

Measuring Post-Quantum TLS Adoption in Brazil

Jhonatan Jauja Ccana, Eder John Scheid

¹Informatics Institute (INF) – Federal University of Rio Grande do Sul (UFRGS)
Porto Alegre, RS, Brazil

{jjccana,ejscheid}@inf.ufrgs.br

Abstract. *The emergence of large-scale quantum computing threatens widely deployed public-key cryptographic algorithms used to secure Internet communications, including those employed by the Transport Layer Security (TLS) protocol. Consequently, Post-Quantum Cryptography (PQC) is being progressively incorporated into TLS, particularly through hybrid key exchange mechanisms that combine classical and post-quantum algorithms. However, the actual adoption of these mechanisms across Internet services remains insufficiently characterized, especially in emerging and regional contexts. This paper addresses this gap through a measurement study of post-quantum TLS key exchange adoption among Brazilian Internet services. We analyze the top-10,000 ranked .br domains from the Tranco list, actively probing each service to identify the negotiated TLS version and key exchange group. Our results show that TLS 1.3 is already predominant, accounting for 87.3% of the measured HTTPS services with a valid TLS version, and that 4,697 of the 8,697 services with a valid key exchange group (54.0%) negotiated a post-quantum or hybrid mechanism. This adoption is highly concentrated in a single group, X25519MLKEM768, which accounts for 98.5% of the observed PQC negotiations. These findings indicate that post-quantum or hybrid key exchange mechanisms have already reached a significant deployment scale among Brazilian Internet services.*

1. Introduction

Quantum computing introduces a computational model with capabilities fundamentally different from conventional computers [Nielsen and Chuang 2010]. Shor’s algorithm can efficiently solve integer factorization on sufficiently large fault-tolerant quantum computers, threatening widely deployed public-key systems such as RSA [Shor 1994], while Grover’s algorithm provides a quadratic speedup for unstructured search, reducing the effective security of symmetric primitives without fundamentally compromising them [Grover 1996].

Public-key cryptography underlies core network protocols such as TLS, VPNs, and digital certificates [Schmeh 2006]. The gradual migration to Post-Quantum Cryptography (PQC) [Bavdekar et al. 2023] is not only a response to future quantum capabilities. It is also driven by the Harvest-Now, Decrypt-Later threat: traffic intercepted today could be decrypted once large-scale quantum computers exist [Kagai et al. 2025]. In response, post-quantum mechanisms have been actively investigated for TLS 1.3, with prior work evaluating their feasibility and performance overhead under controlled and realistic network conditions [Sikeridis et al. 2020, Kampanakis and Childs-Klein 2024]. However, the extent to which this deployment has propagated across live Internet services, as

opposed to being merely supported at the implementation level, remains largely uncharacterized in emerging and regional Internet ecosystems, where infrastructure providers and update cycles may differ substantially from those studied in prior global-scale measurements. Brazil constitutes a relevant case study given the scale of its national domain space and its reliance on both global Content Delivery Networks (CDNs) and locally operated hosting infrastructure.

This paper addresses this gap through an active measurement study of post-quantum TLS key exchange adoption among Brazilian `.br` domains, analyzing the top-10,000 ranked `.br` domains from the Tranco list [Le Pochat et al. 2019] and characterizing the resulting adoption patterns, including the concentration of post-quantum negotiations around a small set of key exchange groups.

2. Background and Related Work

PQC encompasses cryptographic algorithms designed to resist attacks from both classical and quantum computers [Bavdekar et al. 2023]. NIST has standardized ML-KEM for key establishment [NIST 2024b], together with ML-DSA and SLH-DSA for digital signatures [NIST 2024a, NIST 2024c]. ML-KEM underlies the post-quantum and hybrid key exchange mechanisms measured in this work. RFC 10024 standardizes hybrid TLS 1.3 groups combining ML-KEM with classical elliptic-curve key exchange, including X25519MLKEM768 and SecP256r1MLKEM768 [Kwiatkowski et al. 2026]. Hybrid key exchange provides a practical migration path by retaining a classical component alongside a post-quantum mechanism.

