Is MadPQC the new RAMONES? A Testing Center for Experimenting and Planning for the Post Quantum Cryptography Transition

Shadi Motaali[2], Farzam Rezaei[2], Jorge E. López de Vergara[2], Florina Almenares Mendoza[3], Daniel Díaz-Sánchez[3], Javier Blanco-Romero[3], Luis Cruz-Piris[4], Carmen Sánchez-Zas[1], Xavier Larriva Novo[1], and Andrés Marín-López[1]

[1] Departamento de Ingeniería de Sistemas Telemáticos, E.T.S.I Telecomunicación,
Universidad Politécnica de Madrid, Madrid, Spain
{andres.mlopez, carmen.szas, xavier.larriva.novo}@upm.es

[2] Dept. Tecnología Electrónica y de las Comunicaciones, Escuela Politécnica Superior,
Universidad Autónoma de Madrid, Madrid, Spain
{shadi.motaali, farzam.rezaei, jorge.lopez_vergara}@uam.es

[3] Departamento de Ingeniería Telemática, Escuela Politécnica Superior,
Universidad Carlos III de Madrid, Leganés, Madrid, Spain
{florina, dds, frblanco}@uc3m.es

[4] Departamento de Automática, Escuela Politécnica Superior,
Universidad de Alcalá, Alcalá de Henares, Madrid, Spain
luis.cruz@uah.es

https://ramonescm.lab.dit.upm.es/

Abstract. We are facing a threat brought by future Cryptographic Relevant Quantum Computers (CRQC): Store Now and Decrypt Later (SNDL). Our public key algorithms based on discrete logarithms and large number factorization are vulnerable to the Shor quantum algorithm. Symmetric cryptography is not facing such a threat since incrementing the key length is still a working countermeasure. Many different countries like Korea, USA, China, Russia, Spain, France, Germany and others in the European Union, have elaborated recommendations and plans to transition to quantum resistant public key algorithms, many of them proposing new lattice and hash based cryptography. The plans include the need for extensive experimentation with the foreseen algorithms under many different network conditions and applications. A group of four public universities in the Community of Madrid supported by a regional funded project, RAMONES-CM, is promoting an action called MadPQC for setting up a testing centre, which allows running pilots and execution of different tests and implementation of Post Quatum Cryptography (PQC). Not only the new cryptographic algorithms proposed in the NIST competition, those standardised in 2024, but they can be subsequently extended to others including the expected candidates to the new competition promoted from China and announced at the ETSI/PQC last june 2025, the Korean proposals, etc. The action will make it possible to verify other experiments already carried out, validate the use of the new algorithms and offer implementation methodologies for the transition to our industrial companies and administrations. In this paper we explain the plans and schedule of MadPQC experimentation. We present an example of MadPQC initial results using DTLS

1.3, which has not been so tested as TLS 1.3, and present our initial proposals of methodologies for the transition.

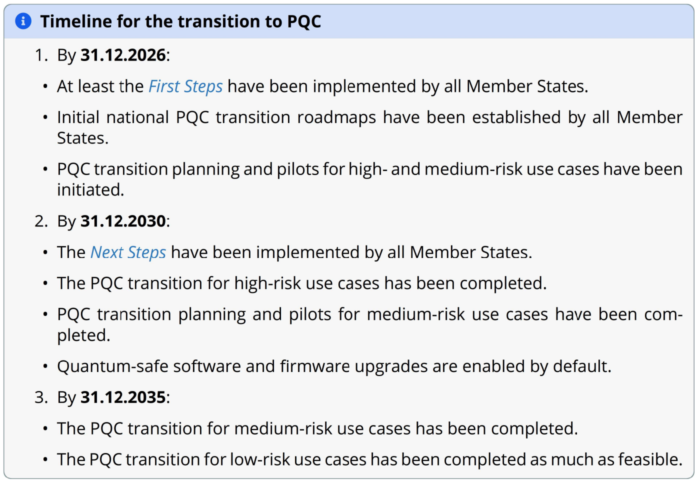
Keywords: post quantum cryptography · post quantum experimentation · crypto agility.

