IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

POST-QUANTUM ENCRYPTED COMMUNICATION IN AIR-GAPPED SYSTEMS

[1]Suyash Bhosale, [1]Dhritee Dwivedi, [1]Sahal Manasia, [1]Riya Singh, [2]Rajesh Gaikwad

[1]Computer Engineering Department, Student, Shree L.R Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India 401107

[2]Computer Engineering Department, Assistant Professor, Shree L.R Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India 401107

Abstract: The purpose of this study is to look into the factors that the goal of "Post-Quantum Encrypted Communication in Air-Gapped Systems" is to increase the security of isolated computer environments. This effort aims to develop and apply quantum-resistant encryption algorithms that can withstand attacks while preserving backwards compatibility and customization for specific use cases. Among the primary objectives are boosting security, ensuring long-term resilience, and offering tailored, user-friendly encryption solutions for a variety of air-gapped applications. The primary goal of the project is to fortify sensitive data and operations inside air-gapped systems to offer a robust defense against the dynamic quantum threats of the digital age.

Index Terms - Post-Quantum Cryptography, Air-Gapped Systems, Quantum-Safe Encryption, Quantum Computing, Encrypted Communication, Key Exchange Protocols, Quantum Key Distribution (QKD), Secure Communication Protocols, Quantum Vulnerabilities.

I. INTRODUCTION

Throughout the wired and wireless realms of current digital communication infrastructures, public key cryptography is a fundamental security mechanism. Key exchange, digital signatures, and public key encryption are the three main cryptographic processes that it may help with, and these are where its importance resides. [1] Conventional public key cryptography implementations rely on robust algorithms like Elliptic Curve cryptography and RSA, which are derived from discrete logarithms and integer factorization, which are known for their computational cost.

Sensitive data protection in isolated situations becomes even more crucial in today's dynamic technological ecosystem of always changing threats. Fortified communication lines that can withstand potential breaches and attacks must be developed as a result. This requirement is the focus of our study effort.

Our project focuses on important domains such as Defense, Military, and SCADA (Supervisory Control and Data Acquisition) systems in Industrial Control Systems (ICS). These industries work in closed-off, isolated locations and handle extremely sensitive data in order to reduce the possibility of outside intrusion. However, the security guarantees offered by conventional cryptographic methods are seriously threatened by the advent of quantum computing.

Important sectors including the military, defense, and SCADA (Supervisory Control and Data Acquisition) systems in Industrial Control Systems (ICS) are the focus of our research. To lessen the chance of outside interference, these industries handle incredibly sensitive data while operating in remote, restricted areas. However, the introduction of quantum computing poses a major challenge to the security guarantees provided by traditional cryptography techniques.

Our methodology entails a comprehensive analysis of existing post-quantum cryptographic algorithms, evaluating their suitability for deployment within air-gapped systems. We also consider the practical constraints and operational requirements specific to the target sectors, ensuring the feasibility and efficacy of the proposed solution. Through rigorous experimentation and validation, we endeavor to demonstrate the effectiveness of our approach in enhancing the security posture of isolated communication networks.

II. POST-QUANTUM CRYPTOGRAPHY

Lattice-based Cryptography: Lattice-based cryptography is one of the most promising candidates for post-quantum cryptography. It relies on the hardness of lattice problems, such as the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem. Examples of lattice-based schemes include NTRU Encrypt, NTRU Sign, and Kyber. [2]

Code-based Cryptography: Code-based cryptography is based on the difficulty of decoding linear error-correcting codes. The McElwee cryptosystem is the most well-known example of a code-based cryptosystem, known for its resistance to quantum attacks.

Hash-based Cryptography: Hash-based cryptography is based on cryptographic hash functions and the Merkle tree structure. The most notable example is the Lam port signature scheme, which is secure against quantum attacks but has limitations in terms of key size and signature length.

Quantum Key Distribution (QKD): While not strictly a post-quantum cryptographic algorithm, QKD enables secure key exchange based on the principles of quantum mechanics, offering provably secure communication channels.

Air Gapped Computers: An air gap is a security measure that involves isolating a computer or network and preventing it from establishing an external connection. An air-gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices.

III. BACKGROUND

One important endeavour aimed at strengthening the security framework of isolated computing environments is "The Post-Quantum Encrypted Communication in Air-Gapped Systems" project. These air-gapped systems are vulnerable to changing threats, especially from the world of quantum computing. They are frequently used in industries handling extremely sensitive data, such as defence, finance, and critical infrastructure. Given the potential for quantum computing to undermine established cryptography systems, the initiative acknowledges the pressing need to create encryption strategies resistant to quantum attacks. The investigation and application of post-quantum cryptography algorithms that provide strong security assurances while preserving compatibility with current legacy systems are essential to its goal.

Moreover, the project strongly emphasizes customizing encryption methods to satisfy the various requirements and limitations of environments that are air-gapped. This means considering practical factors like performance overhead, resource limitations, and simplicity of integration in addition to guaranteeing the effectiveness and robustness of the encryption techniques. The project's goal is to provide encryption solutions that are simple to use, intuitive, and easily integrated into current workflows within air-gapped systems by adopting a user-centric approach. In order to ensure that security measures do not hamper operational efficiency, it is imperative that usability be prioritized in order to stimulate wider adoption.
By safeguarding sensitive data and operations against emerging quantum risks, the project not only mitigates potential vulnerabilities but also contributes to the overall resilience and integrity of the infrastructure underpinning essential societal functions.

IV. POST-QUANTUM CRYPTO VPN SOFTWARE

This project combines post-quantum cryptography with an OpenVPN software derivative. We may assess the functioning and performance of the quantum resistant cryptography by testing these algorithms using VPNs. Sensitive information or communications should not be protected using this project at this time because it is experimental. [3] The next several years will need to be spent on cryptanalysis and research to ascertain whether algorithms are indeed post-quantum safe.

