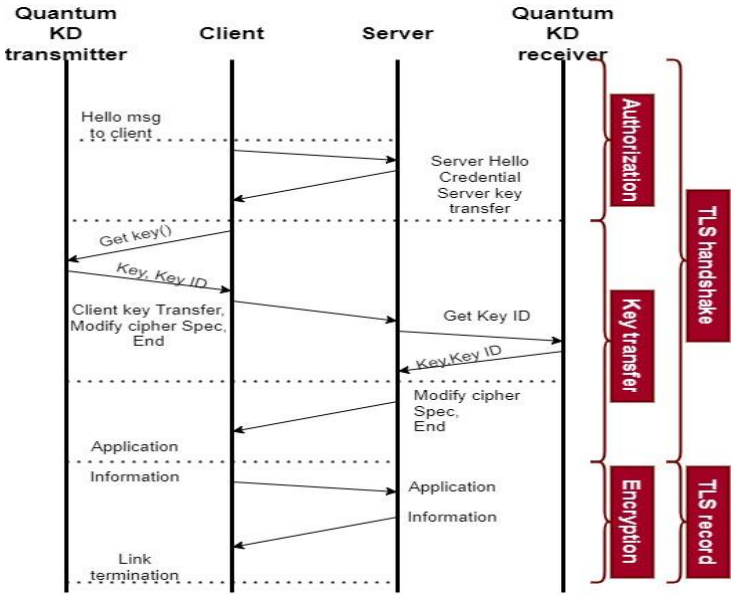

Fig. 1: Hybrid techniques that integrate KD and PQCT inside TLS to achieve QRAKE

PQCT is the initial QR authorization method sufficiently developed to be regarded as a viable option for providing authorization in the TLS interaction. During the TLS handshake, the server employed Dilithium to verify its transitory public key. It has been employed on the client end to check the digital sign on the server's credentials and the validity of the server's transitory public key. Concerning the QRAKE, we elucidate the two primary processes through which we propose the integration of Quantum KD and other PQCT algorithms to enhance QC safety. We also delineate how additional cryptographic algorithms for key transfer might be further incorporated into the framework. Upon completing the Quantum KD key recovery procedure by both sides and generating a joint secret, according to PQCT, the client and server will possess two distinct secrets derived from disparate encryption principles. In the suggested composite QR-based TLS design, quantum-based encryption keys may be used in many ways.

In this context, every hybrid key transfer option is considered a distinct, novel key transfer technique. In this setting, composite key transfer has been defined as implementing multiple key transfer methods based on distinct encryption presumptions, exemplified by the integration of Quantum KD and PQCT. The primary impetus for employing hybrid key transfer methods is to enable early Quantum KD or PQCT supporters to integrate these QR processes into networked devices, ensuring safety over time for the cryptographic methods remains intact.

To implement a mixed key transfer, PQCT-based processes should integrate QR algorithms with PQCT-based QR algorithms, which are relatively novel and have not undergone the same level of scrutiny as established pre-quantum algorithms. Thus, any prospective algorithmic advancement that jeopardizes the safety of PQCT methods may not completely erode the system's safety but would impact the privacy implications established by PQCT. The present approach incorporates Quantum KD with PQCT for validated key transfer, achieving hybrid QR via two distinct QR cryptographic principles.

In the outlined circumstance, when the client authenticates the server's self-identity, it initiates interaction with the relevant Quantum KD node by soliciting a key. Upon acquiring a Quantum KD-based key and a PQCT-based key, the 16-bit sequences are combined to create the quantum-hybrid premaster concealment. The client-side key transfer must include both the ciphertext produced by CRYSTALS-Kyber and the key ID necessary for Quantum KD. This communication may be employed on the server's end to acquire the Quantum KD-based and PQCT-based keys, hence enabling the derivation of the identical quantum-hybrid premaster concealment. This may be used to get the same QR master concealment on both ends and extract the requisite session key information.

Results

The primary reason for this work is to promote the adoption of QRAKE substitutes for TLS; however, performance remains a crucial consideration in practical networking applications. Therefore, it is essential to assess the efficacy of integrating QRAKE into TLS from an efficiency standpoint. A performance assessment of Quantum KD and PQCT about conventional cryptography has been undertaken.