Prior work has investigated the integration of PQC into TLS 1.3 and its performance overhead [Sikeridis et al. 2020, Kampanakis and Childs-Klein 2024], evaluating feasibility and performance under experimental conditions rather than characterizing deployment across a large population of live Internet services. Complementary active Internet measurement studies, combining large domain datasets with automated probing, have characterized the deployment of network and security technologies at scale, such as DNS provider concentration [Azevedo et al. 2024] and SSL/TLS certificate authority centralization [Azevedo et al. 2025]. To the best of our knowledge, no prior study has measured post-quantum TLS key exchange adoption in the Brazilian `.br` domain space.

3. Methodology

This study follows an active Internet measurement approach as depicted in Figure 1.

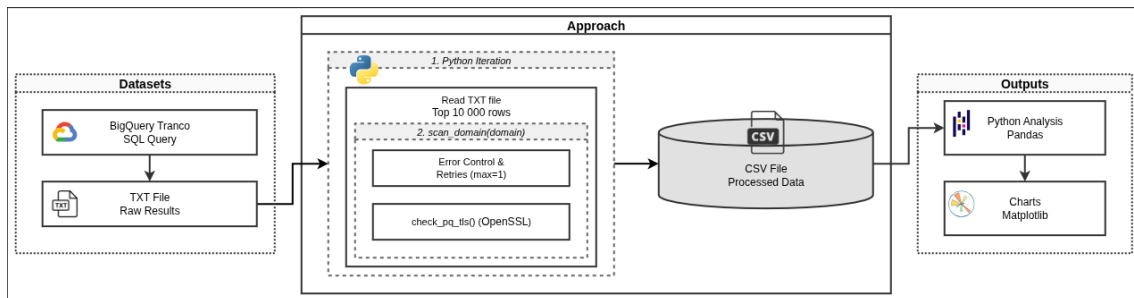


Figure 1. Overview of the measurement pipeline

3.1. Dataset Extraction

The domain population was obtained from the Tranco list [Le Pochat et al. 2019], chosen for its stability and reproducibility in Internet measurement studies, using the daily list generated on August 25, 2026. Domains under the Brazilian country-code top-level domain (`.br`) were filtered from the full ranking, and the top-10,000 ranked `.br` domains were selected to provide a manageable, high-ranked dataset for active measurement. Unlike a random sample drawn from a larger population, this selection is a deterministic top- K cut over an ordered ranking; consequently, the resulting dataset reflects the highest-ranked `.br` domains according to Tranco’s ranking methodology, rather than a population-representative random sample, and no sampling margin of error applies to the reported figures. The extracted domain list was exported as a plain-text file for processing.

3.2. Active TLS Measurement

The measurement pipeline was implemented in Python 3.15.0rc1 with OpenSSL 3.5.7. Each domain was processed sequentially by a `scan_domain` routine, which invokes `check_pq_tls` to establish TLS connections and record the negotiated protocol version and key exchange group. The client was configured with an ordered list of post-quantum groups (i.e., MLKEM512, MLKEM768, MLKEM1024), hybrid groups (SecP256r1MLKEM768, X25519MLKEM768, and SecP384r1MLKEM1024), followed by classical elliptic-curve and finite-field groups. The scanner allowed one retry for selected DNS resolution errors and attempted the `www.` hostname if the original hostname failed to establish TLS. If all TLS attempts failed, an HTTP connection on port 80 was attempted. Results were stored incrementally in a CSV file, including the negotiated TLS version, key exchange group, and connection status. Measurements were conducted in late August 2026 from a single vantage point in Porto Alegre, RS, Brazil.

3.3. Classification and Analysis

The consolidated dataset was processed to isolate successful HTTPS connections and identify post-quantum or hybrid key exchange adoption, defined as the presence of MLKEM in the negotiated key exchange group. Connections negotiating classical key exchange groups, including those using TLS 1.2, were classified as classical. Domains without a successful HTTPS connection were classified separately, while successful connections without an identifiable key exchange group were excluded from the key exchange analysis, as detailed in Section 4. From the resulting data, statistical visualizations were generated to characterize TLS version distribution, post-quantum versus classical key exchange, and the distribution of negotiated post-quantum mechanisms.

4. Results and Discussion

Of the 10,000 evaluated `.br` domains, 8,701 (87.0%) established a successful HTTPS connection, while 379 (3.8%) were classified as HTTP-only after unsuccessful TLS attempts, and 920 (9.2%) remained unreachable through the implemented probes. These failures may involve DNS resolution, connection, or TLS handshake errors, as described in Section 3.2. This failure rate indicates that popularity alone does not guarantee consistent TLS availability. Of the 8,701 successful HTTPS connections, 4 presented no identifiable key exchange group and were excluded from Section 4.2, yielding a base of 8,697 domains.