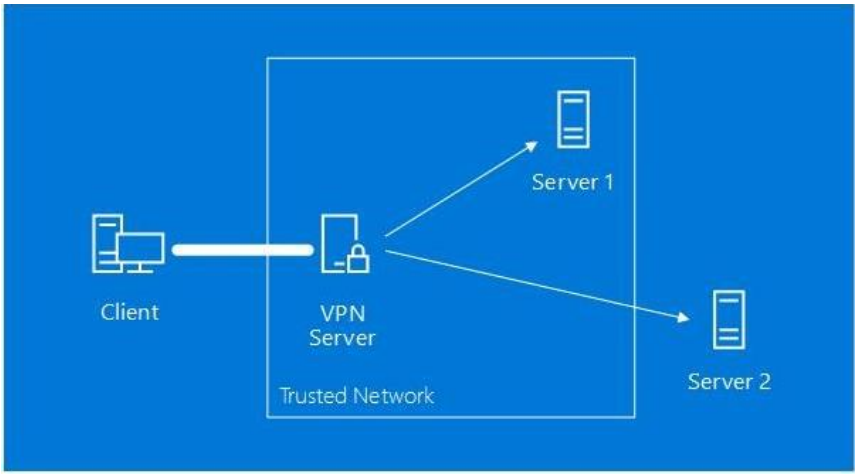

Figure 1: Server 1 is connected to the same secure network as the VPN Server, communication between the Client and Server 1 is protected by post-quantum technology. There is no post-quantum crypto security for communication between the Client and Server.

Communication that remains on an organization's internal network or with a reliable cloud provider is secure once traffic leaves the VPN server. Build your test application architecture with this software in mind to make sure that this is the case. If data leaves Server 2 and enters the public internet, as shown in the picture above, it will only be secured by conventional cryptography, making it susceptible to attack by a quantum computer.

V. OBJECTIVES

- Select Suitable Post-Quantum Encryption Schemes: Evaluate and choose the most appropriate post-quantum encryption schemes based on performance, security, and compatibility with the air-gapped systems' hardware and software limitations.
- Create Secure Communication Protocol: Design a communication protocol tailored to the unique characteristics of air-gapped systems, incorporating the selected post- quantum encryption methods while ensuring efficient and reliable data transfer.
- Implement Secure Hardware and Software Components: Develop and deploy robust embedded systems and software components that facilitate encrypted communication within the air-gapped environment, ensuring data protection even in the absence of internet connectivity.
- Perform Rigorous Testing and Evaluation: Conduct thorough testing, simulations, and security assessments to identify and rectify potential vulnerabilities, ensuring the reliability and effectiveness of the post-quantum encryption solution.
- Ensure User-Friendly Interaction: Design an intuitive and user-friendly interface that allows authorized personnel to securely initiate, monitor, and manage encrypted communication between the air-gapped systems.
- Address Compliance and Regulatory Requirements: Ensure that the project adheres to relevant data protection regulations and industry standards, especially when handling sensitive or regulated information.
- Provide End-to-End Security: Guarantee end-to-end security during data transmission and storage, from the source to the destination within the air-gapped systems.
- Mitigate Quantum-Based Threats: Minimize the risk of potential quantum-based attacks on the communication channels and cryptographic systems used in the project.

VI. LITERATURE REVIEW

[1]. Maran van Heesch, Niels van Adrichem, Thomas Attema, and Thijs Veugen (2019) "Towards Quantum-Safe VPNs and Internet" Cryptology ePrint Archive

Estimating that in 10 years' time quantum computers capable of breaking public-key cryptography currently considered safe could exist, this threat is already eminent for information that require secrecy for more than 10 years. Considering the time required to standardize, implement and update existing networks signifies the urgency of adopting quantum-safe cryptography.

In this work, we investigate the trade-off between network and CPU overhead and the security levels defined by NIST. To do so, we integrate adapted OpenSSL libraries into OpenVPN, and perform experiments on a large variety of quantum-safe algorithms for respectively TLS versions 1.2 and 1.3 using OpenVPN and HTTPS independently. We describe the difficulties we encounter with the integration and we report the experimental performance results, comparing setting up the quantum-safe connection with setting up the connection without additional post-quantum cryptography.

[2]. Aymen Ghilen, Mostafa Azizi, Ridha Bouallegue (2015) "Q-OpenVPN: A New Extension of OpenVPN Based on a Quantum Scheme for Authentication and Key Distribution" International Conference on Cryptology and Network Security

In this paper we have discovered that Virtual Private Network (VPN) tunnels are cryptographic solutions that enable sensitive information to be transmitted over an untrusted environment, and ensure the most imperative security services such as confidentiality, integrity, and authentication. OpenVPN is an open source implementation of VPN. In the present work, we propose the deployment of a quantum protocol for cryptographic key exchange and authentication within OpenVPN between both sides of the tunnel. Our approach is a prominent step towards unconditional security based on the laws of quantum physics. Despite the huge progress in the quantum research field, quantifying the confidence and secrecy of the proposed scheme still remains a hard task. In this context, we adopt a probabilistic approach based on the technique of Model Checking, using the PRISM tool. We basically focus on two pioneering security properties: the ability to detect an eavesdropper independently of its computational power and the minimization of the amount of information gained by the eavesdropper about the secret key.

[3] Karen Easterbrook, Kevin Kane, Brian LaMacchia, Dan Shumow, Greg Zaverucha, Christian Paquin, "Post-quantum Crypto and VPNs" https://www.microsoft.com/en-us/research/project

Every time you make a secure connection over the internet – to your bank, to Facebook, or nearly anywhere online – cryptography is what keeps that communication secure. Some of that cryptography is based upon mathematical problems known to be solvable by a quantum computer. As the scientists working on quantum computers continue to make progress, cryptographers are at work as well, developing new post-quantum cryptosystems based upon mathematical problems which we believe are resistant to quantum attacks.

When it comes time, migrating all network traffic, including communications from services and applications, to new post-quantum cryptography will be a time-consuming and lengthy process. Fortunately, we have some time. Even the most optimistic estimates are that it will be five or more years before a sufficiently powerful and stable quantum computer capable of breaking today's public-key cryptography is running.

As we and other research teams around the world work to develop new cryptosystems, we are testing how candidates work with real-world protocols and applications. One of the most important scenarios for post-quantum crypto is VPNs.

VPNs establish a secure link between two points on the internet and allow applications to run inside them as if they were on the same network. In the future, when post-quantum cryptosystems have been vetted by efforts like the NIST Post-Quantum Project, VPNs that are protected by post-quantum cryptography can be rapidly deployed to protect existing applications, until the applications themselves can be updated to use the new algorithms natively.

