National College of Ireland

Quantum-Safe IAM

MSc Research Project
Msc. Cybersecurity

Keshav Singh
Student ID: 22101624

School of Computing
National College of Ireland

Supervisor: Prof. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Keshav Singh

Student ID: **x**22101624

Programme: MSc Cybersecurity **Year:** 1

Module: Research project

Supervisor: Imran Khan
Submission Due Date: 14th Dec

Project Title: Quantum-safe IAM……

Word Count: 6254…… **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: Keshav Singh……

Date: 14-12-23……

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):	

Quantum-Safe IAM

Keshav Singh
22101624

Abstract
Modern quantum computers threaten the very foundation of IAM systems, this paper provides a solution to the same in the form of post quantum cryptography integration. With the high innovation in quantum computers, there is an emerging requirement for these systems to increase their security posture against quantum computers. Integrating quantum resistant services into IAM components is the objective of the research. This is done through the integration and deployment of approved cipher suites, enhancements to TLS 1.3, and the utilization of NIST-approved algorithms such as SPHINCS+, CRYSTALS-KYBER, FALCON, and CRYSTALS-Dilithium for digital signatures. The research methodology followed is to evaluate and integrate post-quantum cryptographic algorithms, ciphers, and digital signatures into IAM infrastructures. Data collection is achieved by packet analysis during the TLS handshake using Wireshark. Suitability and scalability of NIST approved algorithms are some of the findings of this paper. Special emphasis is given to hybrid algorithms that offer Level 5 cryptographic security approved by NIST's post-quantum encryption standardization process. Potential areas for future work are identified that will aid in public and commercial deployment. Effectiveness and compatibility of these solutions in securing IAM systems against quantum threats is further summarized. But the biggest contribution is aimed to be foundation for future researchers to be helped in following through in quantum resistant IAM solutions.

Keywords: TLSv1.3 web server architecture, Hybrid key exchange mechanism, Post quantum cryptography, Liboqs, X.509 certificates.

1 Introduction

Contemporary digital security uses traditional relatively older cryptographic techniques such as RSA and elliptic-curve encryption. However, the evolving field of quantum computing emerges a severe threat to these traditional methods. Quantum computers, as they advance, have the potential to solve complex mathematical problems that form the base for conventional cryptographic systems. While large-scale quantum computers are still not easily accessible to the public. For large corporations like Google, IBM and some education institutions, building quantum computers is an active area of research. Therefore, a need arises to develop quantum-resistant services for integration into Identity and Access Management (IAM) infrastructures.

This research is inspired by the urgent need to secure IAM components against potential breaches and unauthorized access with the aid of quantum computers. These include safeguarding personally identifiable information (PII) during transit and storage, critical data like military security information, bank account details, and propriety data. The advent of quantum computing is believed to significantly impact IAM systems, especially when considering encryption and authentication.

Of special concern is the vulnerability of asymmetric encryption widely used in public key cryptography. It is believed to have started with Shor's algorithm—an innovation in quantum

computing. Asymmetric encryption, which is widely used in many contemporary cryptographic systems, protects data exchange through two different but mathematically joined keys. Shor's algorithm (Shor, 1997) constitutes a threat as it allows threat actors to factorize encryption keys in just polynomial time. This threatens the integrity of digital signatures, potentially allowing data decryption and compromising authentication processes. Realizing this threat, a report by Craig Gidney from Google and Martin Ekera from the Royal Institute of Technology (Gidney & Ekerå, 2021) suggested that the RSA encryption could be compromised in approximately 8 hours. RSA technique is the same which currently protects our identities and confidentiality over the internet. To secure sensitive data, the development of algorithms resistant to quantum attacks is crucial. In recent times, the creation of quantum resistant algorithms is already underway but the adoption is still in its early stages. In response to this emerging cryptographic reality, standardization bodies like ETSI, NIST, and IETF have initiated efforts to transition and standardised approach towards a post-quantum era. NIST, in particular, has identified the first four quantum-resistant algorithms (NIST, 2022) and had commenced an intiative to standardize the process to choose the next generation of industry-wide public key cryptographic algorithms.

1.1 Research Objective

The specific objective of this research is creating quantum resistant IAM services through the exploration and application of post-quantum cryptographic algorithms. Key components include the integration of approved cipher suites, enhancements to TLS 1.3, and the utilization of NIST-approved algorithms like SPHINCS+, CRYSTALS-KYBER, FALCON, and CRYSTALS-Dilithium for digital signatures (NIST, 2023). The expected outcome is to secure identities while being authenticated and authorized, as well as accesses being unique to all users according to company access policy. Web applications being used for the access are less prone to quantum computer attacks in the future.

1.2 Research Question

Incorporating post-quantum cryptographic algorithms into IAM systems will establish a defense against potential quantum computer attacks. "How can we start our process of movement of our system to a quantum resistant one?". The process to follow for adoption of quantum-resistant key exchange mechanisms and digital signature algorithms into IAM components is the only way to secure it. The name and specifications of algorithms and digital signature configurations to be used and get an idea of the compatibility of the same. The algorithms used align with NIST standards and are facilitated by projects like Open Quantum Safe (OQS), hence are the best possible resources to be used.

2 Related Work

2.1 The quantum threat to current IAM

The document referenced from source (Shor, 1997) discusses the need for systems resilient to quantum threats in the traditional landscape. The study produces a new discovery to factor

2048-bit RSA numbers in less than 8 hours. It does so by using 20 million noisy qubits. The authors show their method of computing discrete logarithms over finite fields and factoring integers by various methodologies and optimization techniques. They assess the approximate cost of large-scale quantum computer production in both the abstract circuit model and under plausible physical assumptions for systems based on superconducting qubits. Additionally, they also provide specific cost estimates for cryptography-related concerns. Surprisingly, their anticipated costs are significantly cheaper than earlier work done with the same physical assumptions.

The authors further compare their findings against the integrity of RSA encryption's traditional use in cryptography. They show that their research raises the need for postquantum cryptography and quantum resistant cryptographic protocols. It surveys the current state of quantum computing and its probable impact on cryptography and various domains. The study serves as a wake-up call to post quantum cryptography development. Especially after the work done by them in redefining the hardware prerequisites in this field.

2.2 Post Quantum cryptography

Developments in the sphere of Post-Quantum Cryptography (PQC) are now a pivotal point for rigorous endeavors to strengthen existing systems against quantum computing's potential risks. The main purpose of Paper (Xu, Mao, Sakk, & Wang, 2023) is to concentrate on the implementation of a post-quantum cryptography scheme based on lattices, with a particular emphasis on delving into the SABRE algorithm and its associated Module Learning-withRounding issue within the PQC framework. The material introduces fundamental concepts and works on the current state of PQC candidates. It praises the talked about design elements of a lattice-based encryption system. It even addresses the implementation, setup, mathematical reference model, and methodology in development of quantum-safe algorithms. In this research, the application lattice-based techniques known for their robustness in PQC is advocated to be the best. However, it's crucial to note that even though these techniques are effective they also come with a compromise on speed and efficiency. The National Institute of Standards and Templates (NIST) presents five primary competitors in the field of PQC, namely code-based, isogeny-based, lattice-based, multivariate, and hash- or symmetric-based encryption schemes.

CRYSTALS-Kyber was selected as the initial approach for key encapsulation due to the third phase of NIST's process for standardizing public-key cryptography systems, known as PostQuantum Cryptography (PQC). The publication (Policarpo, Nery, & Albuquerque, 2022)introduces an FPGA co-processor for Crystals-Kyber by utilizing the Xilinx Vitis HighLevel Synthesis (HLS) tool. To put it simply, this tool lets you make use of hardware accelerators and with a high level of flexibility and performance. By employing VHDL or Verilog, the HLS tool enables the synthesis of a specification for the Register Transfer Level (RTL) architecture. In this study, Verilog served as the synthesis language for CRYSTALSKyber C/C++. The authors presented their findings on various parameters such as performance, circuit area, and power consumption. These findings provide support for the implementation of the CRYSTALS-Kyber key encapsulation technique within a quantumsafe IAM architecture.

The two previously mentioned studies have substantively progressed the understanding of post-quantum cryptography's optimal employment within today's environment.

2.3 X.509 Certificates

X.509 certificates are employed in IAM systems willingly vulnerable to quantum threats despite having a robust public key architecture. There is an urgent impetus of quantum-safe cryptography and its related technologies in ensuring the integrity, usability, confidentiality, and non-repudiation of X.509 certificates. Depicted in the academic work (Kinkelin, Von Seck, Rudolf, & Carle, 2020) a thorough research on strengthening X.509 certificates have been carried out. This paper thus uses Hyperledger Fabric which is an open-source smart contract framework and distributed ledger for its implementation. Scope is to establish a multi-party policy-defined validation and authorization process for requests in certificatesigning facilitating effective functioning of a X.509 certification authority and the authorities of registration under its control. Though the proposed method may not inherently provide quantum security, yet it stands a robust contender especially when complemented with Post Quantum Cryptography (PQC).

2.4 Transport Layer Security

From the paper (Lokesh B & Kaulgud, 2023), it goes deeper into the TLS security evaluation, with an explicit summary of Open Quantum Safe (OQS) project. The OQS research quantum-safe digital signatures and KEM (key encapsulation mechanisms), which are key to securing Identity and Access Management systems. In the context of TLS, the research concerns performance regarding the use of different cryptographic algorithms. Of primary contenders, Kyber, Sabre, and Newhope, the best key size of Sabre makes it while its operational efficiency is within sub-millisecond.

The analysis also assumes a code-based approach with inclusion BIKE, NTRU, with the representation of Frodo. Also, SIKE is deployed to do data encapsulation or decapsulation that completes the operation in less than 3 seconds using sufficient key size. In resourceenabled environment (REC), Sabre outperforms for key encapsulation mechanism (KEM) compared to BIKE, Kyber, HQC, and FrodoKEM over a set of assumed parameters. Paper discusses various suites of ciphers, use of constant KEM on the way of signing and verifying processes and vice versa. The time duration of handshake in range from 80 to 90 milliseconds in case of transport layer security. The paper provides a lot of review on TLS security customized towards a quantum-safe IAM while displaying commendable analysis across diverse cryptographic algorithms and their applicability in such contexts.

2.5 Multi-Factor Authentication

Quantum-resistant Multi-factor Authentication is the focus of a pertinent investigation on quantum security outlined with the publication (Murray & Malone, 2021). The study proposes

quantum multi- factor authentication approach which refers to the quantum communication complexity inherent in hidden matching. By employment with quantum token, it facilitates a step-up graded authentication for users. This protocol is further detailed, demonstrating its applicability in a predominantly traditional scenario. The work explains the integration of this approach into SASL (Simple Authentication and Security Layer) and delves into emerging security considerations. A comparative analysis is presented, contrasting this method with the latest advancements in MFA (multi-factor authentication) processes. It's crucial to note that given the quantum-computing landscapes at the time of the research, a practical hardware based application is not currently viable due to the limited storage duration of qubits in quantum memory.

In a separate contribution, detailed in paper (Wang, Wang, Cheng, & He, 2023), an enhanced approach to quantum-secure MFA is presented. This system incorporates a Wang-Wang's "fuzzy-verifier + honeywords " strategy and lattice-based key exchange within a password authentication system based on smart card (IEEE TDSC'18). Notably, Quantum2FA addresses potential vulnerabilities, including leakages of signal attacks and mismatch in key attacks against lattice-based key exchange schemes which can be referred by ACISP'18, CTRSA'19 . The method imposes specific requirements, necessitating the attacker to start the key exchange to analyze the given signal. Additionally, honeywords are incorporated to detect key disparities between the server and the smart card, mitigating the risk of loss of smart card attacks. However, this method is more suited for mobile based devices and is heavily based on microcontrollers.

Both solutions contribute significantly to the quest for securing MFA in a quantum-safe manner. Nevertheless, it's emphasized that the initial solution's implementation is currently unfeasible with existing hardware resources, demanding substantial advancements and the discovery of new, efficient algorithms for practical implementation.

2.6 Quantum-safe Authentication

The paper (Murray & Malone, 2021) serves as a direct illustration of an optimal solution adviced for quantum-safe authentication. Within the given information-theoretic context, the authors establish stringent upper limits on the success probability for adversaries attempting impersonation and substitution attacks, bounded by $1/|T|+'$ and $+|T|'$, respectively. An proper example provided in the paper attains this bound, underscoring the sharpness of the bound even when it surpasses initial expectations. A similar observation holds for trace distance. In light of these findings, Wegman-Carter authentication emerges as a favorable choice for integration into a quantum-resistant IAM architecture, especially when being compared to alternative propositions. Nonetheless, the adoption of the Open Quantum Safe method for authentication has gained traction among researchers due to its perceived ease of implementation and prototyping.

2.7 Quantum Key distribution

Quantum Key Distribution (QKD) is one of the suggested solutions to the key distribution problem used in IAM systems. Beside RSA or ECC, there also exist other public-key scheme based key distribution techniques. However, Quantum key distribution being used as a cryptographic tool provides cyber protection that is guaranteed by the laws of physics unlike traditional public key techniques. It follows that QKD, information theoretically secure method of the key establishing against any quantum attacks from both sides. In paper there was given the overview and comparison of various techniques of quantum key distribution based on the phase coding and computer simulation of this process. All these subjects get into an umbrella of quantum cryptography 's generators of making secure communication protocols which apply the laws of quantum physics. The paper designs a QKD using an autocompensating two-wire PlugPlay approach together with the phase coding technique relying on the Mach-Zehnder interferometer.

However, the paper fails to indicate the limitations of applying QKD. Current limits of quantum key distribution fall only a few hundred kilometres behind in distance of transmission, higher costs for specialized gear, and a key generation rate that diminishes with distance between sender and recipient. However, research further extends the distance over which quantum key distribution can be achieved, and QKD is likely to become a highly attractive option in future years for some of the niche applications that require stringent compliance with security requirements.

2.8 Single sign On

Utilizing GHZ state entanglement, a research documented is referred in source (Ren, Wang, & Dai, 2015) introduces a quantum-resistant Single Sign-On (SSO) based technique. This specific protocol incorporates three distinct channels: first one a quantum based channel for secure key distribution, second one a unjammable public based channel for dissemination of classical information, and third one a jammable public based channel for procession of realresults.

The security capability of this approach relies on quantum processes, leveraging the inability of eavesdroppers to replicate statistical based correlations among & as between C, SSOS, and C accordingly. Moreover, SSOS, TTP is incapable of acquiring the session keys of K C,SSOS and K C,AS. Consequently, the method proposed during this study offers enhanced safety. However, security for authentication with the help of session key K C,SSOS or K C,AS is contingent over the effectiveness of traditional cryptography.

An integral aspect of IAM design is Single Sign-On (SSO), a mechanism preventing users from repetitive sign-ins. Addressing the challenges posed by ongoing leakage and quantum era threats in password-based SSO methods, source (Jiang, Wang, Zhang, & Chen, 2022) introduces a password-based threshold Single Sign-On (SSO) for authentication technique. The concept of "perpetual leakage" arises when a threat agent gains access to crucial password database, enabling future unauthorized logins. The proposed solution employs a dynamic and resilient password-based threshold authentication (PTA) system, regularly updating the master-

secret to thwart perpetual leakage. Consequently, even if an attacker breaches the password database, authentication is restricted to users who had credentials compromised before the latest master-secret update. While not achieving perfect security in the quantum era, this approach contributes valuable ideas to guide future research, acknowledging that making standard SSO authentication quantum-safe remains a challenge for the future.

3 Research Methodology

3.1 Research model

Attempts were made to build an Apache hosted web server with the functionality of TLS 1.3, X.509 certificates and TLS hybrid key exchange method. OpenSSL 1.1.1l fork from the Open Quantum Safe project had been used for this purpose as it is an excellent open-source initiative for prototyping NIST's candidate post-quantum algorithms. The features of this prototype include the use of TLS version 1.3, a hybrid signature scheme for CA and server certificates, and a hybrid key-exchange method during the TLS handshake. The chosen hybrid algorithms, NIST's P-521 elliptic curve combined with Falcon 1024 and Firesaber, exemplify Level 5 cryptographic security. The hybrid signature and key-exchange both offer Level 5 cryptographic security and use hybrid algorithms that are Round 3 finalists in NIST's post-quantum encryption standardization process. The claim behind hybrid algorithms is that they secure encrypted traffic against cryptanalysis by current age classical computers as well as tomorrow's quantum computers. The GNOME web browser (Epiphany) is a good candidate for being used as web client since we are not able to use traditional browsers like Chromium. Epiphany is useful as it supports OpenSSL as its TLS stack. This selection was populated in Post quantum cryptography research by the historical use of this browser by (Schwabe, Stebila, & Wiggers, 2021) in demonstrating their version of OpenSSL using the NTRU quantum-safe algorithm.

3.2 Liboqs and OQS-OpenSSL 1.1.1

In liboqs, three main APIs are provided for key encapsulation mechanisms (KEM):

OQS_KEM_keypair: Generates a public-private key pair for key encapsulation.
OQS_KEM_encaps: Takes a public key and generates a shared secret for the other party.
OQS_KEM_decaps: Uses the public key from the other party and the private key to generate a shared secret.

The limitation that is imposed in the instantiation of hybrid methods in OQS-OpenSSL 1.1.1 is on simultaneously combining a maximum of two algorithms where each such pair assigned a "group" identifier. As a result, negotiations take the collective consideration of the combinations and do not consider the individual combinations. In this hybrid scheme, the values of the hybrid system are obtained by setting together the elliptic curve and postquantum algorithms values that are present in ClientHello and ServerHello messages in the keyshare. And finally, the shared secret is computed by concatenation of individual share secrets' values into the ECDH shared secret's role on the TLS 1.3 key schedule. It is important to say that

OpenSSL-based implementation in its part libcrypto does not imply any generic Key Exchange Mechanism (KEM) either a key exchange API. Hence, adaptation of the existing OQS-OpenSSL implementation mostly consists of modifications within OpenSSL's ssl directory and involves calls into OpenSSL's libcrypto for ECDH algorithms, and into the liboqs library from the Open Quantum Safe project for post-quantum Key Encapsulation Mechanisms (KEMs).

3.3 Justification and relevance

The research methodology for Quantum-safe IAM infrastructure is based on the evaluation of post-quantum cryptographic algorithms, ciphers, digital signatures with the help of the learnings of the previously referred published research papers. The implementation is done with the help of Post-quantum cryptography algorithms in the form of a liboqs library as it was identified to be one of the easily available and approved technology for the same.

The data collection process is achieved by capturing the server-client interaction using Wireshark. Wireshark is a widely adopted network packet analyzer. Wireshark facilitates the in-depth analysis of packet exchanges during the TLS handshake, providing us insight into variables like TLS version, cipher suite and supported groups.

For evaluation purposes, we can measure the key exchange efficiency, packet loss, public key size, latency and overall system performance during the secure communication process. The setup involves configuring the server and client environments with specific versions of TLS and cryptographic libraries.

4 Design Specifications:

Inherent in this design is the incorporation of post-quantum cryptographic algorithms, such as CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, and SPHINCS+, within the TLS protocol. The system architecture is designed to be customizable which allows integration of new key exchange and signature algorithms without many modifications to the existing protocol structure. This involves the addition of curves and algorithm types in the Supported Group and Signature Algorithms extensions within the Client Hello/Server Hello exchanges. Collaboration with liboqs in wolfSSL turns out to be a key component of the design, ensuring the efficient incorporation of these algorithms into the IAM infrastructure. The resulting interaction diagram visually depicts the flow of communication during the TLS handshake, highlighting the role of post-quantum cryptographic algorithms in securing the exchange between server and client.

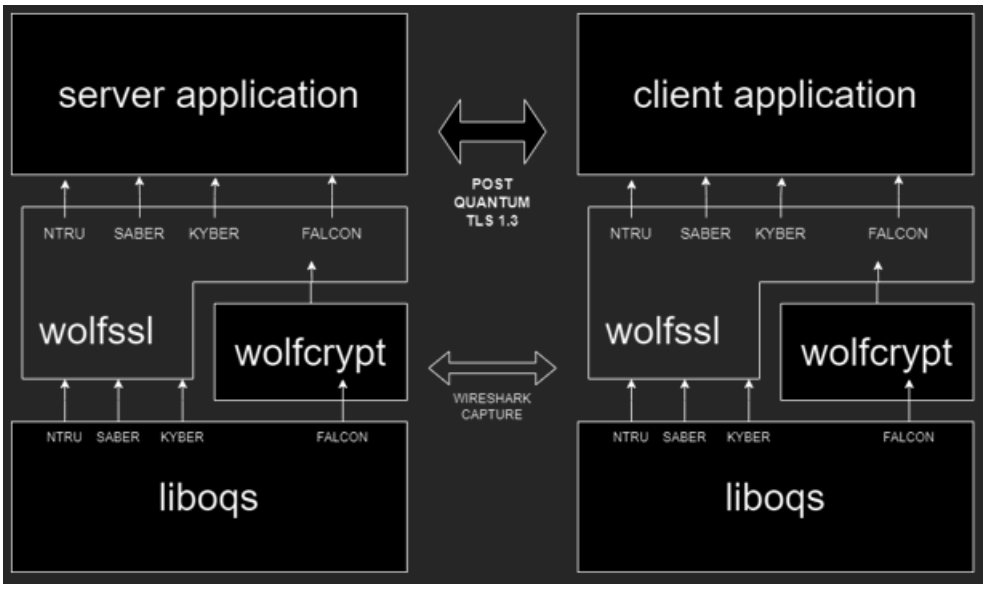

Figure 1: Server Client communication

The web server is built upon the OpenSSL 1.1.1l fork from the Open Quantum Safe project, ensuring compatibility with post-quantum cryptographic algorithms. It uses two of today's strongest data-encryption cipher-suites:
TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256.

5 Implementation

5.1 Trying Post-Quantum Cryptography with TLS (Part 1: Key Exchange)

In the competition for the standardization of post-quantum cryptography by the U.S. National Institute of Standards and Technology (NIST) in Round 3 of 2021, CRYSTALS-KYBER was chosen for key encapsulation, and CRYSTALS-Dilithium, FALCON, SPHINCS+ were selected for digital signatures. Standardization work is underway based on these algorithms. On the other hand, the open-source project Open Quantum Safe (OQS) provides these algorithms as the library "liboqs."

While the standardization of these algorithms within the TLS protocol is still in the draft stage, in essence, these algorithms can be handled by adding new key exchange and signature algorithms to the protocol structure without significant changes. In other words, it is possible to support them by adding curves and algorithm types in the Supported Group and Signature Algorithms extensions during the TLS handshake's Client Hello/Server. Here, we explore key exchange, particularly post-quantum cryptography key exchange, using these libraries. It's worth noting that the liboqs library provides standalone QS algorithm implementations and hybrid algorithms with ECC.

DISCLAIMER: At this stage, it's not guaranteed that these post-quantum cryptography algorithms have sufficient robustness under a wide range of conditions. The project

recommends using hybrid encryption, combining them with traditional elliptic curve cryptography.

When applied to the TLS 1.3 handshake, the flow is similar to (EC)DH key exchange, as illustrated in the diagram below. The public keys generated by OQS_KEM_keypair and OQS_KEM_encaps are stored in the Key Share extension of the Client Hello and Server Hello messages. The resulting shared secret becomes the pre-master secret.

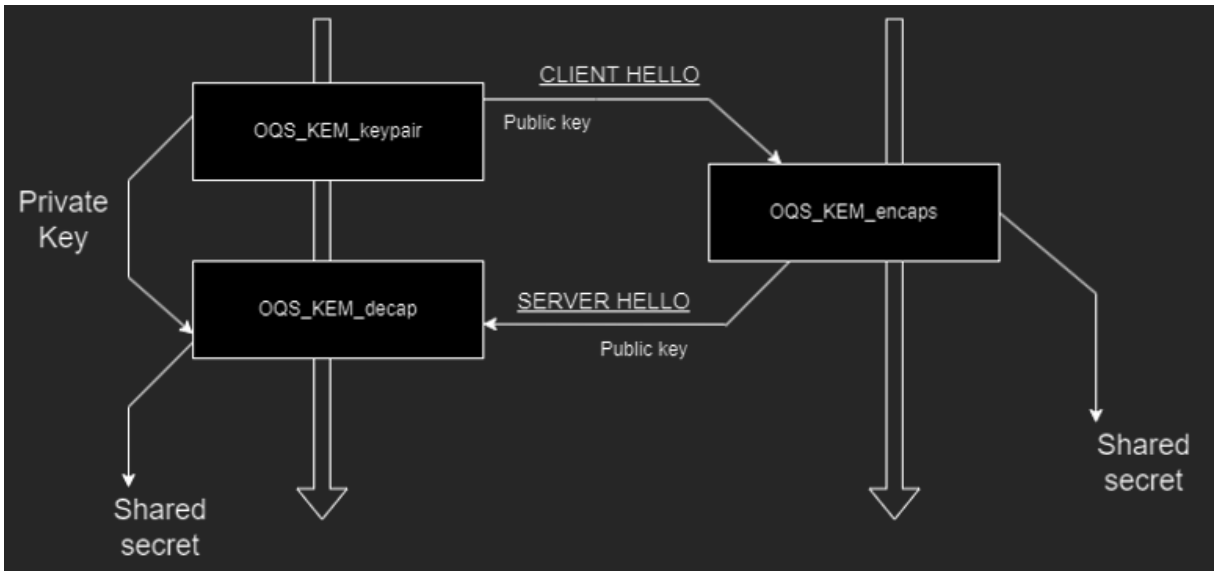

Figure 2: KEM key exchange in TLS 1.3

While this example demonstrates the use of only OQS_KEM, in reality, hybrid algorithms with ECC (ECDH) are also implemented. In the case of hybrids, the ECDH process is performed concurrently, and both keys are combined and stored in the Key Share extension of the Client Hello and Server Hello.

Here is a summary of the KEM algorithms supported by liboqs:

Table 1: Liqoqs supported KEM algorithms specs

Algorithm	Public key size	Private key size
Kyber512	800	1632
Kyber768	800	1632
Kyber1024	1184	2400
Kyber512-90s	1184	2400
Kyber768-90s	1568	3168
Kyber1024-90s	1568	3168

We run a simple benchmark program for each algorithm, including KEM: Kyber, and signatures: Dilithium, Falcon, SPHINCS. The benchmark program repeats these algorithms for approximately one second, displaying the average time taken in milliseconds and operations per second.

```
KYBER512    128  key gen     96600 ops took 1.001 sec, avg 0.010 ms, 96518.538 ops/sec
...
KYBER1024   256    decap     45400 ops took 1.001 sec, avg 0.022 ms, 45333.043 ops/sec
...
DILITHIUM     5     sign      5900 ops took 1.003 sec, avg 0.170 ms, 5881.262 ops/sec
DILITHIUM     5   verify     11800 ops took 1.002 sec, avg 0.085 ms, 11773.521 ops/sec
...
FALCON     5     sign      1700 ops took 1.008 sec, avg 0.593 ms, 1686.290 ops/sec
FALCON     5   verify      8800 ops took 1.007 sec, avg 0.114 ms, 8741.720 ops/sec
SPHINCS-FAST     5     sign       100 ops took 10.592 sec, avg 105.920 ms, 9.441 ops/sec
SPHINCS-FAST     5   verify       200 ops took 1.207 sec, avg 6.034 ms, 165.723 ops/sec 2
```

Figure 3: Benchmark program results

After necessary configurations and changes referred to in the configuration manual, TLS communication between a sample server and client can be set up. Open two windows on your local PC, one for the server and the other for the client and launch the sample server and client as follows. Also, ensure to start Wireshark. We'll specify ECC-P521 and Kyber Level 5 as the hybrid key exchange algorithm.

The server and client will perform TLS connections and one round-trip message communication. Each window will display TLS 1.3 connection information and application messages as shown below:

```
root@ubuntu2:~/oqs/liboqs# cd build
root@ubuntu2:~/oqs/liboqs/build# cd wolfssl
root@ubuntu2:~/oqs/liboqs/build/wolfssl# ./examples/server/server -v 4 --pqc P521_KYBER_LEVEL5
Using Post-Quantum KEM: P521_KYBER_LEVEL5
SSL version is TLSv1.3
SSL cipher suite is TLS_AES_128_GCM_SHA256
SSL curve name is P521_KYBER_LEVEL5
Client message: hello wolfssl!
root@ubuntu2:~/oqs/liboqs/build/wolfssl#
```

Figure 4: Server TLSv1.3 handshake

```
root@ubuntu2:~/oqs/liboqs/build/wolfssl# ./examples/client/client -v 4 --pqc P521_KYBER_LEVEL5
Using Post-Quantum KEM: P521_KYBER_LEVEL5
SSL version is TLSv1.3
SSL cipher suite is TLS_AES_128_GCM_SHA256
SSL curve name is P521_KYBER_LEVEL5
I hear you fa shizzle!
root@ubuntu2:~/oqs/liboqs/build/wolfssl#
```

Figure 5: Client TLSv1.3 handshake

5.2 Wireshark capture:

Inspecting the Server Hello, you can see "Cipher Suite: TLS_AES_128_GCM_SHA256," indicating agreement on one of the standard TLS 1.3 cipher suites. The key exchange algorithm is marked as "Group: Unknown (12093)," indicating that Wireshark does not yet support the ID for post-quantum algorithms, hence displaying the raw ID value.

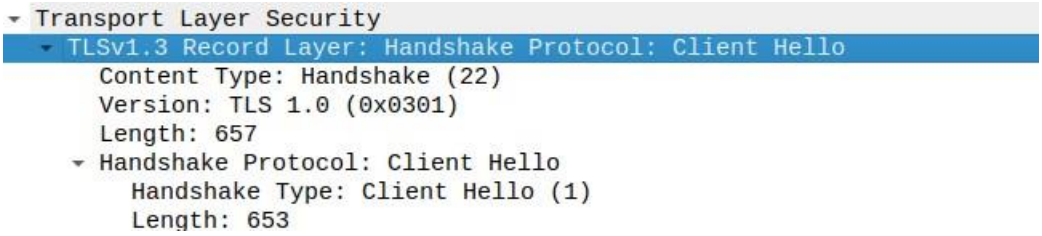

Figure 6: Wireshark packet capture

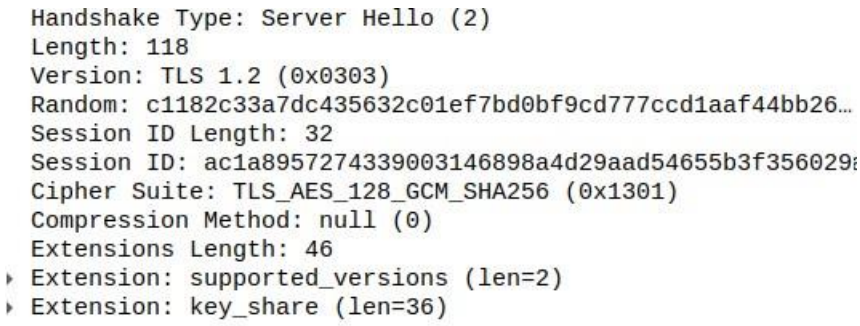

Figure 7: Algorithm group details

5.3 Quantum-Safe TLS 1.3 Web Server-Client Architecture with NIST Level 5 Security:

We further build a complete web client-server build, which helps in securing communications against both today's classical and tomorrow's quantum threats.

It offers the following features:

a) TLS Version 1.3
b) Server and CA certificates are signed via a hybrid signature scheme which makes use of NIST's P-521 elliptic curve with Falcon 1024.
c) TLS handshake with hybrid key-exchange method
d) Quantum-safe X.509 certificate

Since the Chromium browser and its derivatives use BoringSSL as their TLS back-end, and the Open Quantum Safe fork of BoringSSL does not currently support hybrid signature algorithms .We require a browser that uses OpenSSL for TLS, since only the Open Quantum Safe OpenSSL fork supports both hybrid key exchanges and hybrid signatures. Surprisingly, almost no browsers use OpenSSL, which is primarily a server-side TLS package. Instead, modern

browsers use proprietary TLS libraries (NSS for Mozilla and derivatives, the abovementioned BoringSSL for Chromium and its offspring). The only one suitable for our use case was GNOME web browser (a.k.a. Epiphany) as it has an obscure option to use OpenSSL as its TLS stack instead of the default GNU TLS. It further allows configurations and modifications suitable for our case.

Bash file is created to configure and install all dependencies required, tested on an Ubuntu 20.04.3 LTS virtual machine, to install and configure the Epiphany browser to allow it to conduct a hybrid handshake with the server and read its hybrid-signed certificate. File is referred to in manual.

```
#Step 7: Build Certificate Authority (CA) key and certificate using p521_falcon1024 (NIST Round 3 Level 5 security hybrid
signature Scheme)

/usr/local/bin/openssl req -x509 -new -newkey p521_falcon1024 -keyout p521_falcon1024_CA.key -out p521_falcon1024_CA.crt -nodes
-subj "/CN=oqstest CA" -days 365 -config /usr/local/ssl/openssl.cnf

#Step 8: Copy CA certificate to system trust store and add it as a trust anchor for the web browser (these 2 commmands may be
redundant)

sudo cp p521_falcon1024_CA.crt /etc/ssl/certs
sudo trust anchor /etc/ssl/certs/p521_falcon1024_CA.crt

#Step 9: Generate server's hybrid private key and Certificate Signing Request (CSR)

/usr/local/bin/openssl req -new -newkey p521_falcon1024 -keyout p521_falcon1024_srv.key -out p521_falcon1024_srv.csr -nodes -
subj "/CN=localhost" -config /usr/local/ssl/openssl.cnf

#Step 10: Generate server's hybrid certificate and sign with CA hybrid key

/usr/local/bin/openssl x509 -req -in p521_falcon1024_srv.csr -out p521_falcon1024_srv.crt -CA p521_falcon1024_CA.crt -CAkey
p521_falcon1024_CA.key -CAcreateserial -days 365
```

Figure 8: X.509 certificate configuration process

We create a X.509 self signed certificate using open SSL and specify the use p521_falcon1024 algorithm.

```
root@ubuntu2:~# cd ..
root@ubuntu2:/# /usr/local/bin/openssl req -x509 -new -newkey p521_falcon1024 -keyout p521_falcon1024_CA.key -out p521_falcon1024_CA
.crt -nodes -subj "/CN=oqstest CA" -days 365 -config /usr/local/ssl/openssl.cnf
Generating a p521_falcon1024 private key
writing new private key to 'p521_falcon1024_CA.key'
```

Figure 9: p521_falcon1024 Private key generation

After which, we make it a trusted anchor.

```
root@ubuntu2:/# sudo trust anchor /etc/ssl/certs/p521_falcon1024_CA.crt
```

Figure 10: Browser Certificate trust configuration

We use the CA certificates key to sign the server's CSR. Then we produce a hybrid certificate for the server. After testing and initial attemps, these certificates turned out to be mandatory for establishing secure communication using the specified hybrid security algorithms. We create a certificate authority along with server certificates for use in our application.

```
root@ubuntu2:/# /usr/local/bin/openssl x509 -req -in p521_falcon1024_srv.csr -out p521_falcon1024_srv.crt -CA p521_falcon1024_CA.crt
 -CAkey p521_falcon1024_CA.key -CAcreateserial -days 365
Signature ok
subject=CN = localhost
Getting CA Private Key
root@ubuntu2:/#
```

Figure 11: Signing server's CSR request

The Apache configuration files are modified to support the p521_kyber1024 cipher. Despite creating a Flask application with files app.py and index.html designed to run locally with the specified architecture, we encountered difficulties displaying it on the Epiphany browser. All executed commands indicated successful integration and configuration. However, we encountered the following error:

Figure 12: Epiphany browser results

Despite executing all commands without indications of integration or configuration issues, the application failed to display successfully on the Epiphany browser. The error points towards an inability of the browser to recognize the cipher suite and algorithms for communic ation. Unfortunately, debugging for this is still ongoing to identify and address the underlying issue, ensuring a seamless execution of the Quantum-Safe TLS 1.3 Web Server-Client Architecture with the desired level of security. However, a server client prototype was able to be successfully implemented which gave us enough data to evaluate the implementation for our IAM system.

6 Evaluation

6.1 Security Posture Improvement

The evaluation of the post-quantum cryptography for IAM is done based on the security it would provide to the framework. After implementation, we check the improvement in security posture for the different components of IAM. We do a risk assessment against quantum computer attacks to further evaluate the results.

Risk ID	Risk scenario	Probability without control	Impact (without Control)	Risk level	Probability(For our setup)	Probability(Traditional setup)	Controls
CS001	Public key infrastructure	Frequent	High	8	Medium	High	Hybrid key exchange or Quantum key distribution
CS002	Secure Web browsing	Frequent	Very High	9	Very low	Very high	TLS v1.3
CS003	X.509 certificates	Frequent	Very High	9	Very low	Very high	Using X.509 certs via Post quantum cryptography
CS004	Multi factor authentication	Possible	High	8	High	High	Using Quantum2FA or FIDO2 with PQC (Future work)
CS005	Authentication	Frequent	Very High	9	Low	High	Using Post quantum cryptography
CS006	Federated authorization	Possible	High	8	High	High	Using SSO protocols with GHZ states
CS007	Key Exchange over a public channel	Frequent	HIgh	9	Very low	High	c)TLS handshake with hybrid key-exchange method

Figure 13: Risk matrix

Using the Hybrid key exchange mechanism prevents threat actors from breaking the security features of PKI's. These mechanisms allow secure exchange of cryptographic keys between parties in a way that remains secure even in the presence of quantum adversaries. X.509 protects against phishing , certificate revocation and maintain confidentiality. They even help in compliance and maintaining standards by adhering to a common framework for secure communication. Authentication is secured via post quantum cryptography by eliminating the quantum threat. It also helps in upholding long term security and standardization efforts.

Multifactor authentication via FIDO2 or quantum2FA is highly useful as it has different features like passwordless, enhanced security layers and phishing resistance. Web browsing is secured via TLS v1.3 as it comes with improved handshake protocol.

6.2 Performance Metrics

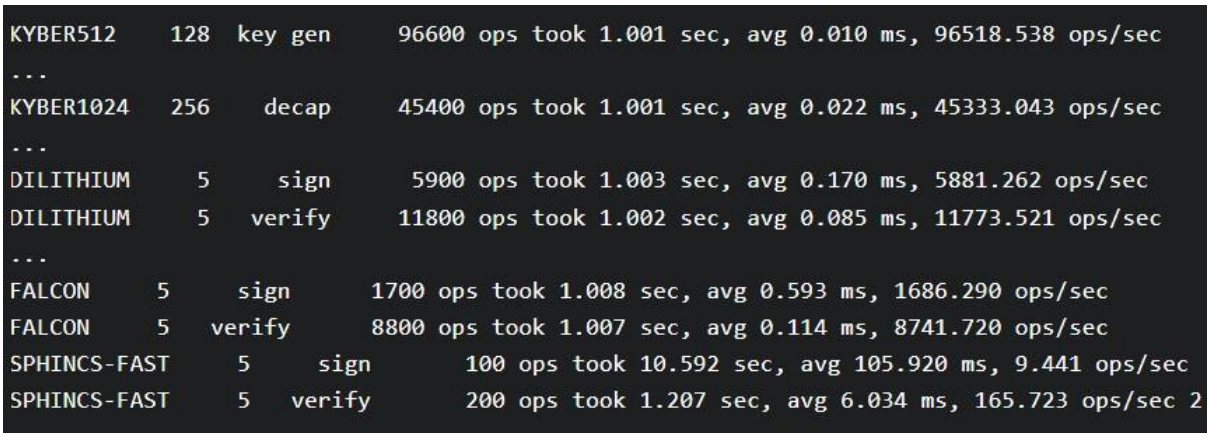

Figure 14: Benchmark tests results

While evaluating the NIST approved algorithms and cipher suites, we run benchmark tests for the same and get the performance metrics for the given algorithms. While comparing the values with traditional algorithm values attained from the internet. It can be evaluated that even though the given algorithms are more efficient and secure. They turn out to be more time consuming and come with greater key sizes and string values. This goes onto say that more research is required to optimize the given algorithms.

6.3 Research Discussion

The Quantum-Safe IAM Research Project ensured the application of approved cipher suites as well as hardened TLS 1.3 with the aid of post-quantum cryptographic algorithms. The schemes are SPHINCS+, CRYSTALS-KYBER, FALCON, together with CRYSTALS-
Dilithium in a prototype. The project found out that lattice-based techniques and algorithms form the most secure way of building quantum-resistant IAM services and this was used by the project. It was noticed however that these techniques come at a compromise in speed and efficiency. The project also produced a detailed analysis of TLS security tailored towards quantum-safe IAM, further demonstrating excellent understanding across multiple cryptographic algorithms and appropriateness in such contexts. It also paved the way for further

research into other IAM quantum resistant services like post-quantum Multi factor authentication. Along with post quantum cryptography into certificates used for SSH and FIDO2 protocols. The research allows other researchers to have a foundation for their research into securing IAM frameworks in the quantum era. It does so by suggesting the most efficient algorithms and configurations required for integrating the same. It underlies the possible compatibility issues and configuration requirements for the same. Evaluation is done on the basis of security posture improvement and measuring performance metrics. postquantum cryptography and IAM are likely to offer endless research options as well as the potential for commercialization by further work.

7 Conclusion

The research question for the project was analyzing and deploying post-quantum cryptographic algorithms to build quantum-resistant IAM services. The objectives were implementing cipher suites which are approved, improving the TLS 1.3, and applying postquantum cryptographic algorithms like the SPHINCS+, CRYSTALS-KYBER, FALCON, and CRYSTALS-Dilithium for digital signatures based on NIST-approved algorithms.

We have successfully been able to meet our objectives and answer the formulated research question through the execution of experiment and case studies. The key findings which can be defined in the report are the implementation part of Quantum-Safe TLS 1.3 Web ServerClient Architecture and the most secure way found in PQC is lattice-based techniques.

The implications of this research have significant importance as within this research, it was focused that these post-quantum cryptographic algorithms should be incorporated within the IAM systems so that a defence from the potential quantum computer attacks can be build up. The successful launching of quantum resistant IAM services has established a most effective how-what of our research. Yet the boundary for conducting this research was under investigation - in order to identify and come across the underlying issues related to the displayed application on Epiphany Browser.

In conclusion, this project has added value to the field of post-quantum cryptography and lays a foundation for advanced research in building quantum resistant IAM services.

7.1 Future work

Future work in post-quantum cryptography and IAM presents numerous avenues for research and potential commercialization. Quantum-resistant services would need to be integrated in different avenues of IAM. Practical implementation and real-world deployment of these enhancements, along with extensive testing and refinement, are crucial for bridging theoretical advancements with practical applicability.

7.1.1 Web application with integrated quantum-resistant services

Web servers are the common applications used by users to access resources and data. They are used to authenticate and authorize identities as well. With the same ideology, this report attempted to implement the same but failed with errors encountered in configuring different packages to allow Post quantum cryptography. More work needs to be done on learning the workings of these packages to allow the same.

7.1.2 post-quantum Multi-Factor Authentication (MFA)

It is one of the key areas of IAM and allows users to authenticate via a secondary method. With the use of quantum computers, current MFA processes even commercial ones are vulnerable and require development in the same domain.

7.1.3 post-quantum cryptography into SSH certificates

Additionally, integrating post-quantum cryptography into SSH certificates and FIDO2 protocols offers opportunities for bolstering the resilience of secure shell protocols and developing quantum-resistant authentication mechanisms.

7.1.4 Directory services

Directory services are used by IAM systems for storing, managing and maintaining identities, a complete IAM system would require securing the same against quantum attacks.

8 References

Bushuev, E. Y. (2023, June 28). Comparative Analysis of Quantum Key Distribution Schemes in Quantum Communication Channel and Quantum Key Distribution Process Simulation. *2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO* (pp. 1–5). Pskov: IEEE. doi:10.1109/SYNCHROINFO57872.2023.10178490

Gidney, C., & Ekerå, M. (2021, April 15). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 5*, 433. doi:10.22331/q-2021-04-15-433

Jiang, J., Wang, D., Zhang, G., & Chen, Z. (2022). Quantum-Resistant Password-Based Threshold Single-Sign-On Authentication with Updatable Server Private Key. In V. Atluri, R. Di Pietro, C. D. Jensen, & W. Meng (Eds.), *Computer Security – ESORICS 2022* (Vol. 13555, pp. 295–316). Cham: Springer Nature Switzerland. doi:10.1007/978-3-031-171468_15

Kinkelin, H., Von Seck, R., Rudolf, C., & Carle, G. (2020, April). Hardening X.509 Certificate Issuance using Distributed Ledger Technology. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium* (pp. 1–6). Budapest: IEEE. doi:10.1109/NOMS47738.2020.9110311

Lokesh B, S., & Kaulgud, N. (2023, February 10). A review on analysis of transport layer security in open quantum safe cryptographic algorithm. *2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC)* (pp. 1–5). Mysore: IEEE. doi:10.1109/ICRTEC56977.2023.10111928

Murray, H., & Malone, D. (2021). Quantum multi-factor authentication. doi:10.1007/978-3030-93747-8_4

NIST. (2023, August 24). *Post-Quantum Cryptography*. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

NIST. (2022, july 5). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. Retrieved from https://www.nist.gov/news-events/news/2022/07/nist-announcesfirst-four-quantum-resistant-cryptographic-algorithms

Policarpo, R. C., Nery, A. S., & Albuquerque, R. D. (2022, November 17). Quantum-resistant Cryptography in FPGA. *2022 Workshop on Communication Networks and Power Systems (WCNPS)* (pp. 1–5). Fortaleza: IEEE. doi:10.1109/WCNPS56355.2022.9969738

Ren, X., Wang, Y., & Dai, G. (2015). A Quantum Single Sign-On Protocol Based on GHZ States. *Int J Theor Phys 54*.

Schwabe, P., Stebila, D., & Wiggers, T. (2021). More Efficient Post-quantum KEMTLS with Pre-distributed Public Keys. In E. Bertino, H. Shulman, & M. Waidner (Eds.), *Computer Security – ESORICS 2021* (Vol. 12972, pp. 3–22). Cham: Springer International Publishing. doi:10.1007/978-3-030-88418-5_1

Shor, P. W. (1997, October). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing, 26*, 1484–1509. doi:10.1137/S0097539795293172

Sikeridis, D., Ott, D., Huntley, S., Sharma, S., Dhanasekar, V. K., Bansal, M., & Kumar, A. (n.d.). ELCA: Introducing Enterprise-level Cryptographic Agility for a Post-Quantum Era.

Wang, Q., Wang, D., Cheng, C., & He, D. (2023, January 1). Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices. *IEEE Transactions on Dependable and Secure Computing, 20*, 193–208. doi:10.1109/TDSC.2021.3129512

Xu, G., Mao, J., Sakk, E., & Wang, S. P. (2023, March 22). An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography. *2023 57th Annual Conference on Information Sciences and Systems (CISS)* (pp. 1–6). Baltimore: IEEE. doi:10.1109/CISS56502.2023.10089619

The Open Quantum Safe Project. (2023). *The Open Quantum Safe Project*. Retrieved from https://openquantumsafe.org/