1 Introduction

In April 2024, the European Commission published a Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (PQC). The EC encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. Eight months later, in November 2024, eighteen partners of the European Union recognized the importance of adopting a common position on the migration to PQC. In June 2025, three more European states signed the paper. Besides the Store Now and Decrypt Later (SNDL) threat, the paper states a second threat: *the long migration periods, which occur for complex systems such as public key infrastructures (PKI) or devices with a long lifetime... the risk arises that the transition to quantum secure cryptography might not be completed in time, endangering the confidentiality and authenticity of all communication.* They propose to work on four steps: (1) quantum threat analysis (inventory of the assets to protect and the applications that use cryptography); (2) risk-oriented roadmap for executing the transition, taking into account the sensitivity and the protection period of the information, as well as the need to mitigate the two identified threats; (3) plan and budget for the migration; and (4) promote the continuation of the extensive research on post-quantum cryptography and standardization efforts. Finally, they encourage all member states to participate in the Work Stream on PQC.

This Work Stream on PQC states the transition is not only a technical change, and two more keys are required: organization/people and processes. Next September 2025, 22 state members, the EC and ENISA are expected participate in the kick-off, with a writing team composed by Germany, the Netherlands, France and Denmark. They agree that urgent adopters should start now, and EU member state governments are urgent adopters. Four scenarios are clearly identified: sensitive information with a long confidentiality span (SNDL); Personal Data with a long confidentiality span, like health records; provide systems of critical infrastructure like payment transactions, energy, or transportation; and provide systems which are built to have a long life span: water management, chemical industry, drinking water, railroads.

The Work Stream initially proposes a comprehensive approach for Member States' authorities to start the roadmap process as shown in Fig.1. The *First steps* identified are: Identify and involve stakeholders; Create dependency maps; Perform quantum risk analysis; Share knowledge and get involved in the EU work stream on PQC; Support mature cryptographic asset management; Include the supply chain; Create a national awareness program; Develop a timeline and an implementation plan. The *Next steps* are: Develop crypto agility and quantum safe upgrades; Allocate resources; Evolve the rules; Transversal activities; Adapt certification schemes; Establish testing centers and pilots; Involve the ecosystem.



Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

Fig. 1. EU PQC Roadmap presented at ETSI/IQC Quantum Safe Cryptographic Conference, June 4 2025. Source: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

This roadmap and derived transition methodologies and processes have to take into account EU state of the art regulation like: Article 32(1) of GDPR [10], which addresses the security of processing personal data; Article 4(1) of e-Privacy [9], which pertains to the confidentiality of communications; Article 21(1) and (2)(h) of NIS-2 [11], which address security requirements for essential and important entities; Article 9 of DORA [12] which addresses the requirements for digital operational resilience, and Recitals (31), (73) and Article 24(2)(e) address various provisions related to electronic identification and trust services [8], e-IDAS 2 [13], or CRA [14].

Several member states are already working on resources, guidelines and recommendations. For example: Germany (BSI) [5] and [4]; France (ANSSI) [2]; The Netherlands (various institutions) [17,16,24]; Spain (CCN) [6]; Czechia (NÚKI) [21]; or Italy (ACN) [3].

In this paper we discuss MadPQC, a testing centre and pilot support for PQC in Madrid. MadPQC will be open to new PQC algorithms. The contributions of this article are: defining a experimentation with PQC in DTLS 1.3 which has not been subject to so much experimentation as PQC in TLS 1.3; parameterizing and automating the setup to include future algorithms, devices and testing partners, both regional and international; validating the use of the new PQC algorithms in different scenarios and offer implementation methodologies for the transition to industrial companies and administrations.

The remainder of this paper is organized as follows: Section 2 examines the state-of-the-art on TLS benchmarks. Next, section 3 outlines our proposal. Section 4 presents the DTLS use case. The paper concludes with the analysis of results and the conclusions and future research directions.