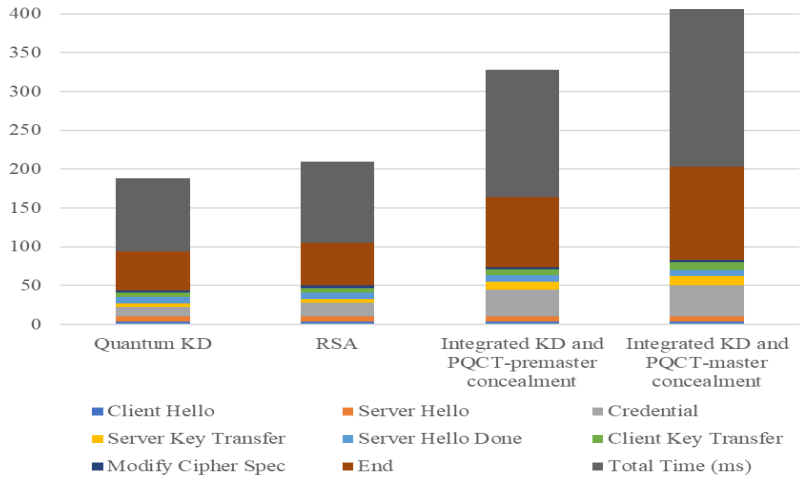

Fig. 2 Performance assessment of Quantum KD and PQCT concerning conventional cryptographic methods

As seen in Fig. 2, there is a comparative assessment of different cryptographic configurations based on the time, in ms, taken at each step of the protocol. Among the configurations, Quantum KD had the least total time of 94 ms, making it the most time-efficient. It also had lower times in key milestones such as Credential (12 ms) and End (50 ms). Conventional RSA showed a total time that is slightly higher than that of Quantum KD at 105 ms. This increase in total time is due to a greater Credential time of 18 ms and an End time of 55 ms. The Integrated KD and PQCT-premaster concealment setup, on the other hand, is more secure and, thus, takes considerably longer at a total of 164 ms mainly due to higher Credential (35 ms), Server Key Transfer (10 ms) and End (90 ms) times. The Integrated Quantum KD and PQCT-master concealment setup is the most time-consuming configuration, reaching 203 ms. This is mainly due to high times of Credential (40 ms), Server Key Transfer (12 ms), Client Key Transfer (10 ms) and End (120 ms). This serves as an indication of the trade-off present between the security of the cryptographic structure and the efficiency of the protocol.

Conclusion

This work introduced and executed two novel hybrid strategies that amalgamate KD and PQCT inside TLS to realize QRAKE: Concatenation and Exclusive-OR (XOR). The Integrated Quantum KD with PQCT-master concealing arrangement is the most time-intensive, requiring 203 ms. This is primarily attributable to prolonged durations of Credential (40 ms), Server Key Transfer (12 ms), Client Key Transfer (10 ms), and End (120 ms). This indicates the trade-off between the security of the cryptographic framework and the efficiency of the protocol.

References

Ristov, R., & Koceski, S. (2023, June). Quantum resilient public key cryptography in internet of things. In *2023 12th Mediterranean conference on embedded computing (MECO)* (pp. 1-4). IEEE. https://doi.org/10.1109/MECO58584.2023.10154994

Rescorla, E. (2018). *The transport layer security (TLS) protocol version 1.3* (No. rfc8446).

Lohachab, A., Lohachab, A., & Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet of Things*, *9*, 100174. https://doi.org/10.1016/j.iot.2020.100174

Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11* (pp. 72-91). Springer International Publishing. https://doi.org/10.1007/978-3-030-44223-1_5

Giron, A. A., Custódio, R., & Rodríguez-Henríquez, F. (2023). Post-quantum hybrid key exchange: a systematic mapping study. *Journal of Cryptographic Engineering*, *13*(1), 71-88. https://doi.org/10.1007/s13389-022-00288-9

Huang, L., Feng, K., & Xie, C. (2020, September). A practical hybrid quantum-safe cryptographic scheme between data centers. In *Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro-and Nanosystems in Security and Defence III* (Vol. 11540, pp. 30-35). SPIE. https://doi.org/10.1117/12.2573558