Hybrid Post-Quantum Cryptography in Network Protocols

Alexandre Augusto Giron[1,2], **Ricardo Custódio**[2]

[1]Universidade Tecnológica Federal do Paraná (UTFPR) – Toledo – PR – Brazil

[2]Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina (UFSC) – Florianópolis, SC – Brazil

alexandregiron@utfpr.edu.br, ricardo.custodio@ufsc.br

Abstract. *The advent of quantum computing presents a significant threat to the security of modern communication systems that depend on public-key cryptography. This work provides a comprehensive overview of a thesis that explores the integration of Post-Quantum Cryptography (PQC) within the Transport Layer Security (TLS) protocol and the Automatic Certificate Management Environment (ACME). We assess the feasibility and performance implications of PQC in various network environments, focusing on the hybrid mode approach as a strategic pathway for PQC adoption. Our research aims to develop practical solutions to mitigate the quantum threat while ensuring the integrity and reliability of critical internet protocols.*

1. Introduction

Public-key cryptography is foundational to modern digital security, underpinning countless online services and applications. Implementing Public Key Infrastructure (PKI) enables secure communication, authentication, and data integrity. Without PKI, the secure operation of the Internet as we know it would be virtually impossible. Key use cases for public-key cryptography include authentication and the distribution of symmetric encryption keys.

The widespread adoption of public-key cryptography, relying on algorithms such as RSA and Diffie-Hellman, is at risk due to the impending threat of quantum computing. As demonstrated by Shor's algorithm [Shor 1994], these cryptographic schemes are vulnerable to attacks from sufficiently powerful quantum computers. Consequently, the confidentiality and integrity of systems reliant on these algorithms will be compromised once quantum computing reaches a critical threshold. This necessitates a proactive approach to developing and deploying post-quantum cryptography to safeguard digital infrastructure.

The threat of record-now-decrypt-later attacks significantly exacerbates the urgency for robust solutions to the problem of data security. In this scenario, malicious actors intercept and store encrypted data transmitted over the internet, intending to decrypt it using future quantum computing capabilities. While current encryption methods protect data in transit, they offer no safeguard against this delayed decryption. As a result, the widespread reliance on Transport Layer Security (TLS) no longer guarantees the confidentiality of communications. In essence, today's encrypted data could be compromised by tomorrow's technology.

To address the threat of quantum computing, researchers are investigating Post-Quantum Cryptography (PQC) [Bernstein and Lange 2017]. PQC relies on mathematical problems that are computationally intractable for both classical and quantum computers. The goal is to protect traditional computer systems from potential attacks by quantum computers. A global transition from traditional to PQC-based cryptography is therefore being considered.

The transition to PQC presents significant challenges. Due to the nascent nature of PQC, a hybrid approach combining established and post-quantum algorithms is often recommended. This requires careful design considerations and analysis of performance and network protocol implications. For digital signatures, a hybrid scheme involves signing with both a traditional and a post-quantum algorithm. Symmetric key exchange mechanisms can concatenate outputs from both algorithms to derive the final key. This hybrid strategy provides a layer of protection, ensuring security even if one of the algorithms is compromised by quantum computing.

A primary challenge in adopting PQC, regardless of whether a hybrid or pure approach is chosen, is the increased size of cryptographic objects. This directly impacts the performance of network communication protocols. Consequently, a thorough evaluation of the transition to PQC is crucial to understand the performance implications and necessary adjustments across the complex landscape of internet protocols.

HTTPS, the foundation of secure internet communication, relies on the Transport Layer Security (TLS) protocol [Rescorla 2018]. TLS is further strengthened by the Automated Certificate Management Environment (ACME) protocol [Barnes et al. 2019], which simplifies the management of security certificates. Together, these protocols form a critical infrastructure for enabling secure internet connections.

2. Objectives

This paper summarizes the thesis focused on accelerating the adoption of hybrid Post-Quantum Cryptography (PQC) within network protocols. To achieve this, the research proposes, implements, and evaluates PQC solutions and transition strategies, encompassing both hybrid and non-hybrid scenarios. Specific objectives include:

- Identifying the key challenges associated with integrating hybrid PQC into network protocols;
- Developing and testing mitigation strategies for these challenges through simulations and real-world experiments;
- Contributing to broader awareness of the quantum computing threat, the complexities of PQC adoption, and potential solutions.

3. Methodology

This research leverages PQC algorithms selected as finalists in the NIST-PQC standardization process [NIST 2024]. Given its prominence in the field, this process provides a robust foundation for evaluating potential PQC solutions. Among the chosen algorithms, Dilithium (as the primary focus), Falcon, and SPHINCS+ have been selected for digital signature schemes, while Kyber, standardized as a Key Encapsulation Mechanism (KEM), will be utilized for key establishment. It is essential to acknowledge that the NIST standardization process is ongoing. This underscores the necessity for in-depth research to facilitate a smooth and efficient transition to PQC within real-world applications.