[4]. Dr. Lily Chen, Dr. Dustin Moody, Dr. Yi-Kai Liu, "Post-Quantum Cryptography" Information Technology Laboratory Computer Security Resource Centre

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

VII. APPLICATION

The application of the "Post-Quantum Encrypted Communication in Air-gapped Systems" project spans across various sectors where secure communication within isolated environments is paramount. Some of the key applications include: [4]

Defense and Military: In military operations, air-gapped systems are commonly used to protect sensitive information and communication networks from external threats. The project's encrypted communication solution ensures the confidentiality and integrity of classified data transmitted between military command centers, field operatives, and unmanned aerial vehicles (UAVs), safeguarding national security interests.

Critical Infrastructure: Industries such as energy, transportation, and utilities rely on air-gapped systems to manage and control critical infrastructure components. The project's encrypted communication solution helps secure communication between control centres, substations, and industrial control systems (ICS), preventing unauthorized access and potential disruptions to essential services.

Finance and Banking: Financial institutions handle vast amounts of sensitive data, including customer information, transactions, and trade secrets, which must be protected from cyber threats. The project's encrypted communication solution enables secure communication between banking servers, trading platforms, and ATM networks, ensuring the confidentiality and integrity of financial transactions and sensitive information.

Healthcare: Air-gapped systems are commonly used in healthcare environments to protect electronic health records (EHRs), patient data, and medical devices from cyber threats. The project's encrypted communication solution facilitates secure communication between hospitals, clinics, medical devices, and healthcare providers, safeguarding patient privacy and medical information.

Government and Intelligence Agencies: Government agencies and intelligence organizations rely on air-gapped systems to protect classified information and communication channels from adversaries. The project's encrypted communication solution enhances the security of communication between government agencies, intelligence analysts, and diplomatic missions, preserving national security interests and diplomatic relations.

Research and Development: Research institutions and laboratories involved in sensitive research projects require secure communication channels to protect intellectual property and research findings. The project's encrypted communication solution enables secure collaboration between researchers, laboratories, and academic institutions, safeguarding valuable research data and innovations.

VIII. ACTIVITY DIAGRAM

Initialize Communication: This is the first step in the process, where the system is initialized and prepared for communication.

Communication Established: The system checks to see if communication has been established with the other party. If so, the process moves on to step 3. If not, the process moves to the Handle Communication Error block.

Encrypt Data: If communication has been established, the data is encrypted using a cryptographic key. This helps to protect the data from being intercepted and read by unauthorized parties.

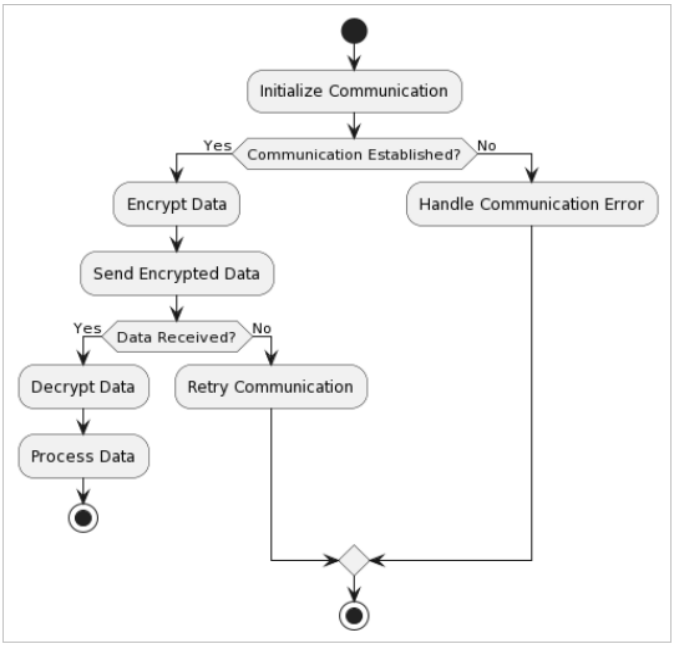

Figure 2: activity diagram

Send Encrypted Data: The encrypted data is then sent to the other party.

Data Received?: The system checks to see if the data has been received by the other party. If so, the process moves on to step 6. If not, the process moves to the Retry Communication block.

Decrypt Data: If the data has been received, it is decrypted using the same cryptographic key that was used to encrypt it.

Process Data: The decrypted data is then processed by the system.

Handle Communication Error: If there is an error during communication, the system will move to this block. The specific actions taken here will vary depending on the nature of the error.

Retry Communication: If there is an error during communication, the system may attempt to retry the communication.

IX. DATA FLOW DIAGRAM

The figure is made up of multiple important parts, each of which plays a distinct role in the overall data security procedure:

Air-gapped hard drives and other storage: Unauthorized users find it challenging to remotely access these since they are physically cut off from any networks.

An edge computer is a compact, high-performance computer that sits at the edge of a network, gathering and processing data before sending it to other systems.

Sentinel hardware key: Cryptographic keys are physically stored on this device and are necessary for both data encryption and decryption.

Before data is transferred to other computers or storage devices, it is encrypted on this encryption server.

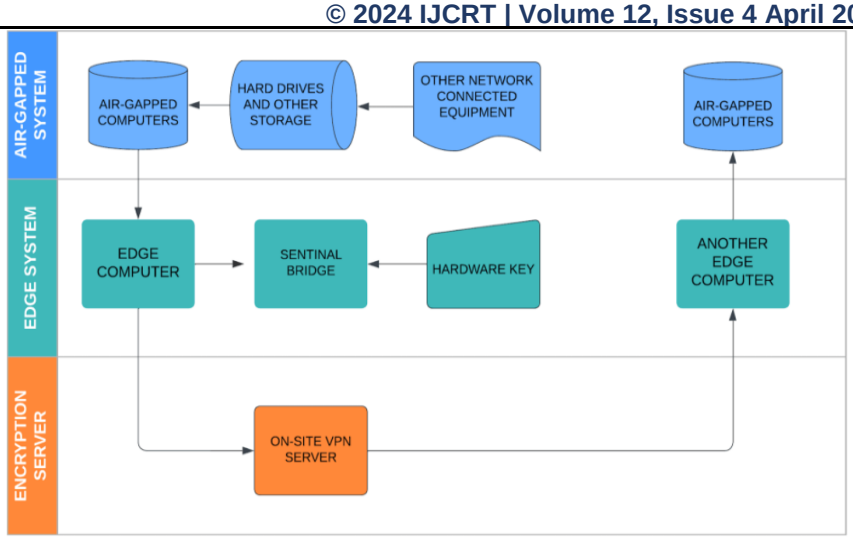

Figure 3: dataflow diagram

On-site virtual private network (VPN) server: This server enables authorized users to access the system remotely by setting up a secure VPN connection.