4.1. TLS Protocol Version

Figure 2a shows TLS 1.3 accounting for 7,592 domains (87.3%) against 1,109 (12.7%) still on TLS 1.2. Since none of the post-quantum or hybrid groups considered here are negotiable under TLS 1.2, this 12.7% share represents a population that cannot negotiate the post-quantum key exchange mechanisms evaluated in this study without first supporting TLS 1.3. The post-quantum adoption rate reported in Section 4.2 is therefore bounded above by the TLS 1.3 population, and the remaining TLS 1.2 deployment constitutes a protocol-level limitation distinct from the configuration-level factors discussed next.

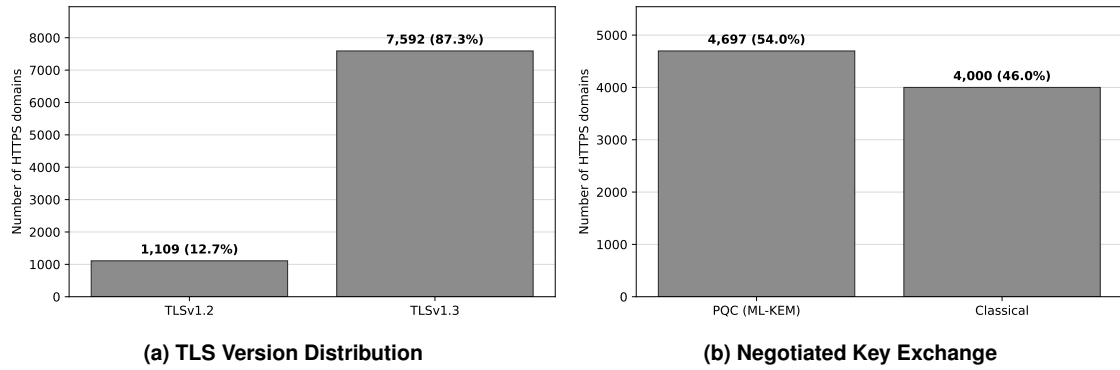


Figure 2. Evaluation results for HTTPS domains

4.2. Key Exchange Mechanism

Figure 2b shows that 4,697 domains (54.0%) negotiated a post-quantum or hybrid mechanism, against 4,000 (46.0%) relying exclusively on classical groups. Since 1,109 of the classical negotiations occurred over TLS 1.2, the remaining 2,891 classical negotiations occurred over TLS 1.3 connections, showing that the absence of a post-quantum or hybrid negotiation cannot be attributed solely to the use of TLS 1.2. These classical negotiations do not necessarily imply a lack of post-quantum support, as the measurements capture the negotiated group rather than all groups supported by the server.

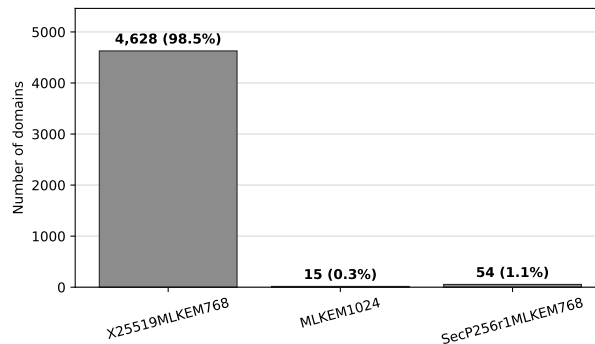


Figure 3. Distribution of the three post-quantum or hybrid mechanisms

4.3. Post-Quantum Mechanism Distribution

The 54.0% adoption rate reported in Section 4.2 is less informative on its own than how that adoption is distributed across mechanisms. Figure 3 shows that X25519MLKEM768

accounts for 4,628 of the 4,697 post-quantum or hybrid negotiations (98.5%), against SecP256r1MLKEM768 (54, 1.1%) and MLKEM1024 (15, 0.3%). Such concentration may reflect shared TLS libraries, Content Delivery Networks (CDNs), or hosting providers, rather than independent configuration decisions by each domain operator. Similar infrastructure concentration has been reported for DNS and TLS certificates [Azevedo et al. 2024, Azevedo et al. 2025]. However, identifying the influence of individual providers requires correlating domains with their underlying infrastructure. MLKEM1024 was observed only marginally and was the only non-hybrid mechanism identified in the measurements.