Research on PQC adoption primarily focuses on two areas: benchmarking and protocol modification. Benchmarking studies, such as Paquin et al.'s work [Paquin et al. 2020], compare the performance of protocols with and without PQC. Protocol modifications aim to better integrate PQC, like KEMTLS [Schwabe et al. 2020] which replaces TLS signatures with KEMs due to their smaller size. Given the criticality of TLS and ACME and their imminent need for PQC, this work evaluates the performance of various PQC integration strategies within these protocols.

4. Main Contributions

This work focuses on evaluating and proposing network protocols incorporating PQC, particularly in the hybrid mode. Our primary contributions are as follows:

- **Systematic Mapping Study:** We conducted a rigorous Systematic Mapping Study (SMS) [Petersen et al. 2015] to classify and understand hybrid key exchange mechanisms. This study identifies research gaps for both newcomers and experts in the field;
- **PQC Awareness Tool:** We developed an application to inform users about the use of PQC algorithms (hybrid or not) in TLS 1.3 connections, raising awareness of quantum threats;
- **Hybrid Mode Implementations:** We implemented the hybrid mode for TLS connections and ACME certificate issuance, addressing gaps in existing research and providing practical examples;
- **Innovative Hybrid Property:** We introduced a novel property for hybrid post-quantum authentication, enhancing hybrid resilience by addressing the lack of contingency.

Our initial contribution is a Systematic Literature Mapping (SLM) of hybrid key exchange (KEX) mechanisms [Giron et al. 2023a]. This SLM categorizes hybrid approaches and pinpoints open research challenges, aiding researchers, designers, and developers in exploring this field.

This work developed the TLS 1.3 Handshake Analyzer [Giron et al. 2022], a tool addressing the scarcity of tools capable of assessing PQC in TLS 1.3. By identifying PQC algorithms (hybrid or otherwise) in TLS 1.3 connections, the analyzer enhances user awareness of PQC. It further provides performance metrics through a web interface and detects vulnerable ciphersuites.

While ACME is a cornerstone of internet security, its performance in a post-quantum world remains largely unexplored. This work evaluates the implications of using Post-Quantum Cryptography (PQC) for certificate issuance and renewal within the ACME protocol. Our findings indicate that adopting PQC significantly increases resource consumption on the ACME server, leading to a reduced rate of certificate requests processed. However, the impact on clients is less pronounced.

To expedite certificate issuance during the transition to PQC, we introduce a novel ACME challenge mechanism termed the PQ-Transition Challenge. Our evaluation demonstrates that this approach accelerates certificate issuance by an average of 4.22 times while decreasing data transfer by up to 35%. Notably, the performance overhead of employing a hybrid cryptographic mode is minimal, particularly for ACME clients, making it a practical solution for widespread adoption.

KEMTLS offers a post-quantum alternative to TLS by replacing digital signatures with Key Encapsulation Mechanisms (KEMs) for handshake authentication. However, the performance implications of hybrid KEMTLS, combining classical and post-quantum cryptography, remain largely unexplored. This work presents a comprehensive evaluation of hybrid KEMTLS, encompassing diverse post-quantum algorithms and real-world network conditions. Our proposed hybrid KEMTLS design demonstrates negligible performance overhead compared to traditional TLS, fostering practical adoption. Moreover, hybrid KEMTLS outperforms TLS with hybrid post-quantum signatures at lower NIST security levels, but the performance gap widens at higher levels, suggesting a trade-off between security and efficiency.

This work also addresses a critical oversight in hybrid cryptography: the absence of a robust contingency plan. Should a vulnerability be discovered in the post-quantum component, the hybrid system would retain classical security but lose its post-quantum resistance. To mitigate this risk, we introduce PKI Extended Lifetime Period (PKIELP), a novel approach to hybrid post-quantum authentication. PKIELP employs "wrapped certificates" to encrypt the public key, preventing quantum adversaries from extracting the classical private key. Our proposal significantly reduces the byte overhead of post-quantum authentication compared to NIST-selected algorithms. This reduction in certificate size is expected to enhance TLS connection performance and bolster the overall security properties of hybrid systems.

In summary, this work presents several groundbreaking contributions:

- **Pioneering Hybrid KEMTLS Evaluation:** We conducted the first comprehensive evaluation of hybrid KEMTLS, quantifying performance overhead through extensive experimentation;
- **Optimizing ACME for Hybrid PQC:** We introduced a novel ACME protocol modification that accelerates certificate issuance and reduces data transfer by 35% when using hybrid post-quantum cryptography;
- **Developing PKIELP for Hybrid Resilience:** We proposed PKIELP, a quantum-safe contingency mechanism for hybrid systems that also reduces communication overhead compared to other post-quantum approaches.

