National College of Ireland

The Performance Impact of Post-Quantum Cryptography on User Experience

MSc Research Project
MSc Cybersecurity

Damien Nalty
Student ID: x23272414

School of Computing
National College of Ireland

Supervisor: Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: .....Damien Nalty.....

Student ID: .....x23272414.....

Programme: .....MSCCYBE_JAN24_OL..... **Year:** 2025-2026

Module: .....Research Project Practicum II.....

Supervisor: .....Dr. Raza Ul Mustafa.....

Submission Due Date: .....28th January 2026.....

Project Title: The Performance Impact of Post-Quantum Cryptography on User Experience...

Word Count: .....6790..... **Page Count**.....20.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

..... Damien Nalty .....

Date: .....24/01/2026.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

The Performance Impact of Post-Quantum Cryptography on User Experience

Damien Nalty
X23272414

Abstract

This paper poses the key question - is web user experience actually impacted by post-quantum cryptography? In this research I have developed a test utility that provides visibility of how the performance of the cipher profiles differ, from legacy security right up to the highest-level standard quantum-resistant profiles. This research provides unique visibility of how the security profiles compare and perform and seeks to validate the KPIs used with a commercial security performance test suite. This paper and utilities used will serve as a guide to those needing to quantify the migration challenge ahead and which security posture and level best suits their needs.

Key findings from this research activity - the traditional approach of observing throughput and latency (round-trip time) metrics is not sufficient for evaluating user experience. A combination of connection-based metrics along with visibility of discrete exchanges within the connections, plus the key and signature data per profile provide the context required to assess performance. A pattern emerges when we analyse the bytes and packets transferred per handshake, regardless of the volume of packets or bytes exchanged.

The biggest challenge in the pending migration lies in supporting classical and post-quantum technologies in parallel. Hybrid profiles were the worst performers across the KPIs observed. The ultimate benefit is that a fully post-quantum landscape has a consistent performance profile across security levels out-performing equivalent classical solutions currently in place in performance and consistency.

1 Introduction

Cryptography is an essential component in modern electronic communications. It provides users with a method of protecting their personal data, at rest and in transit. It achieves this objective by using complex mathematical techniques to obfuscate data so that it can only be read by the sender or receiver with previously agreed or negotiated keys. Cryptography is also used to verify users by exchanging uniquely identifiable information, calculating unique signatures that cannot be replicated by a malicious user. This ensures user privacy is verifiable and maintained and the secure transfer of sensitive data can be achieved. However, there is a performance trade-off for this level of security.

With the advent of quantum computing, all of the current cryptographic methods in use are at risk by quantum computing's processing power. Quantum computing reduces the complex mathematics of modern cryptography to computational challenges that can be practically solved[1]. Shors Algorithm (Shor, 1994) and its impact on RSA encryption is a prime example

[1] Current cryptography (e.g., RSA encryption) is based on the factorisation of large integers and the difficulty of breaking down these numbers into their prime factors. Two large prime numbers are multiplied together to create a modulus (n), which forms part of the public key. The corresponding private key needs to know the original two prime factors. Without these primes, decrypting the data requires factoring 'n' which is computationally prohibitive and impractical for a classic computer, even a supercomputer to achieve.

of this power. As a result, there is a clear pathway for threat actors to compromise current security. Post-Quantum Cryptography (PQC) provides functions and algorithms to combat this threat and protect internet users in the long term. However, by adopting PQC are we compromising the performance of the current information technology landscape? There are a number of challenges which may have profound implications on all standard electronic transactions and communications. The challenge of how long we have left to adopt Quantum safe mechanisms is articulated by co-founder of the Institute of Quantum Computing Professor Michele Mosca. Mosca's Theorem in particular deals with the phenomenon of 'harvest now, decrypt later' which describes the speculative approach of exfiltrating sensitive encrypted data now, safe in the knowledge that the algorithms used to protect this data will be crackable within the next decade. Moscas Theorem, presented initially at the Global Risk Institute in October 2018 (Mosca, 2018) defines the following:

$$x + y > z$$

Where (x) is the measure of how long we need our cryptographic keys to be secure, termed as "the security shelf life". (y) represents how long it will take to develop and deploy a set of tools that are quantum safe. Lastly, (z) represents how long it will take before a quantum computer can crack the current public key cryptography environment? If the theorem above holds true, then we are in trouble. Mosca hypothesised that there was a 1-in-7 chance that quantum computing will produce sufficient stable qubits to crack a 2048-bit RSA key by 2026 and 1 in 2 possibilities by 2031, based on the acceleration of quantum computing research and development. The main focus of this paper relates to y – specifically how long to deploy a quantum safe infrastructure? To elaborate on this question, now that the industry has had some initial time to assess developments in post-quantum cryptography. The key questions this paper poses are:

- Can the impact of post-quantum cryptography on application performance be measured?
- Can this impact be quantified as real user experience?

To follow-on from these key questions the research will also explore: -

- Could PQC adoption present a detrimental impact for general users?
- Could this impact require us to re-evaluate how we secure data for applications in common use.

In this paper we shall investigate this impact, by using the common protocols used to conduct secure electronic transactions. We will focus solely on application-level encryption securing web traffic and investigating how it impacts performance, We will quantify the processing overhead associated with post-quantum, when compared with legacy security and also with classical and hybrid encryption. This study will also quantify SaaS application behaviour, as an example study, (using Microsoft 365 traffic) so that the direct impact can be measured and quantified in the context of familiar well-known applications in widespread use.

The objective is to translate the impact of adopting post-quantum cryptography into a user-friendly and meaningful output. This is achieved by experimenting using a controlled test environment consisting of

- A custom developed test harness – designed to measure the primitives of the transaction and present KPIs in a comparison dashboard.
- A network traffic application emulation and performance toolkit, supporting classical and post-quantum cryptographic profiles.

The data will be analysed to derive key insights into performance and user experience.

This paper proceeds by analysing recent peer developments in this field of academic research in section 2. Section 3 will outline the methodology, test profiles and resulting key performance indicators for analysis. In section 4 the architecture of the systems used to test the research will be presented. In section 5 the test case execution and implementation are discussed and in

section 6 the analysis data gathered will be presented to derive insights into the research questions posed and, in conclusion, section 7 proposes areas for advancement and further study.

2 Related Work

This section examines existing research that has contributed to the subject of post-quantum cryptography performance to establish a baseline for the research undertaken.

2.1 Post-Quantum Cipher Analysis

Bharat Rawal and Peter Curry introduced the challenges and opportunities of adopting post-quantum cryptography in their journal article for APL Quantum (Rawal, 2024). They delve deep into the building blocks of all available quantum-safe ciphers and digital signatures, providing essential background on the algorithms and functions used. In relation to performance, they predict latency issues caused by larger key lengths and consider the impact this is likely to have on wireless network communications, especially for low power, low processor devices such as IoT, presenting a potential security issue for such solutions. The paper finishes by presenting a novel solution of splitting the control and data plane processing of encryption and decryption using a multi-homed dedicated host device (splitting the processing into separate network streams on separate network interface cards on the same device.) This paper represents a seminal introduction to the world of post-quantum ciphering and relative performance of ciphers, this however, does not translate to a practical solution. The proposal for multi-homed devices with dedicated processing, may introduce needless processing overheads. The authors cite another body of work that examines the performance of post-quantum ciphering using dedicated data-processing units (DPU). In their analysis Aguilera et al. (Aguilera, Clemente, Lawo, Monroy, & Olmos, 2023) present their work as the first successful PQC connection between two hosts using dedicated DPU devices. They advocate the necessity of dedicated processing components with the advent of post-quantum cryptography for offloading tasks and crypto-acceleration (dedicated encryption/decryption processing). As with the previously cited work, the authors capture insights into potential use cases for the ciphers and signatures tested. The experimentation in both submissions focuses on machine specific performance indicators, although useful to begin benchmarking behaviours, they do not present PQC as a mass adoption solution unless accompanied by (unnecessary) dedicated hardware to offload the processing overhead challenges.