2 State of the Art

In response to the significant threat to current public-key cryptographic algorithms posed by advent of large-scale quantum computers, the USA National Institute of Standards and Technology (NIST) launched a multi-year standardization process in 2016 to identify, evaluate, and standardize quantum-resistant cryptographic algorithms. In July 2022, first set of algorithms selected for standardization was announced: CRYSTALS-Kyber (FIPS 203: Module-Lattice-Based Key Encapsulation Mechanism, ML-KEM) [18] for key-establishment, CRYSTALS-Dilithium (FIPS 204: Module-Lattice-Based Digital Signature Algorithm, ML-DSA) [19], SPHINCS+ (FIPS 205: Stateless Hash-Based Digital Signature Algorithm, SLH-DSA) [20] and FALCON (Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm, FN-DSA) for signature. The specification for this last one is ongoing as other NIST's standardization efforts.

There is a need for additional algorithms based on different schemes to diversify the portfolio and address specific use cases or provide alternative security assumption. Thus, recently, in March 2025, NIST announced its decision to standardize HQC (Hamming Quasi-Cyclic), a code-based mechanism for KEM. For signature, "on-ramp" process aims to bring new candidates. The transition is expected to be a multi-year process, with timelines for phasing out vulnerable legacy algorithms by 2030 and 2035. Such PQC transition requires extensive experimentation in realistic scenarios, as well as benchmarking on controlled scenarios, to understand the real-world performance impact of these new algorithms.

In this way, there are some notable experimentation works on the Transport Layer Security (TLS) protocol 1.3 such as Paquin et al. [22][5], Tasopoulos et al. [23], Henrich et al. [15], and Abasi et al. [1]. Paquin et al. was a primary work focused on benchmarking the performance trade-offs of various PQC schemes, using a framework to emulate network conditions, allowing for testing under different scenarios (e.g., varying packet loss rates) [22]. Tasopoulos et al. showed on performance evaluation on resource constrained embedded systems (i.e., the NUCLEO F439ZI), using wolfSSL library and pqm4 implementations of selected algorithms on a local Ethernet network. Henrich et al. extends Paquin et al. work evaluating the performance impact of PQC KEM algorithms under varying network characteristics such as using servers in three locations with different average delays. In [1], a practical PQC benchmark in three distinct hardware environments, i.e., server, laptop and IoT device, and various network conditions, i.e., latency, packet loss, and MTU restrictions, is presented. Although most these research work have simulated various network conditions in order to model realistic conditions, the core benchmarking has not been on a live, Internet-scale network with real user traffic.

Companies like Cloudflare and Google are actively conducting significant live experiments by deploying PQC algorithms, specifically hybrid key exchange schemes like X25519+Kyber, in their production networks since about 2019 [7]. These experiments involve real user traffic and provide valuable insights into the performance and challenges of PQC in actual internet environments. For these reasons, in this paper we have conducted a realistic internet experiment across three distinct locations. This involved

[5] github.com/xvzcf/pq-tls-benchmark

deploying test clients and servers to generate traffic that flowed through the live network.

3 Setting up a PQC centre

As shown in Figure 2, MadPQC testing infrastructure is designed to support the four-step transition roadmap by enabling controlled, repeatable experiments across both virtual and physical environments.

In the **client** domain—whether physical hardware or VM—a WireGuard egress tunnel (interface `wg0` over `eth1`) routes all application traffic into the **provider** testbed. There, an SDN-based *tee* forwards live traffic to the Internet unchanged, while duplicating streams via GRE tunnels to a **capturer** module for real-time quantum-risk analysis: extracting performance metrics, flagging anomalous exchanges, and cataloguing long-lived session data in line with SNDL requirements.

Complementing this, an **injector** component—also connected via GRE through the same *tee*—can introduce, modify or drop packets on-the-fly, simulating PQC upgrade scenarios or attack vectors to validate resilience and incident response procedures.

Multiple isolated instances can be spun up concurrently—defined as Infrastructure-as-Code templates in our repository—so that Member State authorities, vendors and researchers can:

- Pilot diverse migration plans.
- Benchmark PQC extensions in DTLS 1.3.
- Refine implementation budgets and timelines before large-scale roll-out.

This end-to-end orchestration directly maps to the “plan and budget” and “pilot/testing” phases of the EU Work Stream risk-oriented roadmap, ensuring that migration methodologies are stress-tested under realistic conditions.