Other devices and PCs linked to a network: These are the gadgets that exchange data and communicate with the edge computer. An extra security precaution can be applied to an air-gapped system, which is a separate system that is physically isolated from the network as well.

X. USE CASE DIAGRAM

Users:
User 1: This user interacts with the computer system directly to encrypt data.
User 2: This user interacts with an air-gapped system to encrypt data. An air-gapped system is physically isolated from any network, making it more secure from cyber-attacks.

Systems:
Computer System: This is the main system where data is processed and encrypted.
Edge Computers: These are smaller, more powerful computers located at the network's edge, where data is first collected and processed before being sent to the main system.

Air-Gapped Systems 1 & 2: These are isolated systems used for added security. They are not connected to the main network, making it more difficult for attackers to access them.

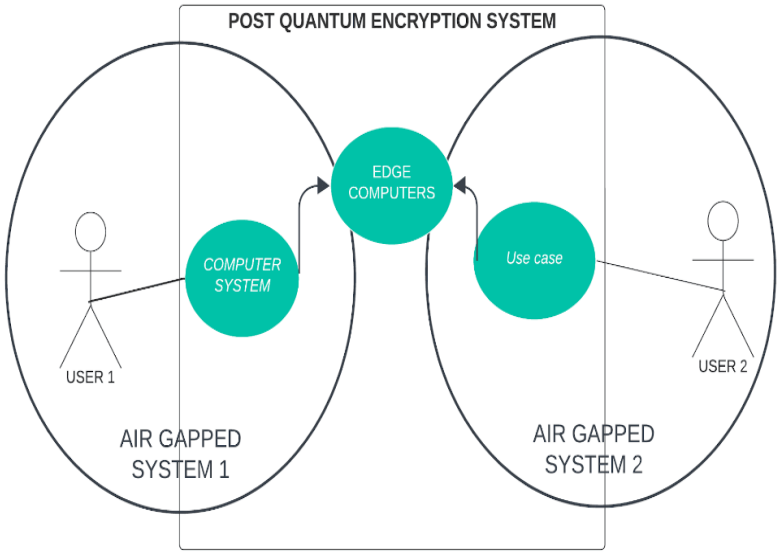

Figure 4: use case diagram

Data Flow:

User 1 or User 2 initiates encryption: User 1 interacts with the computer system directly, while User 2 interacts with the air-gapped system. Both users can initiate the encryption process.

Data is transferred to edge computers: The data to be encrypted is transferred to edge computers for initial processing.

Data is encrypted: The edge computers encrypt the data using post-quantum cryptography algorithms, which are resistant to attacks from quantum computers.

Encrypted data is transferred: The encrypted data is then transferred from the edge computers to the main computer system or one of the air-gapped systems, depending on the user's choice.

Decryption (optional): If needed, the encrypted data can be decrypted using the appropriate keys on the designated system.

XI. ALGORITHMS

Crystal Kyber: The security of Kyber, an IND-CCA2-secure key encapsulation mechanism (KEM), is predicated on how difficult it is to solve the learning-with-errors (LWE) issue over module lattices. A finalist in the NIST post-quantum cryptography project is Kyber. [5] Three distinct parameter sets, each targeting a different security level, are listed in the proposal. Kyber-512, for example, seeks security that is roughly equal to that of AES-128, Kyber-768, roughly equal to that of AES-192, and Kyber-1024, roughly equal to that of AES-256.

We suggest the following for people who are interested in utilizing Kyber:

Utilize Kyber in a "hybrid mode" in conjunction with recognized "pre-quantum" security measures, such as elliptic-curve Diffie-Hellman.

Block Cipher: A block cipher is a kind of symmetric key technique used in cryptography that works with data blocks of a predetermined length, usually 64 or 128 bits. It converts readable plaintext data into unreadable ciphertext data and vice versa using a secret key. A key component of many cryptographic systems, such as password hashing, secure communication, and data encryption, are block ciphers. AES, DES, and 3DES are a few examples of widely used block ciphers.

Hardware Token (TOTP): Time-based One-Time Passwords (TOTPs), or hardware tokens, are actual physical devices that provide one-of-a-kind, transient codes for two-factor authentication (2FA). Because hardware tokens store the cryptographic key and algorithm within, they provide an additional layer of protection above codes delivered over SMS or email, which can be intercepted. They are hence a well-liked option for protecting critical data and apps.

XII. RESULTS

Result 1:

The image is a screenshot of a terminal window on a Linux system. The window is split horizontally into two panes. The top pane is titled "Parrot Terminal" and the bottom pane is titled "Parrot Terminal (root)". Here's a breakdown of what each pane shows:

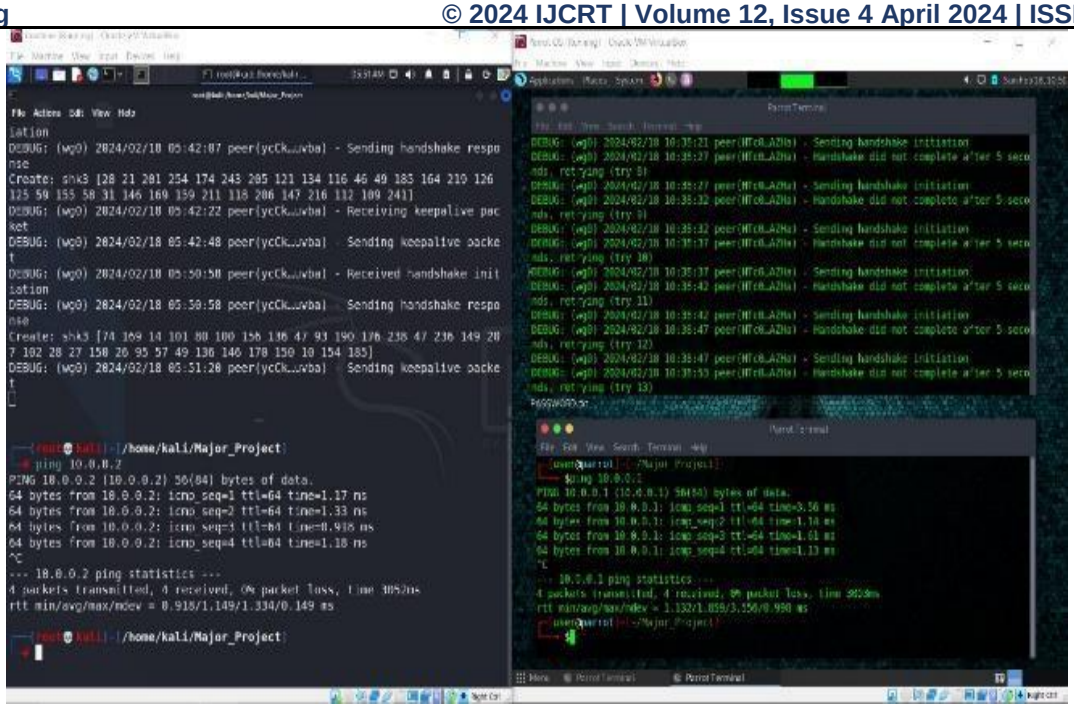

Figure 5: connection between 2 machine and sharing information without any data loss

Top Pane:
The top pane shows the user's home directory which is /home/kali.
The user is currently in a directory named "Major_Project".
The prompt at the bottom of the pane indicates the user is huser@parrot-Major_Project.
The user has executed the ping command twice. The first time pinging the IP address 10.0.0.2 and the second time pinging 10.0.0.1. The results show that the user has a successful ping to both addresses.

Bottom Pane:
The bottom pane shows the user is root with the prompt root@kali:/home/kali.
The contents of the file /home/kali/Major_Project/peerA.conf are displayed. This file appears to be a configuration file for WireGuard, a VPN (Virtual Private Network) software.

Here are some of the details of the configuration file:
Lines 1-2: These lines define the private and public keys for the device running this configuration file.
Line 4: This line describes the handshake process which is done between the 2 virtual machines for initiating the connection between 2 virtual machines.
Line 3: This line tells Wire Guard to replace any existing peers in the configuration with the ones that are specified in this file.
Line 5: This line defines the public key of a peer that this device will connect to.
Line 6: This line specifies the protocol version that will be used by the VPN connection.
Line 7: This line tells Wire Guard to replace any existing allowed IP addresses in the configuration with the ones that are specified in this file.
Line 8: This line specifies the IP address that is allowed to connect to the VPN server.
Line 9: This line specifies the endpoint of the VPN server, which is its IP address and port number.

So overall this image shows the process of connection between 2 virtual machines through a crystal kyber algorithm which can help to start the communication between the machines so they can easily exchange information without any data loss through exchanging their public and private keys. [6]

In summary, the bottom pane shows the configuration for a Wire Guard VPN client that might be trying to connect to a VPN server at the IP address 192.168.1.7, port 1000. The client would use the private key specified in the configuration file and would only allow connections from the IP address 10.0.0.2.

Result 2:

The image describes a configuration file for Wire Guard, a VPN (Virtual Private Network) software that creates secure, encrypted connections between devices. The file is named peerA.conf, and it is located in the directory /home/kali/Major_Project/pq-wireguard.

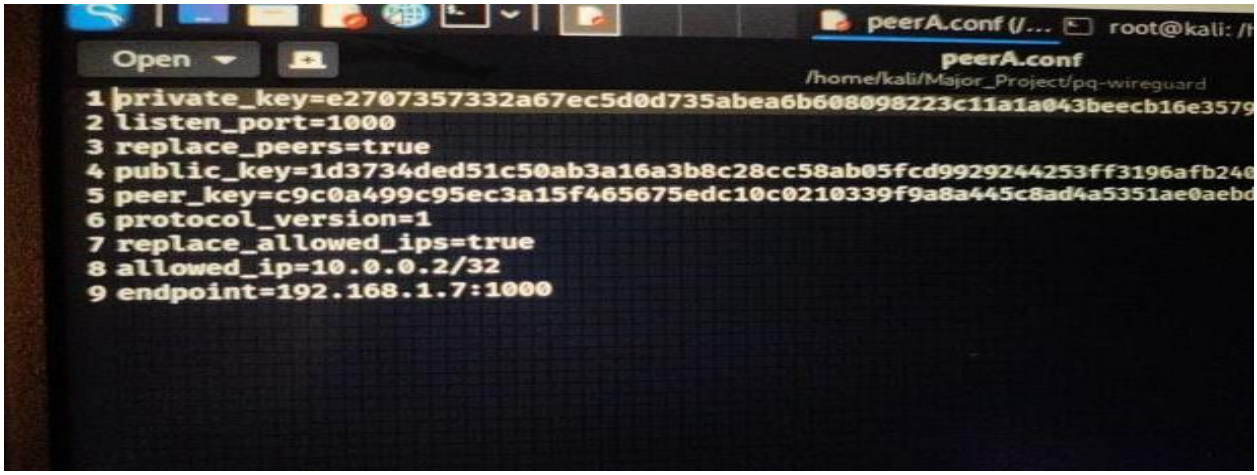

Figure 6: public and private key generated

Let's break down the contents of the file:

Lines 1-2: These lines define the private and public keys for the device running this configuration file. These keys are used to encrypt and decrypt data that is sent over the VPN connection.
Line 3: This line tells Wire Guard to replace any existing peers in the configuration with the ones that are specified in this file.
Line 5: This line defines the public key of a peer that this device will connect to.
Line 6: This line specifies the protocol version that will be used by the VPN connection.
Line 7: This line tells Wire Guard to replace any existing allowed IP addresses in the configuration with the ones that are specified in this file.
Line 8: This line specifies the IP address that is allowed to connect to the VPN server.
Line 9: This line specifies the endpoint of the VPN server, which is its IP address and port number. [7]

In summary, this configuration file is for a Wire Guard VPN client that will connect to a VPN server at the IP address 192.168.1.7, port 1000. The client will use the private key (e2707357332a67ec5d0d735abea6b608098223c11a1a043beecb16e3579) and will only allow connections from the IP address 10.0.0.2.

Result 3:

Terminal window on a Kali Linux system is split into two panes. The left pane is showing the output of various commands that have been run and a simple http server hosting a file, while the right pane is showing the contents of all network devices and the right machine accessing the http server content.