2.2 Post-Quantum Performance in Production Network Topologies

Subsequent research focused on post-quantum cryptography applied to production network topologies. A novel approach was presented in the following paper, (Ojetunde, 2025) which the authors proposed and tested a hybrid cryptographic method blending post-quantum techniques with classical cryptography by using PQC-based and PQC with AES hybrid public key encryption to transmit securely between host devices. The authors, Ojetunde et al. provided a noteworthy test methodology transferring fixed size files between two commercial-off-the-shelf host devices (no specialised hardware) with a socket-based python file transfer program measuring throughput and round-trip time (RTT) as key performance indicators across a wireless LAN. The authors compared results from classical, post-quantum and their hybrid solution. Their solution brought a distinct element of practicality and furthered the research using standard equipment with PQC, but the measurements made focused solely on performance. In addition, the hybrid solution which exchanged a shared key over PQC

negotiated key encapsulation channels appears to be a retrograde step. The study ended with areas of improvement focused on production grade networks such as 5G environments where they hypothesised that their hybrid approach could be of practical use.
Following on from this study, the article "Towards a Quantum-safe 5G" (Asier Atutxa, 2024) outlined a novel solution for secure communications within the 5G Core network functions, focusing on security while exchanging subscriber information across Service Based Architecture (SBA) components. The research problem described a lack of adequate security coverage when dealing with multi-access edge computing where network functions need to register and send service requests across the 5G core. 3GPP has evolved over the generations from strict point-to-point defined interfaces between key functions to a more flexible, cloud-native approach using familiar protocols such as HTTP/2 and RESTful APIs in 5G. It is a natural progression that those HTTP/2 connections should adopt TLS to protect the exchanges between components as they transfer sensitive data. The authors make a case of using quantum key distribution (QKD) keys as the secure foundation of quantum-safe connectivity. The overhead associated with using quantum keys coupled with TLS exchanges for the keys is discussed. This approach, although commendable for ensuring secure communications between previously unsecured network functions, seems to be creating a problem and subsequently offering a resolution, one which will be resolved via evolution in 3GPP standards to adopt HTTP/3, which is secure by default, between the core components.

Quantum key distribution in production networks is explored in a number of papers, initially written for the Optical Fiber Communications conference in San Diego, in March 2024 (O. Alia, Quantum-safe 10 Gbps Site-to-Site IPsec VPN Tunnel over 46 km Deployed Fibre, 2024) showcasing 10Gbps network traffic achieved across a quantum-safe dedicated test network extended across two sites connected by a fibre link. This topology utilises dedicated site-to-site VPN technology using post-quantum pre-shared keys (PPK) sourced using quantum key distribution from dedicated quantum channels between sites. This was extended to 100Gbps in a follow-up paper (O. Alia, 100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber, 2024). The team successfully scaled traffic by utilising multi-link VPNs to generate a steady 100Gbps (99.62Gbps) throughput across the metropolitan link for 45 days. The output of both papers focuses on the stable throughput and data delivery across the quantum-safe network only. Other key performance indicators focused on the QKD layer with metrics such as stable key rate, and quantum bit error rate measured, along with overall volume. The team wanted to extend this test by deploying a production equivalent 5G network between the PPK tunnel links and adopt PQ-TLS at subscriber-level to quantify the practical impact for specific use cases.

2.3 TLS Post-Quantum Cryptography Performance Investigations

Relevant research into Post-Quantum Cryptography and its impact on Web-based traffic services have presented challenges for standard services across the internet, utilising Transport Layer Security (TLS), specifically how users may be impacted by the migration to post-quantum algorithms to protect their data. In their paper 'Benchmarking Post-Quantum Cryptography in TLS' for PQCrypto Conference in Paris in April 2020, (Paquin, 2020) Paquin et al. present a framework to test the performance of PQC implemented in TLS on a focused scope of network conditions - network latency and packet loss percentages. This is the first instance that this author finds of TLS handshake delay as a factor of performance[2]. In their paper they cite previous progress made by Google and Cloudflare in this domain but mention

[2] One of a number of key performance indicators proposed in my research as 'Time to first Byte' indicating the overhead associated with additional setup incurred by adopting Post-Quantum algorithms

the difficulty in providing a "commensurate infrastructure" to test at scale across the open internet. To address this challenge, they used tools such as NetMirage and Mininet along with a confined lab experiment expanded to the public cloud. This helped to make the test results relevant and contextual. In a recent follow-up paper from January 2025 (Rios, Montenegro, Muñoz, & Ferraris, 2025), submitted to IEEE, Rios et al. discuss benchmarking post-quantum TLS and published findings that the overhead is comparable to existing classical cryptography. The testing focused on a single lab system used for focused experiments based on a controlled timeframe – the measure of performance was taken on the range of ML-KEM (FIPS 203) and PQC Signatures (FIPS 204) benchmarking how many TLS sessions could be achieved within a specified timeframe and also how many bytes were used to complete the transactions, using the liboqs library extensions for openssl. The focus on the specific primitives of the cryptographic components provides a key insight into the atomic operation of the classical and post-quantum key exchange and signatures as an indicator measurement of how user experience could be impacted. Although this brings us closest to how the post-quantum algorithms will impact TLS overhead, the key piece missing was the practical testing using a commercial or commonly used application to validate findings.

To extend this research, we must leverage both approaches to benchmarking TLS into a uniform set of metrics, that can identify if an application will be adversely impacted by the overhead associated with adopting post quantum algorithms and signatures. The proceeding chapters will describe the approach taken and provide visibility on the actual impact as closely as possible to real-world functionality, to derive a perspective of the impact on user experience.

3 Research Methodology

The plan is to structure all tests around the categorisation criteria using NIST's PQC security levels as outlined in the following paper (Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, 2016), focusing on Security Levels 1, 3 and 5.

Table 1 – Cipher/Signature/Security Level

Cipher Suite	KEX Algorithms	Signature Algorithms	Description
PQC L5	MLKEM1024	ml-dsa-87	Highest security utility 1,568 Byte public key, 3,168 Private key and 1568 Byte Ciphertext, signature 4,595 Bytes
PQC L3	MLKEM768	ml-dsa-65	1,184 Byte public key, 2,400 Byte private key and 1,088 Byte ciphertext, signature 3,293 Bytes
PQC L1	MLKEM512	ml-dsa-44	800 Byte public key, 1,632 Byte private key and 768 Byte ciphertext, signature 2,420 Bytes
Hybrid L5	secp384r1+MLKEM1024	ECDSA P-521	Highest security hybrid mode using a 192-bit Classical key but 256-bit MLKEM key
Hybrid L3	X25519+MLKEM768	ECDSA P-384	1,216 Public key 2432 Private key and 1,120 Ciphertext - Combines classic DH with PQC using X25519 Elliptical Curve and MLKEM key
Hybrid L1	secp256r1+MLKEM768	ECDSA P-256	Combines classic ECDH with PQC KEX. (kyber768 - pre-standard)
Classic L5	P-521	ECDSA P-521	133 Byte public key, 66 Byte private key and 133 Byte ciphertext, 132 Byte signature - high security
Classic L3	P-384	ECDSA P-384	97 Byte public key, 48 Byte private key and 97 Byte ciphertext, 96 Byte signature - mid-level secure

Classic L1	P-256	ECDSA P-256	65 Byte public key, 32 Byte private key and 65 Byte ciphertext, 64-byte signature - standard TLS etc.
Legacy L1	RSA-2048	RSA	Uses 256 Bytes across keys and signatures with 2048 ciphertext - widest use today for default secure comms

We incorporate a two-phase approach to the research. The initial stage will test the security primitives and identify the key performance indicators to use for the analysis of the reference algorithms outlined above and provide a comparison of results. The focus for this stage will be on the performance of the primitives and the exchanges within the procedures for secure connectivity using each key and signature at the defined security level.
The next stage will utilise a commercially available tool to measure complimentary performance metrics in a broader sense, to generate HTTPS traffic baselined on the parameters, categories and levels used in phase 1. This traffic will traverse virtual machine instance-to-instance via 10Gigabit Ethernet interface bound to each instance, connected by a cable. This allows us to quantify the performance impact in a maintained environment, considering broader influences such as network interface stack, discrete virtual machines and operating systems vs. standalone container functions. This allows us to quantify the impact of atomic operations vs. actual real-world delay factors. Finally this environment will be used to test emulated real-world SaaS traffic (using Microsoft Office 365 based interactions) to illustrate the actual performance impact on user experience for each set of algorithms and compared with the previous test outputs.