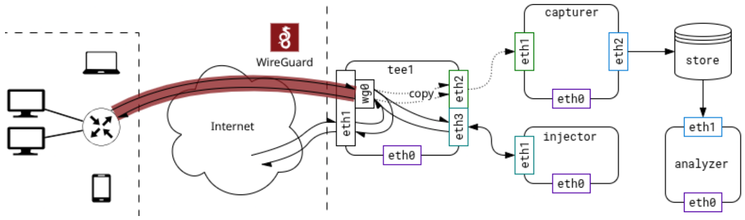


Fig. 2. Testing infrastructure

When we started some preliminary tests, we found out some initial problems with recognizing the certificates in some combination of liboqs and wolfssl. The server sent an ALERT message and we had to restart the server. To facilitate the deployment of the test and to ensure a common set up, we decided to develop a closed set up with containers. We designed a Debian bookworm based Docker with a specific version of the PQC specific software:

- OpenSSL 3.0.16 11 Feb 2025 (Library: OpenSSL 3.0.16 11 Feb 2025).
- OpenSSL OQS Provider version: 0.8.1-dev.
- liboqs version 0.13.0.
- Wolfssl version 5.8.0.

The Dockerfile is available at the downloads page of RAMONES-CM, for anyone interested in running a PQC client, and the servers are free for anyone interested in running the tests. Even more, since we are monitoring the traffic, we can provide the tester with the whole trace of the experiment traffic upon request. Besides this, we decided to run demonized versions of the servers, together with a watchdog to restart the demon in case of problems.

MadPQC was conceived with the mission to test different combinations of PQC algorithms, including signature and KEM algorithms. This is relatively easy with applications which allow for algorithm negotiation in the initial interaction. This is the case for instance of OpenSSL. OpenSSL servers can be initiated with a list of supported groups and key exchange methods KEM so that if the OpenSSL client offers one single KEM, say ML_KEM_1024, it will be the chosen KEM after the TLS negotiation. Other software, such as wolfSSL, does allow a single option in the server, so there is no real negotiation.

That leads MadPQC into the necessity of using different ports for each KEM that we want to test. Besides testing different KEMs using different signature algorithms requires the use of different certificates. The public key of the certificate holder should be an instance of the signature algorithm to test. Since the server and the client can only specify one end-entity certificate, we solved this using the port mechanism to multiplex between certificates. That means that we require a bunch of certificates with the server at each particular port configured to use a different certificate and a different KEM. If we have, say n different DSA algorithms and m different KEM, we would need to allocate $n \times m$ ports for all the possible combinations to test. An alternative would be using renegotiation, but this would make the performance measurement more complex.

Finally, MadPQC deployed a certificate authority (CA) per each different signature algorithm to test. Again each of those CA would issue as many server and client certificates as signature algorithms to test. We decided to include all the CA certificates in the Docker deployment, together with a script to build the client certificate request explicitly setting the subjectAltName to the IP of the client, so that each test user could have their own client certificates. The users run the script, send the request to a central point, and receive the certificates offline. The client certificates are copied into the running container using a simple curl to retrieve from a python http.server in the host. The final result is that each Docker is equipped with its own set of client certificates and keys issued to the corresponding IP address of the client.

4 A DTLS 1.3 use case

To evaluate the practical performance and behavior of DTLS 1.3 in realistic conditions, we conducted a series of measurements involving the DTLS server deployed at Universidad Politécnica de Madrid (DIT-UPM). Clients from two remote locations—two hosted at Universidad Carlos III de Madrid (UC3M) and Universidad de Alcalá

(UAH) and another on a Hetzner cloud server located in Germany—were used to initiate DTLS sessions with the server. The idea is to have measurements from different locations, close and far from the server, to see how the service times varies depending on the network. Close refers to University clients and server in the high speed academic network REDIMadrid, which connects with the Geant Network, where the far client is located.

On the client side, we build a Docker container with the WolfSSL software and employed a custom script designed to automate the tests across multiple runs and algorithms. This script allowed us to test various cryptographic algorithms, including both post-quantum cryptographic (PQC) algorithms (different version of ML_KEM and MDL_DSA) and hybrid configurations combining classical eliptic curves (P256, P384 and P512) and PQC methods. Each algorithm was tested under the same operational conditions to ensure a fair comparison. Tests were done 100 times sending 1 000 and 1 360 bytes of payload.