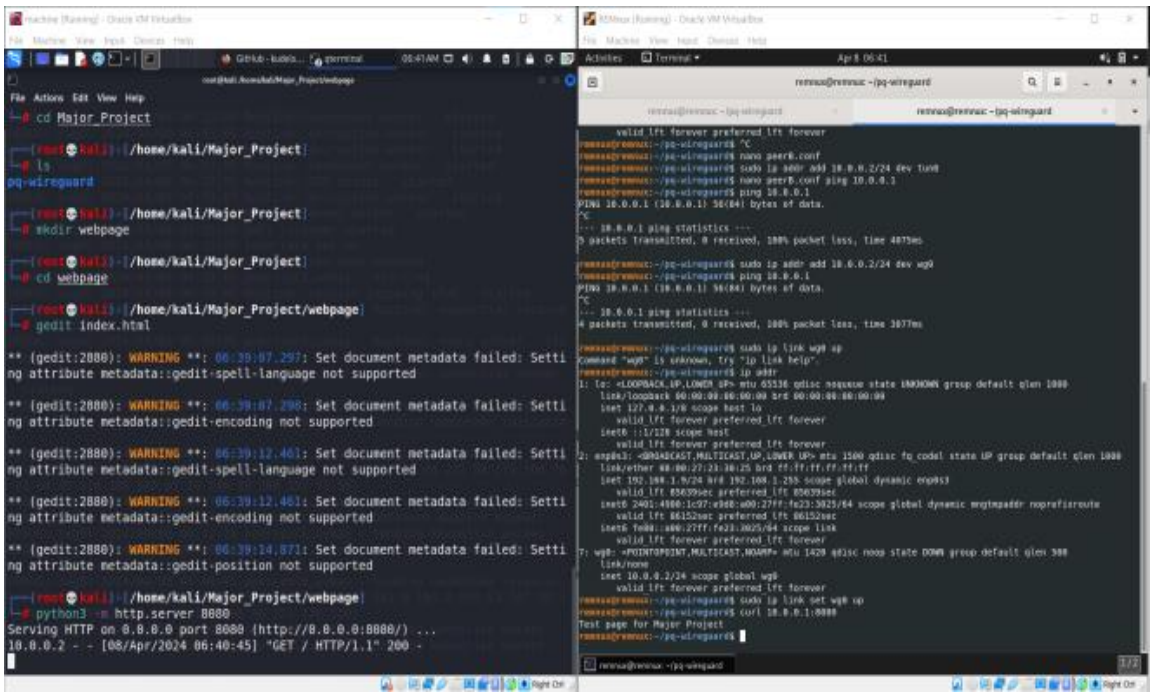

Figure 7 accessing webpage using site to site VPN

The text in the right pane is the contents of a Wire Guard configuration file. Wire Guard is a VPN (virtual private network) that encrypts traffic and tunnels it through a secure connection. The configuration file specifies the settings for a Wire Guard connection, such as the public keys of the peers and the allowed IP addresses.

Accessing Internal Web Page with Wire Guard

The image might depict setting up a Wire Guard connection, a type of VPN, on one of the networks involved in a site-to-site VPN. Here's a hypothetical explanation:

Wire Guard Server on Network A: The left pane shows commands potentially related to setting up a Wire Guard server on Network A (e.g., creating a new network interface and starting a server). The configuration file (peerB.conf) in the right pane might contain details for a peer on Network B that the Wire Guard server will connect to.

Network B with Internal Webpage: Network B could have an internal webpage only accessible on its local network.

Site-to-Site VPN: A separate site-to-site VPN connection exists between Network A and Network B. This allows devices on Network A to communicate with devices on Network B as if they were on the same local network.

Accessing Webpage: With the Wire Guard server established and the site-to-site VPN active, a device on Network A could potentially access the internal webpage on Network B. The Wire Guard connection might provide an additional layer of security for accessing resources on Network B.

Result 4:

The image shows the Wire Guard protocol being used to encrypt the traffic between 2 networks. The encryption used here is different from regular wire guard ChaCha20 whereas the encryption used is Crystal-Kyber.

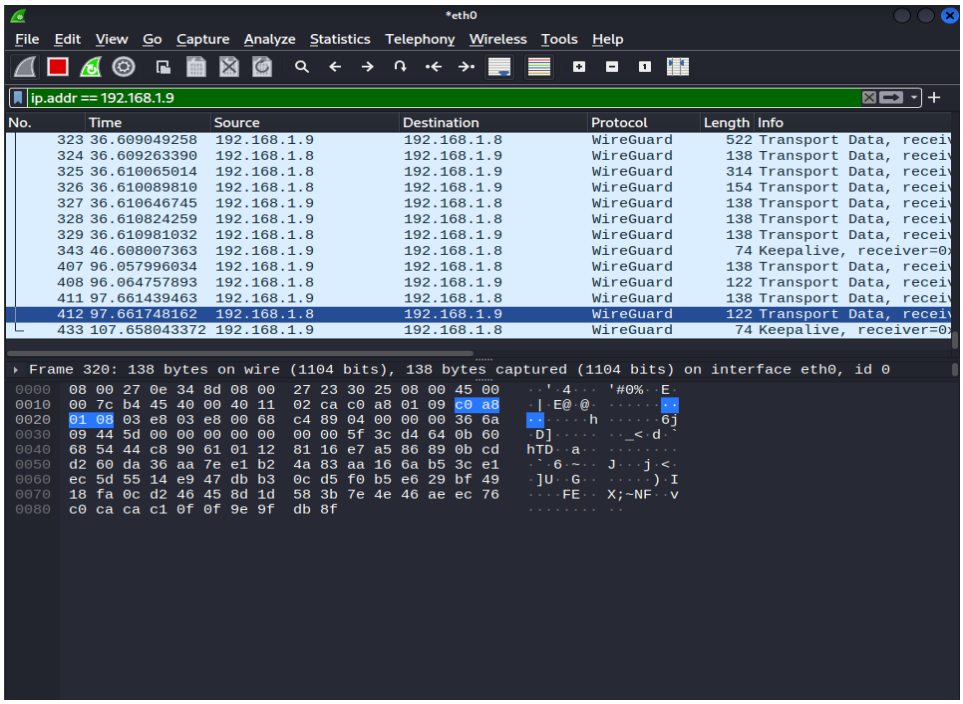

Figure 8: change in protocol

Left Pane: The left pane shows the output of wire shark running on a Kali Linux system. Where the traffic goes through the Ethernet interface of the 2 machines where the traffic is encrypted in PQE
Right Pane: The right pane shows the contents of a wire shark captured on the site to site vpn this file specifies the settings for a Wire Guard connection, such as the public keys of the peers and the allowed IP addresses.

It's possible that the Wire Guard configuration is replacing a different type of VPN connection.

Result 5:

The image you sent is a capture of a terminal window split into two panes.

Normal Interface vs. VPN for Ping Requests

Normal Interface: When you ping a device on a normal interface, the ping request travels through the internet without encryption. This means any device along the path can potentially see the source and destination IP addresses, as well as the data content of the ping request (which is minimal for pings).

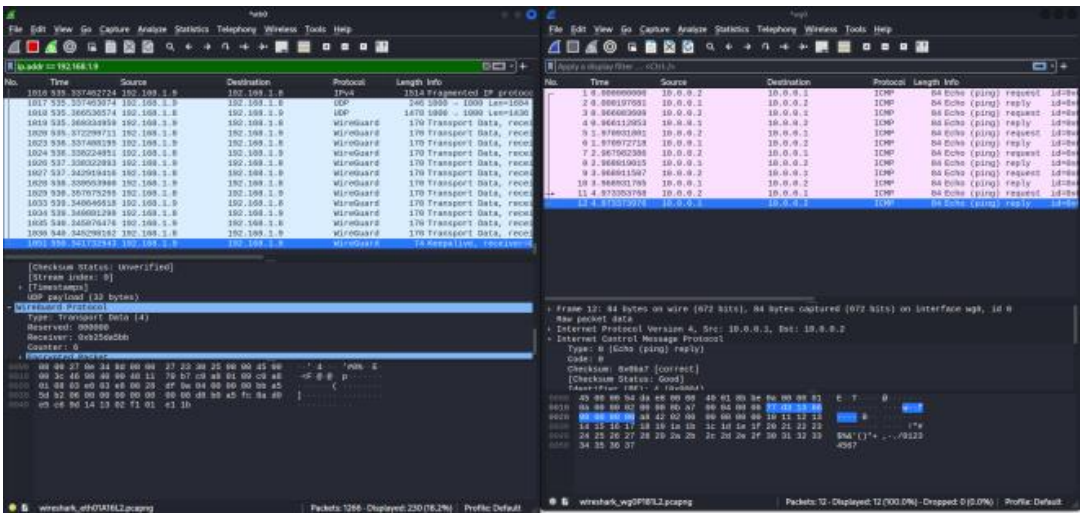

Figure 9: difference in encryption through VPN and normal interface for ping

VPN Interface: When you ping a device through a VPN, the ping request is encapsulated within the VPN tunnel. The VPN tunnel encrypts the data, including the source and destination IP addresses. This encryption makes it much more difficult for someone snooping on the network traffic to see the actual content of the ping request.

The left pane shows commands possibly related to setting up a Wire Guard VPN (creating a network interface and starting a server), it doesn't definitively show actual ping requests being sent.
The configuration file (peerB.conf) on the right pane likely contains encryption keys for the Wire Guard connection, but these keys wouldn't be visible in the capture.

Result 6:

Encrypted Packet in Wire shark
The packet you sent appears to be encrypted based on the following:

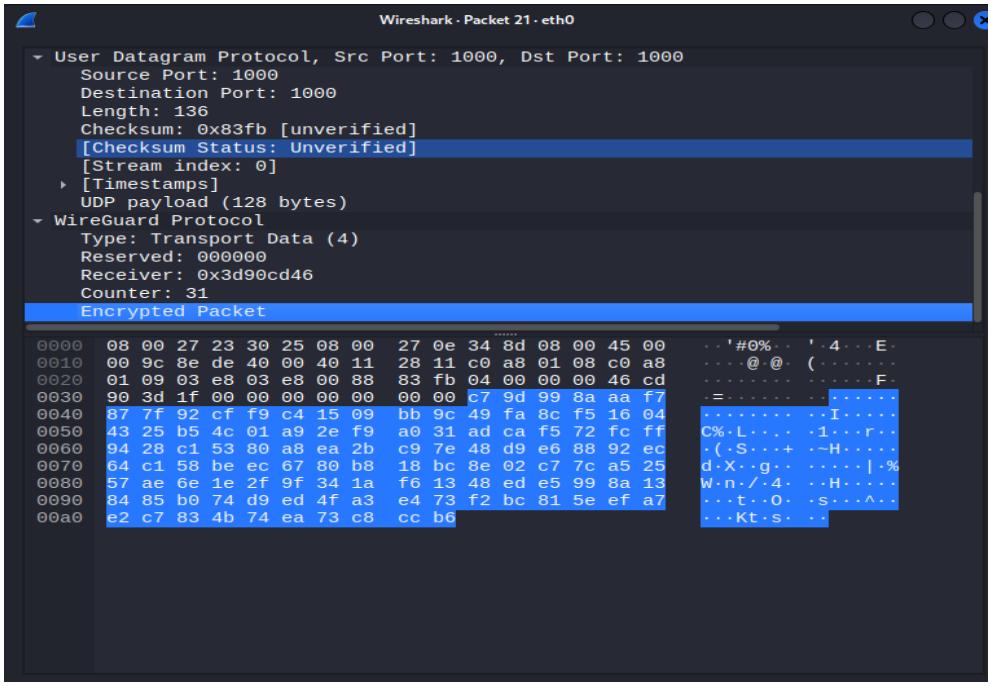

Figure 10: encrypted packet as seen on wire shark

Transport Layer Protocol: The capture shows UDP (User Datagram Protocol) in the Transport Layer field. UDP itself doesn't provide encryption for the data it carries.

Wire Guard Protocol: The capture indicates the packet uses the Wire Guard protocol. Wire Guard is a VPN (Virtual Private Network) protocol that encrypts data traffic.
While the capture suggests the packet is encrypted with Wire Guard, Wire shark itself cannot decrypt the content without additional information

Missing Keys: Wire shark typically needs decryption keys used by the encryption protocol to decrypt the packet content. These keys are not included in packet captures for security reasons.
Pre-Shared Secret: In the case of Wire Guard, decryption would likely require the pre-shared secret used to establish the VPN connection.

General Information on Encrypted Packets
Encrypted packets are essential for securing communication on networks. When data is encrypted, it's scrambled into an unreadable format using encryption algorithms and keys. Only authorized parties with the decryption keys can unscramble the data and read its contents.

Here are some benefits of using encrypted packets:
Confidentiality: Encryption ensures that only authorized users can access the information within the packet.

Data Integrity: Encryption helps to protect data from being tampered with during transmission.

Result 7:

Wire shark, a network protocol analyzer; we can discuss how it potentially relates to data being shared in encrypted and plain text forms on a VPN interface.

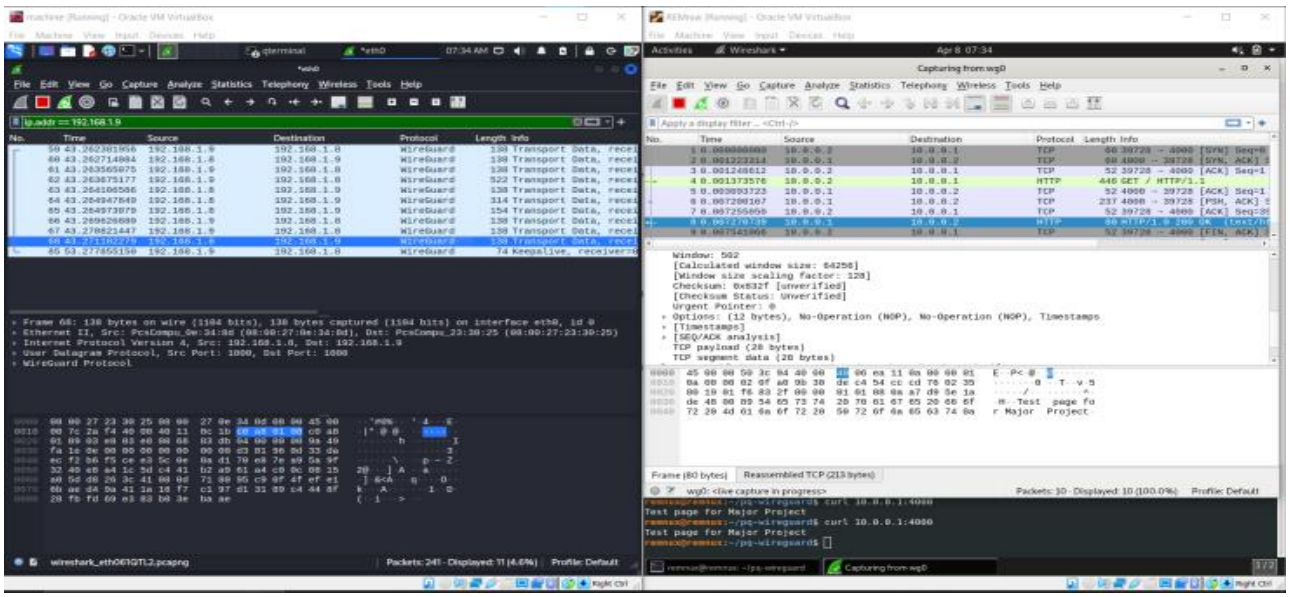

Figure 11: data shared in encrypted form as well as plain text on VPN interface

Encrypted vs. Plain Text Data on VPN

While the capture doesn't definitively show data transfer, it offers clues that data might be shared in both encrypted and plain text forms over a VPN interface:

Wire Guard VPN: The capture mentions "Wire Guard" in multiple places, indicating the traffic is likely related to a Wire Guard VPN connection. Wire Guard is a VPN protocol that encrypts data traffic to ensure confidentiality.
Encrypted Packets: The capture shows several packets with the "Wire Guard" protocol label. These packets likely contain encrypted data because Wire Guard encrypts user data traveling through the VPN tunnel.

Plain Text Source/Destination: The capture shows source and destination IP addresses in plain text for some packets. This suggests that while data within the VPN tunnel might be encrypted, the IP addresses involved in the communication might be visible in plain text.

The capture might be from a device configured with a Wire Guard VPN.
The device might be communicating with another device over the VPN connection.
The encrypted packets likely contain the actual user data being transferred securely.
The source and destination IP addresses, while not necessarily part of the encrypted data, might be visible in plain text within the capture.

XIII. CONCLUSION

The convergence of air-gap systems and Post-Quantum Cryptography (PQC) provides an effective solution for securing communications in an era of evolving threats. While air-gap systems have traditionally offered a high level of security, the potential of quantum computers to break current encryption methods requires a pre-emptive transition to PQC.

The adoption of post-quantum encrypted communication in air-gapped systems iS
Crucial for long-term security in sensitive environments. Quantum computing advancements pose a threat to current encryption methods, making proactive measures essential. This transition involves complex considerations such as compatibility and performance, but it is vital for safeguarding critical operations and sensitive data in the face of emerging quantum threats and ensuring trust and security in the quantum era and beyond.

XIV. REFERENCES

[1] M. A. R. B. Aymen Ghilen, "Q-OpenVPN: A New Extension of OpenVPN Based on a Quantum Scheme for Authentication and Key Distribution," in International Conference on Cryptology and Network Security, December 2015.

[2] N. v. A. T. A. T. V. Maran van Heesch, "Towards Quantum-Safe VPNs and Internet," 2019.

[3] K. K. B. L. C. P. G. Z. D. S. Karen Easterbrook, "post-quantum-crypto-vpn".

[4] D. D. M. D. Y.-K. L. Dr. Lily Chen, "Post-Quantum Cryptography Standardization," NIST Computer Security Resource Center CSRC, 03 January 2019.

[5] C. C. M. N. a. D. S. J. W. Bos, "“Post-quantum key exchange for the tls protocol from the ring learning with errors problem," IEEE Symposium on Security and Privacy, pp. 553-570, 2015.

[6] L. D. E. K. T. L. V. L. J. M. S. J. Bos, "“CRYSTALS-Kyber: a CCA- secure module-lattice-based KEM," IEEE European Symposium on Security and Privacy (EuroS&P), 2018.

[7] A. B. F. C. G. P. a. P. S. M. Baldi, "a post-quantum key encapsulation mechanism based on qc ldpc codes," in International Conference on Post-Quantum Cryptography, 2018.

[8] "OpenVPN," [Online]. Available: https://openvpn.net/.

[9] "OpenSSL," [Online]. Available: https://www.openssl.org/.

[10] "Open Quantum Safe - OpenSS," [Online]. Available: https://github.com/open-quantum-safe/openssl.

[11] "Post-Quantum, VPN," [Online]. Available: https://www.postquantum.com/vpn/.