3.1 Phase 1: Classical/Hybrid/PQ-TLS Primitive Test Environment

For the first phase, I am building a testbed that facilitates the measurement of classical, hybrid and post-quantum cryptography performance across a number of key performance criteria.
It also provides a dashboard with visibility of the performance metrics associated with user experience.
The tool is designed to be as lightweight as possible facilitating the execution of tests on each key/signature pair from a web-based configuration page, at the defined security levels and output these metrics to an HTML dashboard for comparison and visibility.

3.2 Phase 2: Real-World Traffic Emulation Test Environment

For the second phase, I introduce a commercial test tool called 'TeraVM™' on the same test environment to generate client and server HTTPS traffic based on the same TLS profiles outlined in table 1.

3.2.1 Baseline HTTPS Tests Comparison

The test profiles are provisioned and executed comparing results to the initial primitive assessment. As we are running on a single host the objective is to identify the impact associated with the machine level functions. The establishment of definitive measurements based on this approach means that any further delay incurred by introducing network traversal can be quantified.

3.2.2 Testing Real-World SaaS Traffic Profiles Comparison

To conclude the testing, the commercial test tool will be used to generate HTTPS traffic profile approaching real-world behaviour for SaaS traffic in a controlled repeatable method, as before.

We use individual client and servers dedicated to each of the cipher profiles from table 1[3] so that comparisons of the ciphers and security levels, can be achieved and actual user experience observed when compared with the primitive's assessment and baseline derived in earlier tests. In order to ensure consistency of measurements we will use raw traffic capture and protocol analysis during test runs, which will also be used as a verification mechanism to ensure the traffic is behaving as expected under the controlled conditions.

4 Design Specification

The architecture of the systems used for the user experience research and tests are outlined below, along with descriptions of the metrics, key performance indicators, and derivations to present the quantitative results analysis.

4.1 Cassini – Post-Quantum Cryptography Experience Test

The following diagram outlines the custom-built testbed designed for measuring the primitives used in the secure data exchange undertaken when Secure HTTP is used to communicate and deliver data across the web.

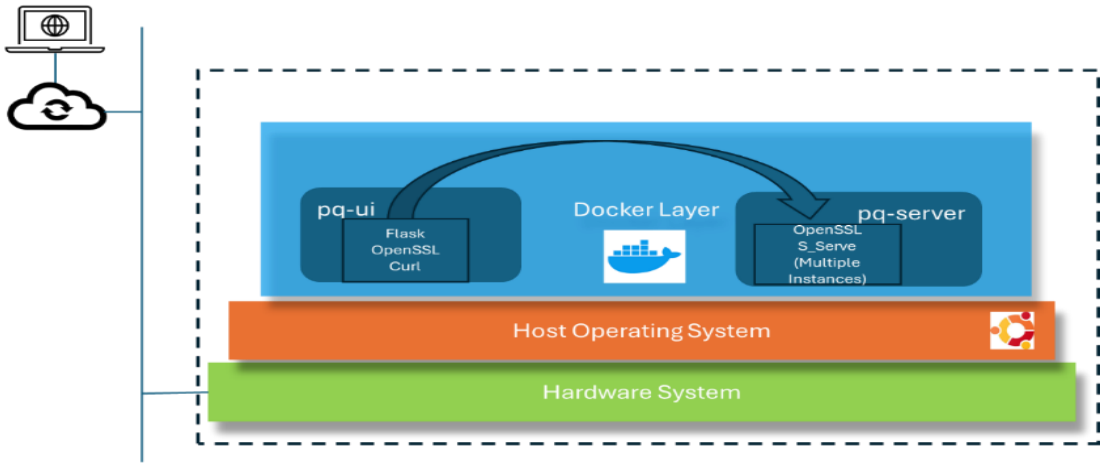


Figure 1 – Bespoke Post-Quantum Cryptography Test Environment Architecture

4.1.1 Designing and Comparing Application Metrics

A web client's timing provides a high-level, user-centric view, but it conflates two distinct sources of delay:

- **Computational Delay:** The time spent by the CPU on the cryptographic operations (key generation, signing).
- **Propagation Delay:** The time it takes for packets to travel across the network between the client and server (network latency).

By harnessing the OpenSSL utility 's_time' and using 'curl' we can isolate key factors :
Establish a Performance Baseline: The 's_time' results provide the pure cryptographic cost of each cryptographic profile, described as testing of primitives. This measures discrete handshakes per second. This is the low-level visibility as primitive baseline.

[3] One key difference is that TeraVM does not support Post-Quantum signatures yet so Classical signatures will be used to authenticate the client and server traffic – comparisons of signature exchange are not made.

The measurement itself is passive, not active: The timing logic in our testbed (utilising curl's internal timing variables and openssl s_time's reporting[4]) does not perform additional computational work during the handshake phases. It operates around the connection process, simply reading the start and end timestamps from the underlying stack (OpenSSL/Kernel).
Standard, Native Interfaces: The tools employed (curl, openssl) are not heavy application-layer scripts. They are directly compiled, native binaries that interface directly with the kernel's networking stack and the OpenSSL library. They provide direct access to high-precision internal timers (such as *time_starttransfer* in curl). This is a standard method for low-level protocol analysis precisely because it is designed to be lightweight, highly optimized, and non-intrusive.

4.2 TeraVM™ Network Application and Security Performance Test

The architecture of the commercial test tool is outlined below. TeraVM, developed by VIAVI Solutions (Solutions, 2025) is virtual machine-based and consists of a controller instance, comprising of a Web-based UI, incorporating an embedded Java client user interface. Provisioning and execution of the tests and presentation of results are managed from this instance. The provisioned traffic profiles are copied down to the dedicated application traffic generation modules and generated across the nominated interfaces into the network. Each application traffic module also records metrics for each PDU sent and received, reporting to the controller. This communication is managed via a dedicated internal Linux bridge operating as a virtual switch. This ensures that the control aspects and the test data are isolated from each other minimising contamination and ensuring the integrity of results.