Meanwhile, the server at DIT-UPM was configured to listen on different ports dedicated to each cryptographic configuration, as shown in Table 1. Traffic arriving on these ports was captured using packet sniffing tools to monitor and record the full packet exchanges.

Table 1. Signature and KEM algorithms used in each port in the server

Signature	**KEM**	**UDP port**
mldsa44	ML_KEM_512	11113
mldsa44	P256_ML_KEM_512	11114
mldsa65	ML_KEM_768	11115
mldsa65	P256_ML_KEM_768	11116
mldsa65	P384_ML_KEM_768	11117
mldsa87	ML_KEM_1024	11118
mldsa87	P384_ML_KEM_1024	11119
mldsa87	P521_ML_KEM_1024	11120

The captured UDP traffic was then analysed with Wireshark and its Conversations tool for UDP to determine the duration of each DTLS conversation. Additionally, we examined the integrity and completeness of the exchanges. Some sessions with a significantly reduced number of packets were observed, and were flagged as potential handshake or data transmission failures. Likewise, we identified *fatal-level alerts* DTLS record-layer messages marked "fatal," such as `illegal_parameter` indicating unrecoverable negotiation breakdowns between client and server. These cases were further investigated to understand the underlying causes and assess the robustness of the tested cryptographic schemes. We also observed very long sessions, finding in this case that there were two sessions with the same client port (probably a port reincarnation), discarding these from the results. Figure 3 shows the different errors we found on each case:

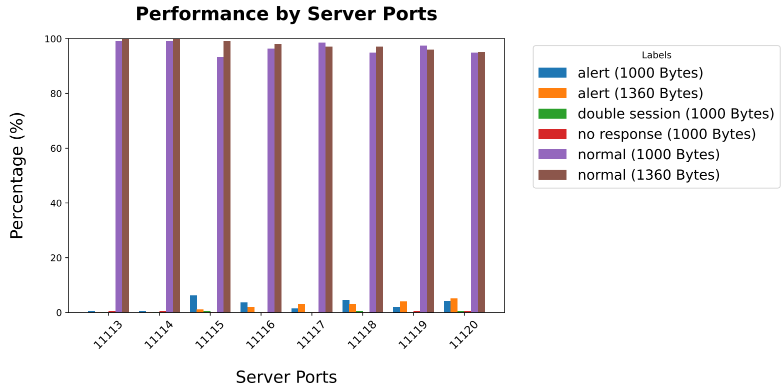


Fig. 3. Successful sessions and errors with each server port.

This setup provided us with valuable insights into the practical viability of various PQC and hybrid algorithms in real-world DTLS 1.3 deployments, under both local and geographically distributed conditions.

5 Analysis of results

Our measurements drive evaluated post-quantum and hybrid cryptographic algorithm performance in DTLS 1.3, utilizing a server at Universidad Politécnica de Madrid, a geographically distant client in Germany to assess real-world deployment characteristics. We also show the results of the same experiment with a client in REDIMadrid.

Performance Analysis Across Cryptographic Configurations Our analysis of session durations across different cryptographic configurations and payload sizes (1 000 bytes and 1 360 bytes), as illustrated in Figures 4 to 7, revealed several significant patterns:

1. **Parameter Size Impact**: Our results demonstrate a clear security–performance trade-off across parameter sizes. For identical algorithms, larger parameter sets consistently required longer processing times. Comparing across payload sizes, `mldsa87+ML_KEM_1024` showed median durations of 0.150 s (1 360 bytes) versus 0.125 s (1 000 bytes), while `mldsa44+ML_KEM_512` exhibited 0.122 s versus 0.120 s, respectively. This pattern holds for all algorithm variants, confirming that both parameter size and payload size directly influence performance, with the highest security levels (`mldsa87+ML_KEM_1024` variants) consistently showing 20–30% longer processing times than their lower-security counterparts.
2. **Hybrid vs. Pure Implementation Overhead**: The data reveals small but measurable performance differences between hybrid and pure implementations of the same security level. For 1 000-byte payloads, pure ML_KEM_768 showed a median duration of 0.123 seconds while its P256 hybrid variant required 0.126 seconds. This

difference, though modest, confirms the additional computational cost of performing both traditional and post-quantum operations.