Taken together, post-quantum key exchange has reached meaningful deployment scale among prominent Brazilian HTTPS services, but this deployment is highly concentrated in a single negotiated hybrid group. This concentration highlights the importance of considering the specific key exchange mechanisms being deployed rather than relying solely on aggregate post-quantum adoption rates. Finally, these findings characterize negotiated key exchange only; since certificate chains and signature algorithms were not analyzed, they do not imply complete post-quantum TLS adoption, as authentication may still rely on classical, quantum-vulnerable schemes.

5. Conclusion and Future Work

This work measured how widely Brazilian websites have adopted post-quantum TLS key exchange, using the top-10,000 `.br` domains from Tranco. TLS 1.3 is already predominant, while post-quantum or hybrid key exchange was observed in 54.0% of the successful connections with a valid key exchange group. The observed post-quantum negotiations were highly concentrated in X25519MLKEM768, which accounted for 98.5% of all post-quantum or hybrid negotiations. These results characterize negotiated post-quantum key exchange among highly ranked `.br` domains, revealing substantial but highly concentrated adoption within the measured population.

Future work includes expanding measurements to lower-ranked domains and other Latin American country-code top-level domains (ccTLDs), correlating negotiations with Autonomous System Numbers (ASNs) and CDN providers, and conducting longitudinal measurements to assess adoption trends and distinguish server support from negotiated deployment.

Use of Artificial Intelligence Tools

Generative Artificial Intelligence (GenAI) tools were used during the preparation of this study to support brainstorming activities, language refinement, and the organization of ideas. The authors assume full responsibility for the content, conclusions, and scientific contributions presented in this work.

Acknowledgments

This work is related to the project “Observatório da Centralização da Internet (OCI)”, registered at UFRGS under project number 49269.

References

Azevedo, A. C., Scheid, E. J., Franco, M. F., Boeira, D. F. F., Zembruzki, L., and Granville, L. Z. (2024). The role of network centralization in shaping digital

- sovereignty: An analysis under the DNS lens. *International Journal of Network Management*, 35(1):e2309.
- Azevedo, A. C., Scheid, E. J., Franco, M. F., and Granville, L. Z. (2025). Assessing SSL/TLS certificate centralization: Implications for digital sovereignty. In *2025 IEEE Global Communications Conference (GLOBECOM)*, pages 3825–3830.
- Bavdekar, R., Jayant Chopde, E., Agrawal, A., Bhatia, A., and Tiwari, K. (2023). Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations. In *International Conference on Information Networking (ICOIN 2023)*, pages 146–151.
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. ACM.
- Kagai, F., Branch, P., But, J., and Allen, R. (2025). Harvest-Now, Decrypt-Later: A Temporal Cybersecurity Risk in the Quantum Transition. *Telecom*, 6(4).
- Kampanakis, P. and Childs-Klein, W. (2024). The impact of data-heavy, post-quantum tls 1.3 on the time-to-last-byte of real-world connections. In *Proceedings of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)*.
- Kwiatkowski, K., Kampanakis, P., Westerbaan, B. E., and Stebila, D. (2026). Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3. RFC 10024, RFC Editor.
- Le Pochat, V., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M., and Joosen, W. (2019). Tranco: A research-oriented top sites ranking hardened against manipulation. In *26th Network and Distributed System Security Symposium (NDSS 2019)*, San Diego, United States of America.
- Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition.
- NIST (2024a). Module-lattice-based digital signature standard. Technical Report FIPS 204, National Institute of Standards and Technology.
- NIST (2024b). Module-lattice-based key-encapsulation mechanism standard. Technical Report FIPS 203, National Institute of Standards and Technology.
- NIST (2024c). Stateless hash-based digital signature standard. Technical Report FIPS 205, National Institute of Standards and Technology.
- Schmeh, K. (2006). *Cryptography and public key infrastructure on the Internet*. John Wiley & Sons.
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE.
- Sikeridis, D., Kampanakis, P., and Devetsikiotis, M. (2020). Post-quantum authentication in tls 1.3: A performance study. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.