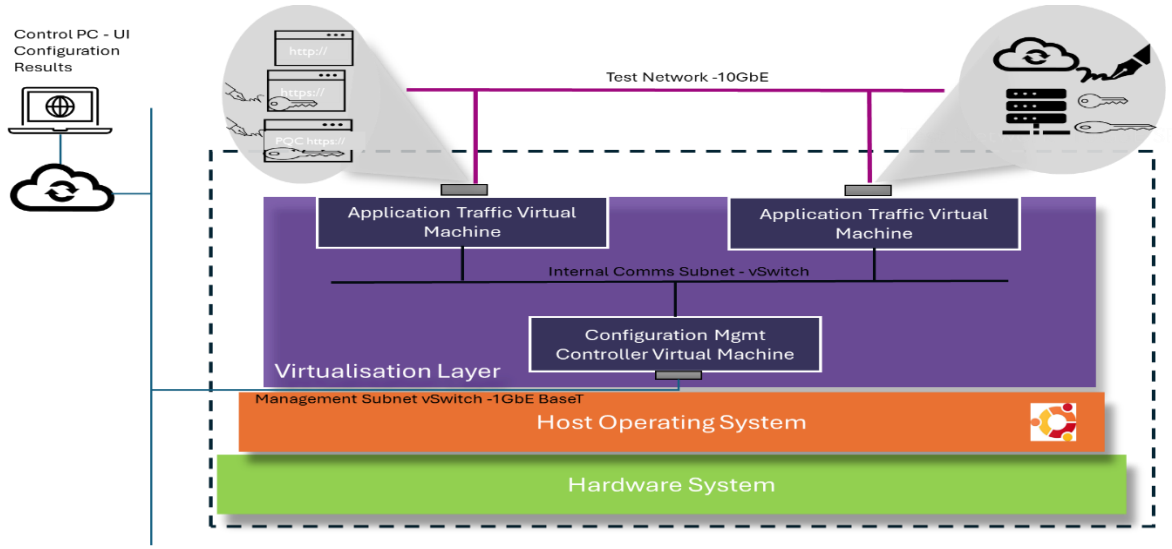


Figure 2 – TeraVM Test Tool Virtual Machine Architecture

Both test software systems present a range of performance metrics which can be used to derive how each of the different profiles may present user experience as outlined below

[4] Whilst building and testing this controlled environment a bug in openssl implementation was encountered – a known issue (Noack, 2017) I worked around this issue for my Connections and CPS statistics reporting by relying on calculation of the overall connections divided by the test duration input (real time), not the 'user time' read from the s_time utility, implemented in Python flask.

4.3 Performance Metrics and Indicators

The key metrics we are most interested in are outlined in the table below, with a description and context.

Table 2 – Metrics and Performance Indicators

	Metric	Description
1	Connections	The count of user communication sessions that occur within a specific test window. A connection is defined as TCP+TLS+HTTP exchanges
2	Connections Per Second (CPS)	The rate at which connections defined in 1 are observed in a single second
3	TCP Connection time (Minimum/Average/Maximum)	The time taken for each connection to initially establish using a handshake protocol.
4	TLS Handshake Time (Minimum/Average/Maximum)	The time taken to negotiate the secure exchange between the endpoints and authenticate/verify.
5	Time to First Byte (TTFB)[5] (Minimum/Average/Maximum)	This is the time from the client request to the response receipt and the first block of data. This occurs after initial handshake and secure negotiations complete.
6	Cert Bytes (DER)	Represents the amount of data to send the Leaf Certificate, reflecting the signature and key size used to authenticate during secure negotiation
7	Round Trip time (RTT)	Metric defined as the time to send a packet from a source endpoint and to receive the acknowledgement of receipt from the destination endpoint.
9	Byte Count (In/Out)	The number of bytes transferred. This is typically a core performance metric for network traffic. For this analysis we use this with the Packets transferred to observe overhead associated with PQC and Hybrid algorithms due to the larger size signatures and certificates.
10	Packet count (In/Out)	This is a count of packets transferred. This is used to gauge the overhead incurred when using PQC or hybrid certificate and signatures as the larger key sizes result in segmentation and potentially fragmentation of the PDUs which has a greater impact on the efficiency of a network stack.

5 Implementation

To provide a uniform approach to testing and analysis, external factors of test execution are aligned in both utilities. For the initial primitive verification the resource size that is sent as part of the HTTPS exchange is set to ten bytes – this ensures that the protocol is engaged but with minimal impact. A uniform duration is also used - ten seconds. This gives a consistent

[5] The definitions between Cassini using the openssl 's_client' function and TeraVM differ – TTFB in TeraVM represents the time from the initial SYN of the TCP handshake to the first data block. For the purposes of comparison the raw network data was captured during the TeraVM test runs and the TTFB measurement derived directly from the PDUs using the tshark utility.

testing window for each of the profiles and also facilitates equivalent comparisons across the test utilities. This approach is progressed to the emulated SaaS traffic profile providing a baseline for evaluation under conditions more reflective of a user with variable profiles for data resources and variable timing primarily dictated by the network propagation delay.

5.1 Test 1: Compare Primitives across all Cipher Categories and Security Levels – Cassini

Cassini - the test utility developed for this research, is used to test and display results. The system uses a web-based front end to control test profiles. The operator chooses the cryptographic profile from the drop-down list, configures the duration then executes the test by clicking on the 'Run Test' button. Figure 3 displays the browser home page.

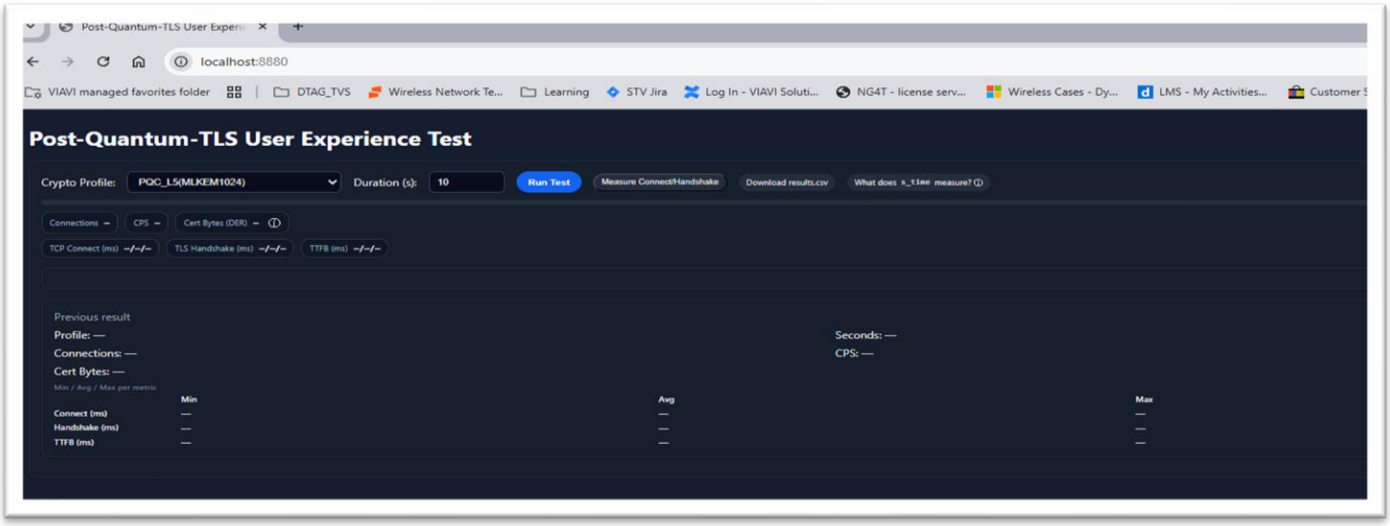


Figure 3 – Cassini - Web-based UI – Test execution home page

As each test is run in sequence, a context is built of the overall performance comparison in the UI results dashboard :