3. **Elliptic Curve Influence**: In hybrid implementations, the choice of elliptic curve significantly affected performance. P384-based hybrids consistently exhibited the longest session durations (median 0.170 seconds for 1 360 bytes), while P256-based hybrids performed better with durations closer to their pure post-quantum equivalents. The violin plots clearly illustrate how the three different curves (P256, P384, P521) form distinct performance tiers within each security level.
4. **The network impact** in the performance of the tests, shows similar violin plots of the closer client, in a different scale, with a reduction of almost seven times for the media of the session duration in 1000 bytes and six times in the 1360 bytes sessions.

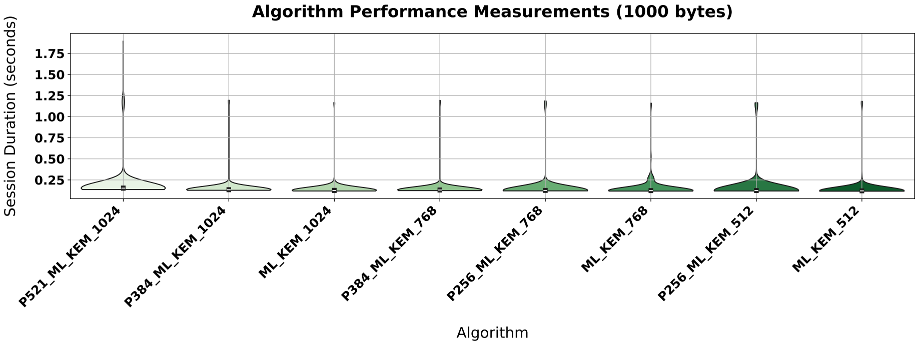


Fig. 4. Violin plots for 1 000 bytes sessions and different algorithms (client in Germany)

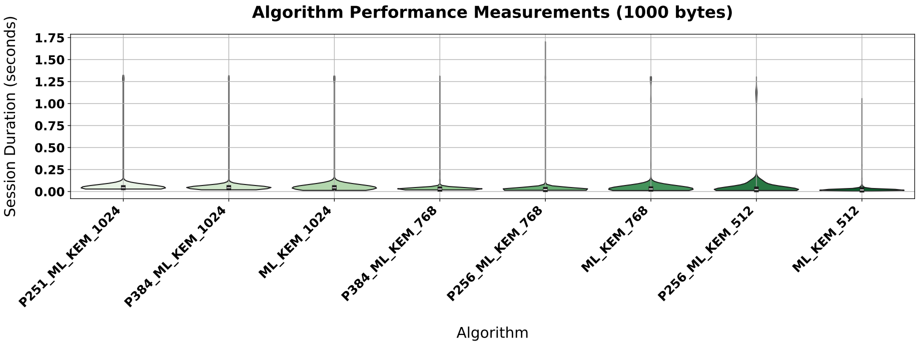


Fig. 5. Violin plots for 1 000 bytes sessions and different algorithms (client in REDIMadrid)

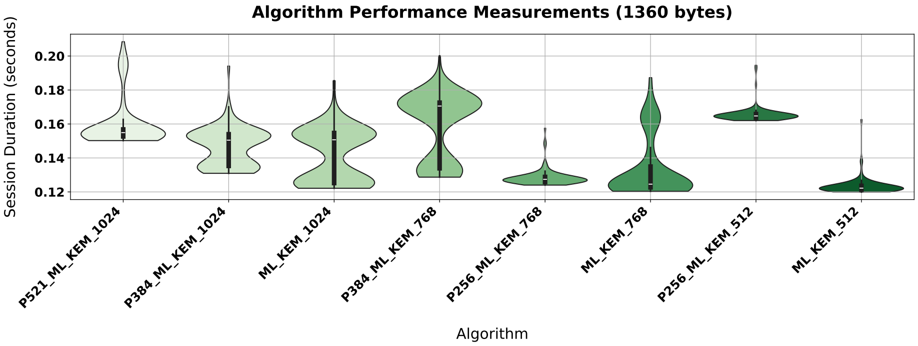


Fig. 6. Violin plots for 1 360 bytes sessions and different algorithms (client in Germany)