5. Integration and Interdisciplinary Nature

Beyond its contributions to post-quantum cryptography, this work intersects with broader computer security research. By incorporating related topics, we foster collaboration with other researchers in the field and gain a holistic understanding of the challenges and opportunities within the computer security landscape.

The additional contributions of this work are divided into two parts. The first part summarizes the collaborations (with other researchers), both in the adoption of post-quantum cryptography in protocols involved in digital identity management (such as OpenID Connect) [Schardong et al. 2022], and in the analysis of substitution attacks on post-quantum algorithms [Marchiori et al. 2021].

The second part of the additional contributions showcases the additional contributions of this work. Two publications are related to proposing and practically evaluating a mechanism for detecting unauthorized use of steganography in blockchains

[Giron et al. 2020, Giron et al. 2021]. This work was the first to analyze Bitcoin and Ethereum blockchains in the search for steganographic evidence. Steganography deals with hiding communications from the observer. Steganography can be particularly worrisome for public blockchains since the hidden communication data is shared with all network participants without consent.

Finally, this work also included a mechanism for aiding random number generation in Internet-of-Things (IoT) devices as the last additional contribution [Giron and Custódio 2020]. The proposal is based on Bluetooth but could be used with other wireless technologies. Since trusting a single source of random numbers is a security concern, the proposal allows adding a second source, given that other devices are nearby (within the Bluetooth range).

6. List of Publications

Table 1 presents the publications produced during this four-year Ph.D. program at UFSC. To reflect the program's duration, the table includes works from 2020 to 2023. The publications encompass a range of formats, including research papers, posters, workshops, and position papers, to demonstrate the breadth of research conducted. It is important to note that an additional paper related to the thesis was published after the Ph.D. defense and is not included in this list [Giron et al. 2024].

Tabela 1. List of Publications. ID Labels indicate the following: P = publications described in this work; C = collaborations with other authors; A = additional contributions from this Ph.D. research.

ID	Reference	Research Topic	Type of Contribution	Year	Venue
P1	[Giron et al. 2023a]	Post-Quantum Crypto.	Regular Paper	2023	Journal (JCEN)
P2	[Giron 2023]	Post-Quantum Crypto.	Position Paper	2023	SECrypt
P3	[Giron et al. 2023b]	Post-Quantum Crypto.	Regular Paper	2023	LatinCrypt
P4	[Giron et al. 2022]	Post-Quantum Crypto.	Workshop Paper	2022	SBSeg-SF
P5	[Giron 2021]	Post-Quantum Crypto.	Ph.D. Poster Paper	2021	SecureComm
C1	[Schardong et al. 2022]	Post-Quantum Crypto.	Regular Paper	2022	CANS
C2	[Marchiori et al. 2021]	Post-Quantum Crypto.	Regular Paper	2021	SBSeg
A1	[Giron et al. 2021]	Steganography	Regular Paper	2021	Journal (Sensors)
A2	[Giron et al. 2020]	Steganography	Workshop Paper	2020	AIBlock
A3	[Giron and Custódio 2020]	IoT Security	Regular Paper	2020	SBSeg

7. Conclusions

The transition from traditional cryptographic systems to post-quantum cryptography is crucial for mitigating the emerging threats posed by quantum computers. This work addressed the challenges inherent in implementing hybrid PQC systems, focusing specifically on the TLS and ACME protocols.

Our research explored various proposals to facilitate the adoption of hybrid PQC. This investigation was essential in understanding the potential impacts and raising early awareness. Additionally, the studies contributed to comprehending alternative PQC adoption strategies, both hybrid and non-hybrid, with the protocol modifications implemented in this work yielding improved performance indicators. As a result, this early analysis enables the evaluation of protective scenarios and the selection of optimal approaches before quantum computing becomes a widespread reality.

Despite recommending a hybrid approach based on our findings, it is important to recognize that the migration to PQC will still face significant challenges in the future. Our experience with the TLS and ACME protocols revealed that certain scenarios might still be vulnerable to quantum attacks, even after migrating to PQC. Specifically, this work identified a risk where a "record-now-decrypt-later" strategy could exploit a reused certificate issuance authorization in ACME. Therefore, long-term information captured today and decrypted in the future could enable unauthorized interactions with the protocol. Such risks imposed by quantum computers were discussed in a position paper [Giron 2023].