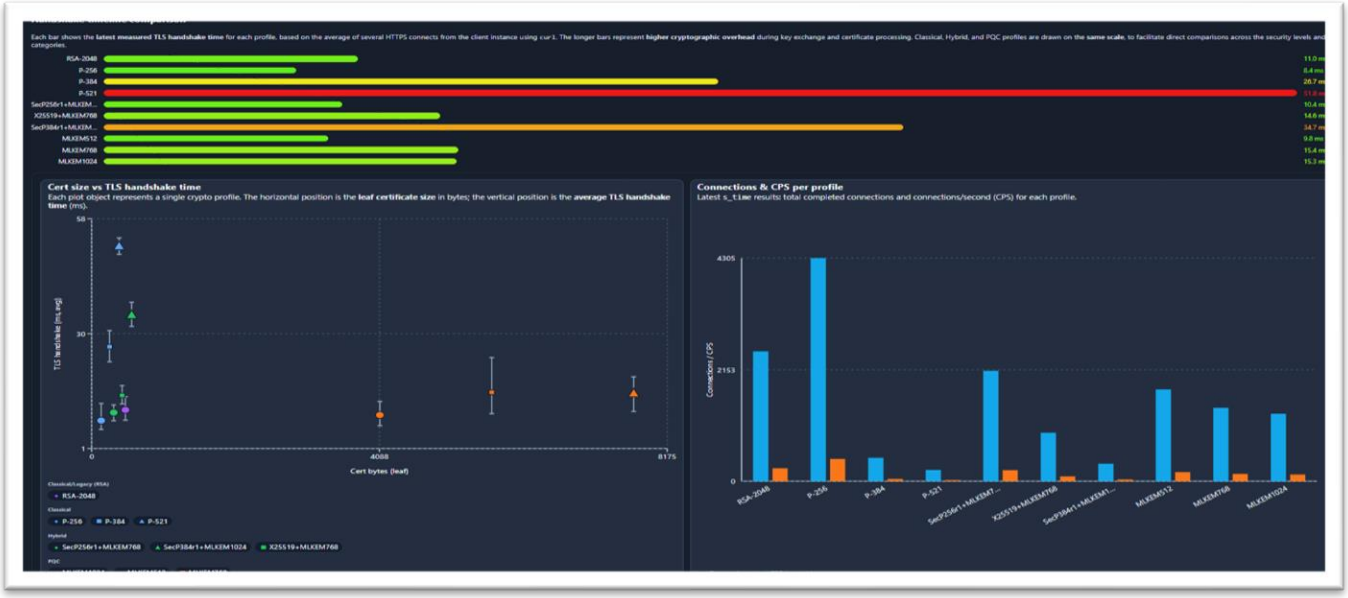


Figure 4 – Cassini PQ-TLS Test Results Dashboard

The results dashboard encompasses a number of views to highlight the performance of the cipher profiles

- Timeline comparison – a heatmap-based comparison of the TLS handshakes
- Cert Leaf vs. TLS Handshake scatter plot – graphs the average handshake time vs. signature transfer bytes of each profile
    - Utilises whisker plot to provide maximum and minimum visibility
- Connections and CPS bar chart – counts the number of overall connections and connections per second during each test execution

Each of these views provides the user with an instant perspective of performance on a per profile basis.

5.2 Test 2: Compare KPIs across all Cipher Categories and Security Levels - TeraVM

For the purposes of this analysis I create 10 specific profiles in separate test groups to ensure separation of the test functions.
NB: All test groups were configured manually from first principles, no templates or pre-existing test profiles were used, there are no pre-loaded profiles provided in the tool.
The system includes a command line framework that facilitates automated testing. A bash script which interacts with the command line interface to run each test above for the specific duration and stops in between each test run for five seconds. Performance data is collected using the TeraVM results data – in CSV format. To align specific KPIs to the Cassini test utility, PDU capture of the raw data is taken, with automatic ssl keylogging enabled. This capture is run before the first test initialises and terminates after the conclusion of the final test. This raw data capture is saved and post-processed to extrapolate the KPIs to compare with Test 1.

5.3 Test 3: Testing Real-World SaaS Traffic Profiles Comparison – Microsoft 365 traffic

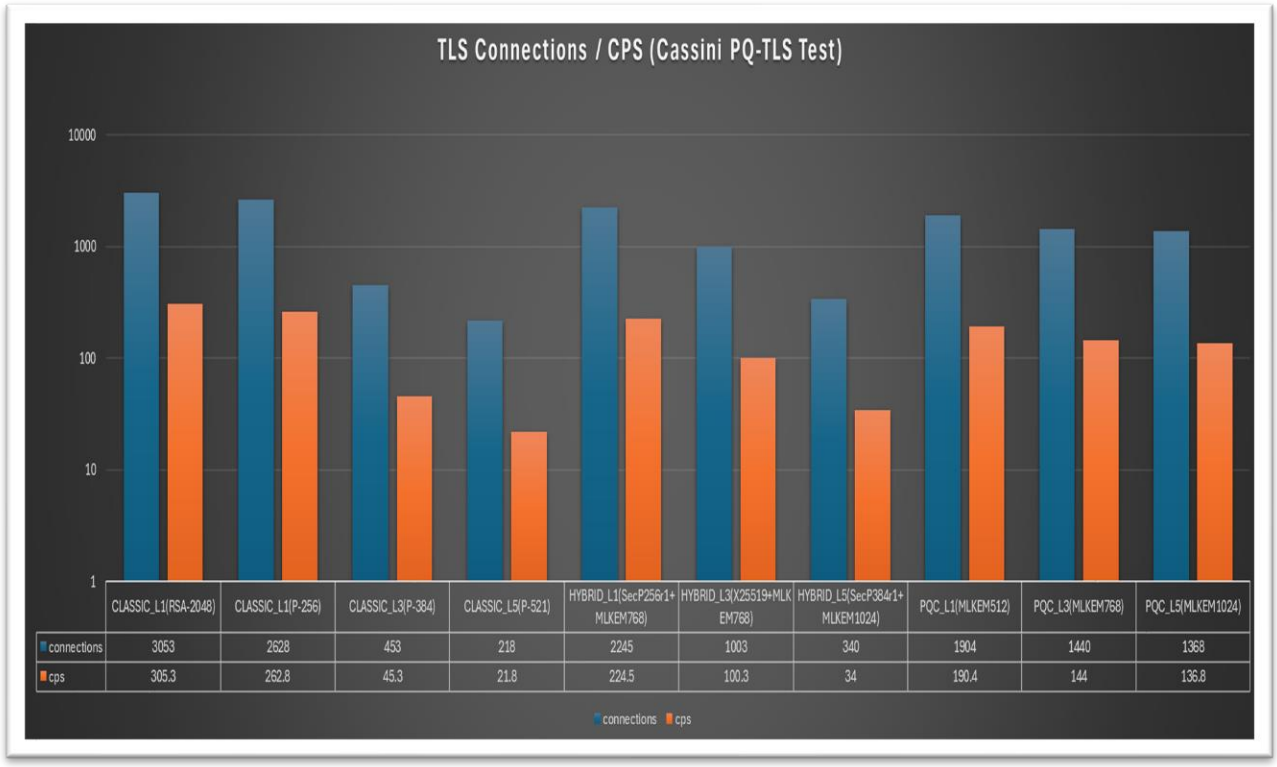
Using the baseline tests, we establish a foundation of performance that has been validated from two distinct sources. The TeraVM tool has in-built traffic profiles for a range of Software-as-a-Service (SaaS) applications, we can use these traffic profiles to enhance the baseline tests with realistic traffic for each cryptographic profile and category. For this test, the profiles are merged into one test and a service state mechanism is used to control the activation and termination of each profile within the test group using command line. In addition, a raw traffic capture is initialized under the same conditions as Test 2 above. The traffic profile chosen is Microsoft Office 365, as it is one of the most widely adopted productivity SaaS offerings in business environments. The traffic profile consists of Office 365 connectivity, along with Sharepoint upload and download activity and a network storage request using the OneDrive application.
The results of all tests and insights derived are discussed in the next section.

6 Evaluation of Results

Initial analysis and performance data yield insights relating to both new and existing cipher and signature profiles in use. The following data was taken from the initial dataset using the custom developed tool for this research – Cassini.

6.1 Dataset 1: Compare SSL Primitives across All Categories and Levels

The results in figure 6 below show us that RSA as a legacy encryption function (using TLS1.2) has the highest number of connections and subsequently connections per second of any other cipher profile underpinning the theme and default outcome of less security, more performance.



	CLASSIC_L1(RSA-2048)	CLASSIC_L1(P-256)	CLASSIC_L3(P-384)	CLASSIC_L5(P-521)	HYBRID_L1(SecP256r1+MLKEM768)	HYBRID_L3(X25519+MLKEM768)	HYBRID_L5(SecP384r1+MLKEM1024)	PQC_L1(MLKEM512)	PQC_L3(MLKEM768)	PQC_L5(MLKEM1024)
connections	3053	2628	453	218	2245	1003	340	1904	1440	1368
cps	305.3	262.8	45.3	21.8	224.5	100.3	34	190.4	144	136.8

Figure 5 – Connections and CPS per Crypto profile - Cassini

A significant reduction in Connections and CPS for the current Eliptical Curve classical ciphers are observed as we increase security level. The merging of PQC ciphers and classical in the hybrid categories and levels improves performance at the entry level but has the opposite impact of lowering performance at the highest security level when comparing to pure PQC. What is interesting is that pure PQC ciphers outperform the current classical eliptical curve ciphers at level 3 and level 5 indicating an enhancement in performance is experienced for critical use cases, which does bode well for a fully post-quantum supported internet = 44% increase at security Level 3 and (conservatively) over 3 times more connections at security level 5.

The following test is run on the commercial test tool, TeraVM, with HTTP (unencrypted) traffic in the same test cycle – notice the stark difference in connections and connection rate ~68,000 HTTP vs ~7,400 HTTPS (EC P-256) - using logarithmic scale on the y-axis to normalise the results.

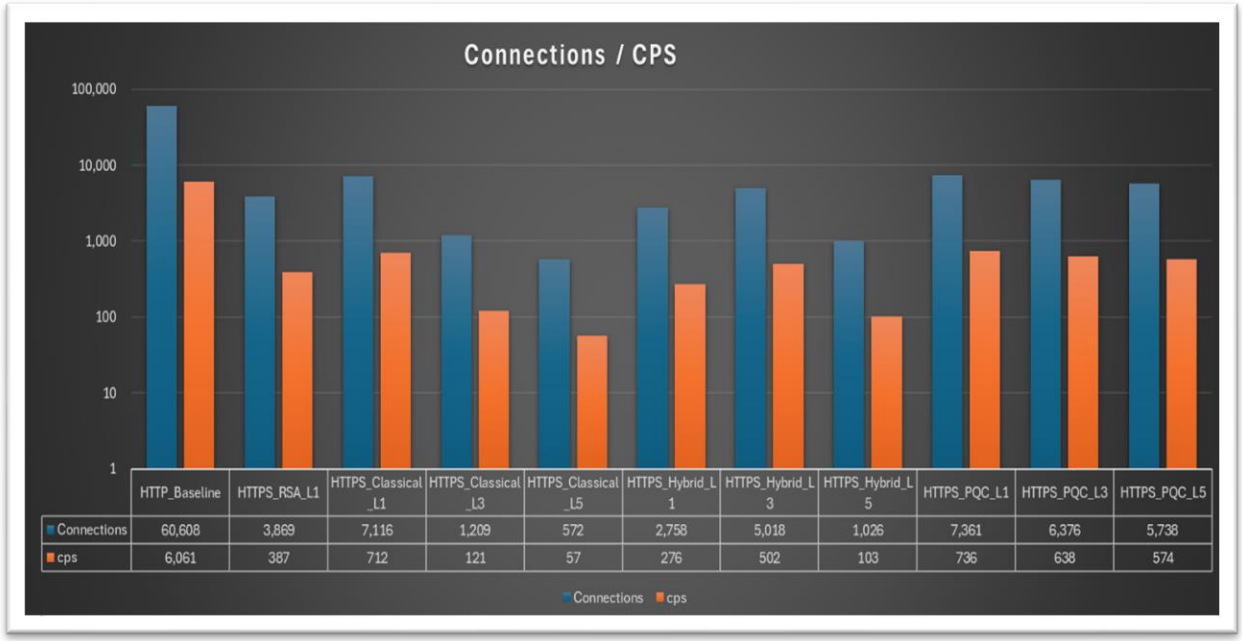


Figure 6 – Connections: HTTP vs. HTTPS Crypto Profiles – TeraVM

6.2 Dataset 2: Compare Handshake Metrics – Cassini vs. TeraVM

This next dataset breaks down each connection into its constituent components to identify where bottlenecks may manifest. These metrics highlight exactly where the common overhead resides within the connection – at the TLS handshake. We compare the relative TLS latency against its adjacent profile for each category. This is a visual indicator of the delay and computational overhead incurred by the complexity of the ciphers and signatures in transforming from cleartext communications to negotiated, authenticated end-to-end encrypted communications.

The scale for the measurements is in milliseconds. As expected, the TLS handshake on both test platforms manifests as the bottleneck. In both cases the highest contributor to TLS exchange is Classical level 5 – P521 – this overhead is observed in the standalone and the hybrid profiles and is significantly higher than all other profiles. Some interesting insights are presented when comparing discrete timings

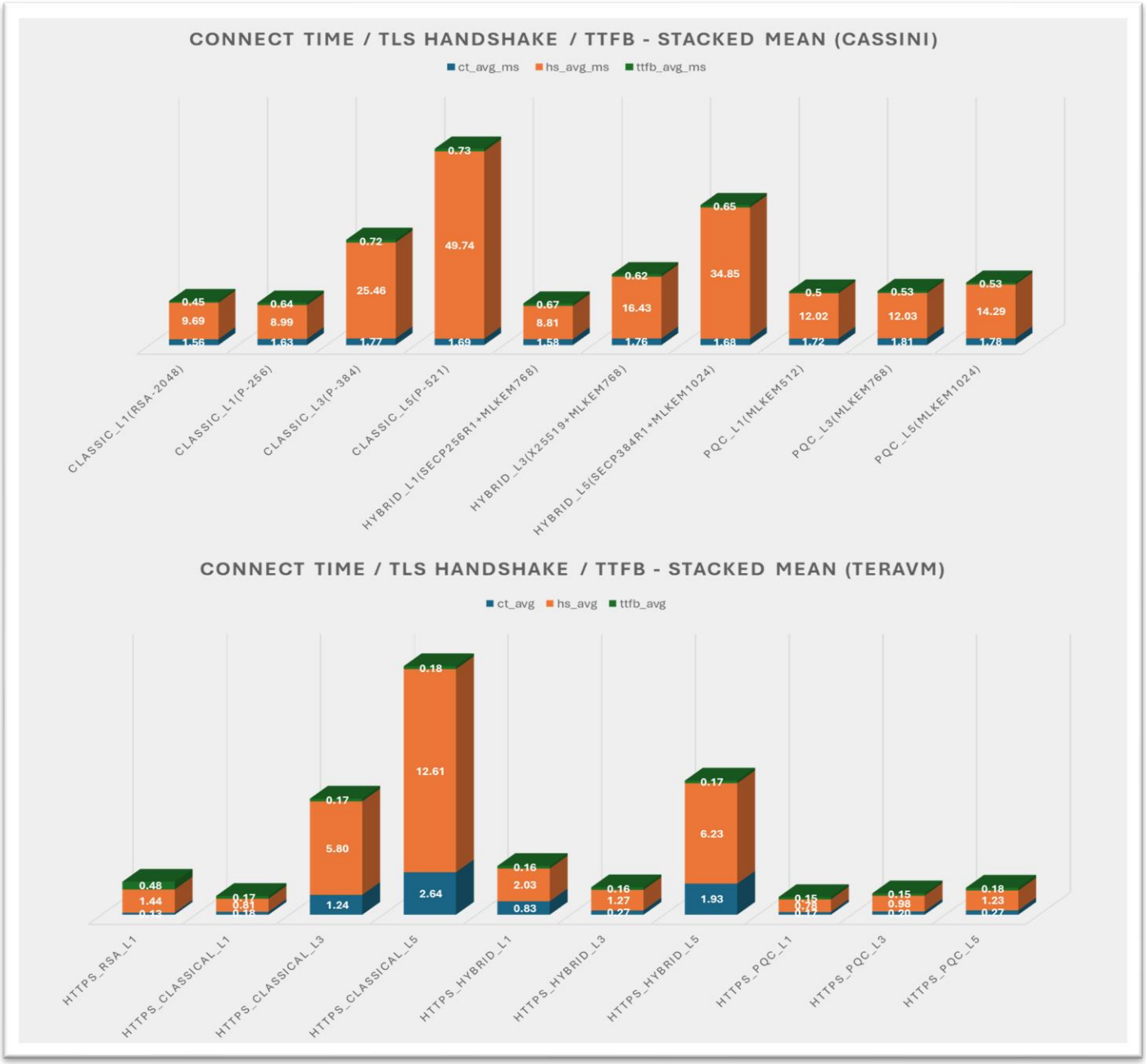


Figure 7 – Stacked Comparison of Application Latency per cipher profile, (TCP, TLS, TTFB)

1. The TLS handshake time for RSA, Classical (EC) and Hybrid are all higher than the post-quantum ciphers when using the connection-optimised tool commercial tool.
2. Cassini shows better performance in RSA and P-256 than the equivalent PQC L1.
3. The same pattern is true for L3 profiles, however at the highest security level PQC outperforms Classical and Hybrid. Bearing in mind that Cassini is using the significantly larger Post-Quantum signatures, TeraVM is using Classical signatures for the same authentication/verify exchange in the TLS handshake for PQC levels, which would account for the much smaller TLS latency observed in the charts above.
4. It is also worth noting that:
    a. the variation (max and min values) of MLKEM profiles is larger than the other cipher profiles (visible in the whiskers on scatter plots on Cassini dashboard)
    b. The TTFB is equivalent in all scenarios (this is the pure application-level latency, agnostic of the key and signature used)

6.3 Dataset 3: Testing User Performance with SaaS Traffic Profile

Testing with the SaaS traffic profile we lose the determinism of the previous tests due to variable byte and timing profiles. The performance data should follow the same outline patterns as the controlled test, for each cipher profiles.
Comparing the handshake analysis from the previous dataset to the new dataset presents a different perspective. As the data traffic is more complex, incorporating uplink and downlink traffic with variable session establishments, the analysis manifests a different set of results for Dataset 3:

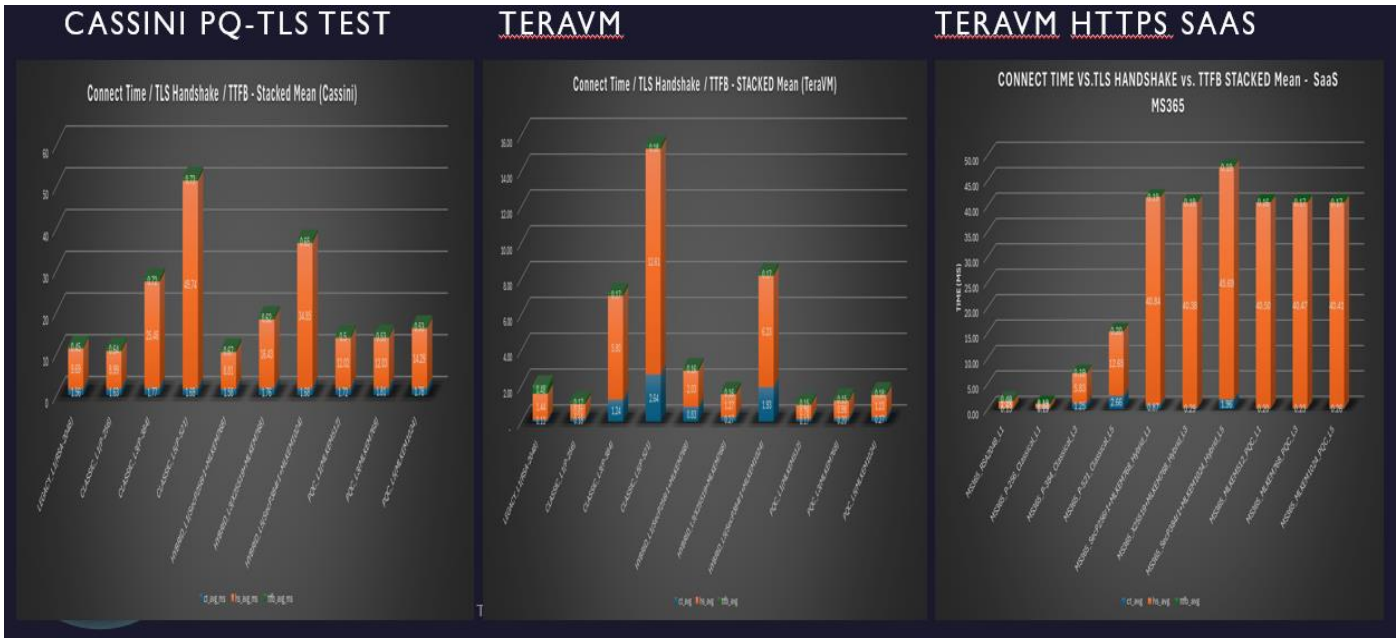


Figure 8 – Handshake Analysis across all three datasets (including MS365 SaaS traffic profile)

To understand the deltas observed I compare the average packets per connection for the profiles, the expectation is that more packets are required to process the connection for post-quantum profiles compared to classical exchanges due to larger keys and signatures. This is observed in the identical numbers for Cassini and baseline testing in TeraVM, providing further validation of the approach. The difference in numbers is observed for the TeraVM SaaS dataset for Microsoft 365 traffic, as expected, however the sequence per profile and general pattern is generally consistent with the other datasets as shown below.

The distinct pattern is identified regardless of numbers of packets within a connection, the sequence of packets used for each profile is consistent. We have a behaviour that is repeatable - from primitives testing to complex real-world traffic analysis.

Figure 9 - Comparison of TLS handshake and average Bytes vs. Packets per session (across 3 Datasets)

With the SaaS test traffic profile in use, it is worthwhile to re-visit the established performance KPIs - Throughput and Latency (Round Trip Time). The plots in figure 10 below show the highest throughput at Classical L1 (P256) profile and RSA next. Round trip times reflect the high values, with low RTT (both below 1ms). The highest round-trip time (Classical L5) does not reflect the lowest throughput neither does the second lowest or third lowest values – the delta being only 2ms and less than 0.5ms(500 microsecs) between second and third highest values. The lowest RTT values reflect lowest throughput values, but even fluctuations in RTT in Hybrid profiles make zero difference in the throughput observed as a result, the finding is that RTT values do not provide a universal indication of performance or user experience in this use case.

6.4 Discussion

From the results produced by the research, the traditional data traffic performance – bandwidth/throughput and latency/round-trip time – are not linear indicators of performance in secure communications and by extrapolation, user experience. The post-quantum keys and signatures although adding processing load due to larger key size and signatures during the critical TLS security handshake, do not suffer from additional propagation delay, in fact, TLS handshake performance is on par with the most efficient classical security profiles, consistently across the tools and datasets utilised. We see correlation when we examine the packet/byte exchanges of the TLS connections which appear to be independent of the volume of packets used to establish and complete each connection.

There were challenges and limitations encountered during this research. The lack of post-quantum signature support in TeraVM made load comparisons less compelling and may produce additional overhead on the real-world traffic testing dataset. The additional overhead

of having to take raw captures and post-process to extract equivalent performance metrics due to a lack of consistency in the metrics was extra effort but very worthwhile in terms of validation and deeper understanding of the behaviours.

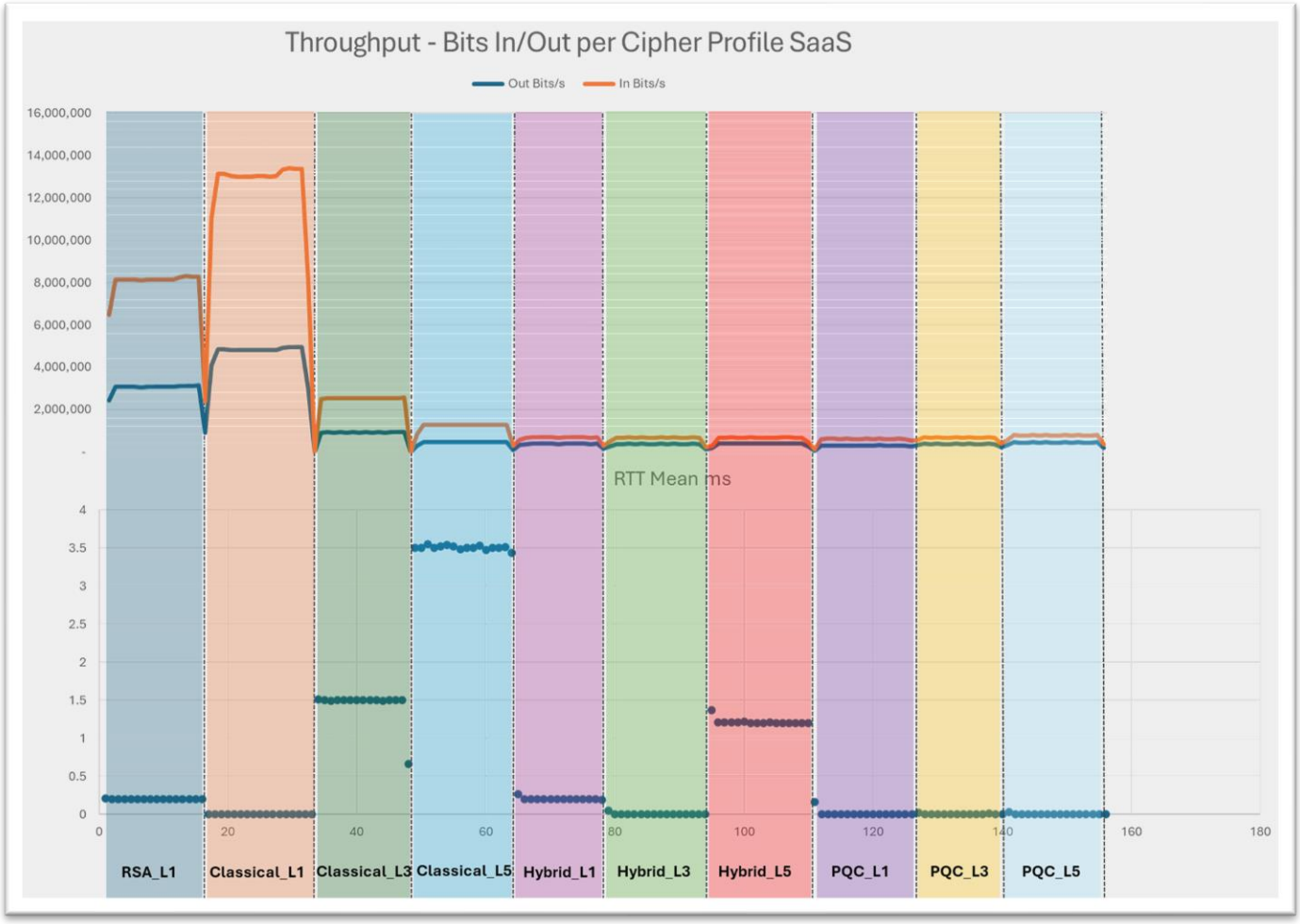


Figure 10 – Throughput and Round-Trip Time Comparison – SaaS Traffic

7 Conclusion and Future Work

This paper posed the following key questions: Can we measure and quantify the impact of adopting post-quantum cryptography on application performance and user experience? From the research and analysis conducted the answer is yes, it is possible to measure the impact of adopting post-quantum cryptography and it is possible to compare to existing security profiles. The results and specific KPIs examined demonstrate that quantification is possible by comparing overall connections, connection rates, granular measurement of TCP, TLS and Time-to-first-Byte along with the measurement of packets per connection and certificate Bytes transferred – each providing an insightful component in a multi-dimensional view of how the users experience is impacted.

Expanding on the original follow-up research questions - could PQC adoption present a detrimental impact on how transactions are conducted electronically? My conclusion is that the migration to post-quantum will not impact user experience, it is more likely to improve performance, from our analysis. The potentially challenging stage will be the hybrid migration phase, the need to support post-quantum and classical users. In the research conducted hybrid

profiles underperformed the classical and post-quantum profiles at each security level. The ideal recommendation would be to migrate directly to post-quantum cryptography but in practical terms, the realistic outcome will be to reduce the hybrid migration phase to as short a time that is practically possible.

Areas for future study and analysis - testing was performed using HTTP1.1 and without DNS. I would like to expand the tests to use HTTP/2 and QUIC plus HTTP/3 and to utilise current implementations of secure DNS with post-quantum cryptography incorporated, to reflect a complete view of secure user experience in the modern internet.

Another area of future research would be to combine the quantitative analysis from this research into a qualitative model, by introducing a rating scheme to provide quality scores at each level and develop a model to derive a quality score. This would provide the industry with a tool to assist and provide confidence in the migration initiatives for all users - service providers, financial institutions, government organisations and enterprises.

8 References

Aguilera, A. C., Clemente, X. A., Lawo, D., Monroy, I. T., & Olmos, J. V. (2023). First end-to-end PQC protected DPU-to-DPU communications. *Electronic Letters, 59*(17).

Asier Atutxa, A. S. (2024). Towards a quantum-safe 5G: Quantum Key Distribution in core networks. *Computer Communications, 224*, 145-158.

ETSI. (2025, February). *ETSI 104 015 v1.1.1 - Cyber Security (CYBER); Quantum-Safe Cryptography (QSC);Efficient Quantum-Safe Hybrid Key Exchanges with HIdden Access Profiles.* Retrieved June 20, 2025, from https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy Volume: 16; Issue: 5*, 38-41.

Noack, P. A. (2017, January 23). Performance measurement with s_time counts user time and not real time. *https://github.com/openssl/openssl/issues/2274*. Github.

O. Alia, A. H. (2024). *100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber.* Singapore.

O. Alia, A. H. (2024). Quantum-safe 10 Gbps Site-to-Site IPsec VPN Tunnel over 46 km Deployed Fibre. Optical Fiber Communication Conference (OFC) - San Diego: Optica Publishing Group.

Ojetunde, B. K. (2025). Performance Evaluation of Post-Quantum Cryptography Algorithms for Secure Communication in Wireless Networks. 22nd Consumer Communications & Networking Conference (CCNC) - Las Vegas: IEEE.

Paquin, C. S. (2020). Benchmarking Post-quantum Cryptography in TLS. *Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science()* (pp. 72–91). Paris: Springer, Cham.

Rawal, B. S. (2024). Challenges and opportunities on the horizon of post-quantum cryptography. *APL Quantum, 1*(2).

Rios, R., Montenegro, J. A., Muñoz, A., & Ferraris, D. (2025). *Towards the Quantum-Safe Web: Benchmarking Post-Quantum TLS.* Malaga: IEEE Network.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). Santa Fe, NM, USA: doi: 10.1109/SFCS.1994.365700.

Solutions, V. (2025, November). *VIAVI TeraVM - Application Emulation and Security Validation*. Retrieved from VIAVI Solutions Prodcuts and Services: https://www.viavisolutions.com/en-uk/products/teravm

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. (2016, Dec). Retrieved from National Institue of Standards and Technology: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf

Xu, Z. &. (2019). Network Traffic Type-Based Quality of Experience (QoE) Assessment for Universal Services. *Applied Sciences*, 9(19) 4107.