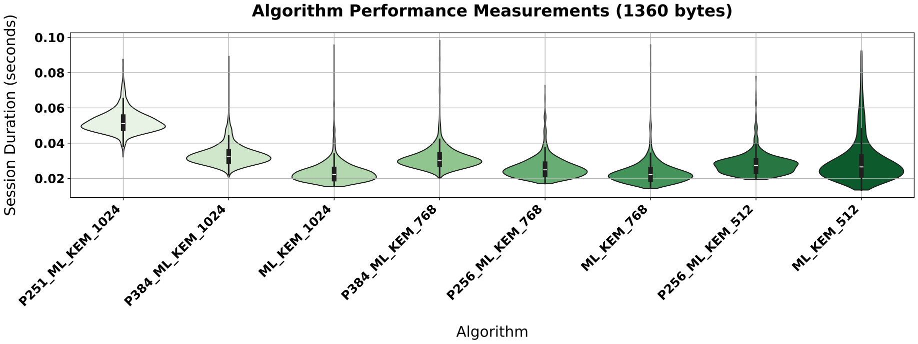


Fig. 7. Violin plots for 1 360 bytes sessions and different algorithms (client in REDIMadrid)

6 Conclusions

The experimental use case presented in this work has demonstrated the practical feasibility of deploying and evaluating post-quantum and hybrid cryptographic algorithms in real-world DTLS 1.3 environments. The comparative measurements conducted from geographically distributed clients—both from university campuses (UC3M, UAH) and a cloud server in Germany—provided valuable insights into latency, reliability, and the impact of cryptographic configurations on handshake duration and session integrity. The analysis revealed expected performance trade-offs based on key sizes, algorithm types, and hybrid combinations, with measurable differences in session duration across configurations. Notably, higher-security settings introduced 20–30% additional latency, and certain hybrid schemes with larger elliptic curves (e.g., P384) incurred further delays. This is shown in the relative displacement of the violin plots in all the figures. Violin plots where chosen because they show the median and the interquartile range of the confidence interval, but they also show the probability distribution, which let us see that besides the large distribution around the median, there is another hich probability region in the lower part of the plot. This is clearly appretiated in Fig. fig:violin0407.

This case study confirms the importance of fine-grained testing across use cases and locations to guide the selection of algorithms in PQC transitions.

MadPQC will continue to evolve as a reference environment for experimentation, benchmarking, and guidance, enabling industry and government actors to prepare for and execute quantum-safe transitions in alignment with EU-level strategy and national regulations. In the near future we plan to set up a whole automated procedure to allow anyone to perform the tests including the issuance of the required client certificates that will be available upon mail registration. We are discussing some points left: limited devices and result tracking. Besides RPi and laptop clients we expect to offer support for more limited devices. Result tracking involves automation of the actual results extraction and sharing with the RAMONES-CM consortium. We include aspects of energy and memory requirements in future analysis, to offer better advice for the roadmap to PQC implementation in companies and administration.

Acknowledgments. This action has been financed through the R&D activities programme with reference TEC-2024/COM-504 and acronym RAMONES-CM granted by the Comunidad de Madrid, Spain through the Directorate General for Research and Technological Innovation by Order 5696/2024. It has also been partially funded by Ph.D. grants from the Department of Electronics and Communication Technologies at Universidad Autónoma de Madrid.

Disclosure of Interests. Authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abbasi, M., Cardoso, F., Váz, P., Silva, J., Martins, P.: A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography **9** (2025), https://doi.org/10.3390/cryptography9020032
2. Agence nationale de la sécurité des systèmes d'information (ANSSI): ANSSI views on the post-quantum cryptography transition (2023), https://short.upm.es/61mkz, accessed: 2025-07-07
3. Agenzia per la Cybersicurezza Nazionale (ACN): Crittografia post-quantum e quantistica, preparazione alla minaccia quantistica (2024), https://short.upm.es/nfirh, accessed: 2025-07-07
4. Bundesamt für Sicherheit in der Informationstechnik (BSI): Technical guideline on quantum-safe key agreement and signature schemes, https://short.upm.es/295tx, accessed: 2025-07-07
5. Bundesamt für Sicherheit in der Informationstechnik (BSI): Migration to post quantum cryptography (2020), https://short.upm.es/64tb8, accessed: 2025-07-07
6. Centro Criptológico Nacional (CCN): Recommendations for a safe post-quantum transition (2022), https://short.upm.es/ramrk, accessed: 2025-07-07
7. The TLS post-quantum experiment (10 2019), https://short.upm.es/ekokq
8. European Comission: Delegated Regulation (EU) 2024/1774 (April 2024), https://short.upm.es/xma9g, articles 6 and 7 pertain to specific requirements related to digital operational resilience.
9. European Parliament and Council: Directive 2002/58/EC of the European Parliament and of the Council (July 2002), https://short.upm.es/3bx1x, article 4(1)

10. European Parliament and Council: Regulation (EU) 2016/679 of the European Parliament and of the Council (April 2016), `https://short.upm.es/g5g71`, article 32(1).
11. European Parliament and Council: Directive (EU) 2022/2555 of the European Parliament and of the Council (December 2022), `https://short.upm.es/0bli0`, article 21(1) and (2)(h)
12. European Parliament and Council: Regulation (EU) 2022/2554 of the European Parliament and of the Council (December 2022), `https://short.upm.es/w1xv7`, article 9
13. European Parliament and Council: Regulation (EU) 2024/1183 of the European Parliament and of the Council (April 2024), `https://short.upm.es/pglft`, recitals (31), (73) and Article 24(2)(e) address various provisions related to electronic identification and trust services.
14. European Parliament and Council: Regulation (EU) 2024/2847 of the European Parliament and of the Council (April 2024), `https://short.upm.es/v13sa`, article 6, Article 13(1) and (2), Article 19(1), and Annex I, Part I (1) and (2)(e) address various requirements related to the regulation.
15. Henrich, J., Heinemann, A., Wiesmaier, A., Schmitt, N.: Performance impact of PQC KEMs on TLS 1.3 under varying network characteristics. In: Athanasopoulos, E., Mennink, B. (eds.) Information Security. pp. 267–287. Springer Nature Switzerland, Cham (2023)
16. National Cyber Security Centre (NCSC): Make your organization quantum secure (2024), `https://short.upm.es/yy5ga`, accessed: 2025-07-07
17. National Cyber Security Centre (NCSC) and various institutions: Guidelines for quantum-safe transport layer encryption (2022), `https://short.upm.es/slsmt`, accessed: 2025-07-07
18. National Institute of Standards and Technology: FIPS 203 module-lattice-based key-encapsulation mechanism standard. Federal Information Processing Standards Publication FIPS 203, NIST (2024)
19. National Institute of Standards and Technology: FIPS 204 module-lattice-based digital signature standard. Federal Information Processing Standards Publication FIPS 204, NIST (2024)
20. National Institute of Standards and Technology: FIPS 205 stateless hash-based digital signature standard. Federal Information Processing Standards Publication FIPS 205, NIST (2024)
21. Národní úřad pro kybernetickou a informační bezpečnost (NÚKI): Minimum requirements for cryptographic algorithms (2023), `https://short.upm.es/xkw7d`, accessed: 2025-07-07
22. Paquin, C., Stebila, D., Tamvada, G.: 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 (2020)
23. Tasopoulos, G., Li, J., Fournaris, A.P., Zhao, R.K., Sakzad, A., Steinfeld, R.: Performance evaluation of post-quantum TLS 1.3 on resource-constrained embedded systems. In: Su, C., Gritzalis, D., Piuri, V. (eds.) Information Security Practice and Experience. pp. 432–451. Springer International Publishing, Cham (2022)
24. TNO: The PQC migration handbook (2023), `https://short.upm.es/mvka2`, accessed: 2025-07-07