This research showed that simply replacing algorithms within an application's security infrastructure is insufficient. A complete migration to the post-quantum era requires a comprehensive protocol analysis, including a risk assessment based on the sensitive information managed by the protocol or application. While this study focused on protocol and hybrid PQC usage, a thorough risk analysis of the type of application data being transferred remains a potential future work. Nonetheless, PQC is fundamental for equipping internet applications to withstand better the potential threats posed by quantum computers.

Thesis availability

The thesis is available for download at the following link: `https://repositorio.ufsc.br/handle/123456789/251847`.

Acknowledgements

Author 1 gives special thanks to Dr. Ricardo Custódio, to the Federal University of Technology - Parana (UTFPR/Brazil) and the Technology Innovation Institute (TII/UAE) for their support during this work. Author 1 also thanks to the "Fundação Araucária" for the support in this submission.

Referências

Barnes, R., Hoffman-Andrews, J., McCarney, D., and Kasten, J. (2019). Automatic certificate management environment (acme). RFC 8555, RFC Editor.

Bernstein, D. J. and Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671):188–194.

Giron, A. and Custódio, R. (2020). An entropy source based on the bluetooth received signal strength indicator. In *Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 106–118, Porto Alegre, RS, Brasil. SBC.

Giron, A., Schardong, F., and Custódio, R. (2022). Tls 1.3 handshake analyzer. In *Anais Estendidos do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 63–70, Porto Alegre, RS, Brasil. SBC.

Giron, A. A. (2021). Encouraging the adoption of post-quantum hybrid key exchange in network security. In Garcia-Alfaro, J., Li, S., Poovendran, R., Debar, H., and Yung, M., editors, *Security and Privacy in Communication Networks*, pages 363–371, Cham. Springer International Publishing.

Giron, A. A. (2023). Migrating applications to post-quantum cryptography: Beyond algorithm replacement. Cryptology ePrint Archive, Paper 2023/709. `https://eprint.iacr.org/2023/709`.

Giron, A. A., Custódio, R., and Rodríguez-Henríquez, F. (2023a). Post-quantum hybrid key exchange: a systematic mapping study. *Journal of Cryptographic Engineering*, 13(1):71–88.

Giron, A. A., do Nascimento, J. P. A., Custódio, R., Perin, L. P., and Mateu, V. (2023b). Post-quantum hybrid kemtls performance in simulated and real network environments. In Aly, A. and Tibouchi, M., editors, *Progress in Cryptology – LATINCRYPT 2023*, pages 293–312, Cham. Springer Nature Switzerland.

Giron, A. A., Martina, J. E., and Custódio, R. (2020). Bitcoin blockchain steganographic analysis. In Zhou, J., Conti, M., Ahmed, C. M., Au, M. H., Batina, L., Li, Z., Lin, J., Losiouk, E., Luo, B., Majumdar, S., Meng, W., Ochoa, M., Picek, S., Portokalidis, G., Wang, C., and Zhang, K., editors, *Applied Cryptography and Network Security Workshops*, pages 41–57, Cham. Springer International Publishing.

Giron, A. A., Martina, J. E., and Custódio, R. (2021). Steganographic analysis of blockchains. *Sensors*, 21(12).

Giron, A. A., Schardong, F., Perin, L. P., Custódio, R., Valle, V., and Mateu, V. (2024). Automated issuance of post-quantum certificates: A new challenge. In Pöpper, C. and Batina, L., editors, *Applied Cryptography and Network Security*, pages 3–23, Cham. Springer Nature Switzerland.

Marchiori, D., Giron, A., Nascimento, J. P., and Custódio, R. (2021). Timing analysis of algorithm substitution attacks in a post-quantum tls protocol. In *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 127–140, Porto Alegre, Brazil. SBC.

NIST (2024). Post-quantum cryptography. National Institute of Standards and Technology. Accessed: 2024-08-13.

Paquin, C., Stebila, D., and Tamvada, G. (2020). Benchmarking post-quantum cryptography in tls. In Ding, J. and Tillich, J.-P., editors, *Post-Quantum Cryptography*, pages 72–91, Cham. Springer International Publishing.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64:1–18.

Rescorla, E. (2018). The transport layer security (tls) protocol version 1.3. RFC 8446, RFC Editor.

Schardong, F., Giron, A. A., Müller, F. L., and Custódio, R. (2022). Post-quantum electronic identity: Adapting openid connect and oauth 2.0 to the post-quantum era. In Beresford, A. R., Patra, A., and Bellini, E., editors, *Cryptology and Network Security*, pages 371–390, Cham. Springer International Publishing.

Schwabe, P., Stebila, D., and Wiggers, T. (2020). Post-quantum tls without handshake signatures. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 1461–1480, New York, NY, USA. ACM.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee.