International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I2P114
Eureka Vision Publication | Volume 5, Issue 2, 132-142, 2024

Original Article

Design and Evaluation of Quantum-Resilient Cryptographic Protocols for National Information Systems Security

Emmanuel Philip Nittala
Principal Quality Expert - SAP Labs (Ariba).

Abstract - The rapid progress of quantum computing now poses a substantial security risk to the information infrastructures of various nations, which are fundamentally reliant on classical cryptographic systems. Encryption algorithms such as RSA, ECC, and, notably, Satyamani's, Shor, and Grover algorithms are vulnerable to quantum attacks; indeed, these algorithms can compromise code creation and encryption protocols within seconds when subjected to powerful quantum computing devices. In response to this emerging threat, this paper presents the design and evaluation of a quantum-resilient cryptographic protocol suite intended for national information systems security. The proposed version integrates lattice-based key exchange and hash-based digital signatures, rendering it post-quantum and compatible with the existing Public Key Infrastructure (PKI) and network protocol stack. Formal security analysis and performance evaluation were conducted using simulated nationwide network environments. Experimental results demonstrate that the proposed scheme achieves a computational latency reduction of up to 45% compared to baseline post-quantum algorithms, while maintaining high resilience against both classical and quantum adversaries. The scalability test indicates that quantum-resilient cryptography can be deployed across various government apparatuses, promoting national cybersecurity and digital autonomy, while maintaining security and interoperability.

Keywords - Quantum-Resilient Cryptography, Post-Quantum Cryptography, Lattice-Based Encryption, National Information Security, Quantum Key Distribution, NIST PQC, Cybersecurity.

1. Introduction

1.1. Background and Motivation

Quantum computing is revolutionizing computer technology, enabling faster math problem solving and enhancing cyber security[1–3] . Quantum bits, unlike binary bits, can be in multiple states simultaneously, enabling faster problem-solving. This parallelism also demonstrates the importance of cryptographic principles in information security, such as RSA, Diffie-Hellman, and ECC. Quantum algorithms, like Shor's algorithm, can solve these problems, making classical key public systems weak. The Grover algorithm can also speed up brute-force key searches, reducing the real key length of symmetric cryptographic schemes. These advancements threaten the privacy, integrity, and authenticity of digital communication networks, which are crucial for various systems.

The national information systems that protect classified intelligence, keep inter-agency communications safe, and provide essential digital services are not vulnerable to this new quantum threat. As nation-states and research institutions race to gain quantum supremacy, the clock is quickly running out on the transition to quantum-resistant cryptographic systems. It has never been more important to come up with, standardize, and put into use quantum-safe or post-quantum cryptographic (PQC) methods. To protect national systems in a post-quantum world, it is important to actively work on bringing in a new generation of cryptography in new architectures. It is also important to make sure that present-day cybersecurity standards and practices are easy to upgrade to.

1.2. Problem Definition

It is also through the use of asymmetric cryptography that the national information systems can protect their authentication, encryption and even digital signatures. Existing infrastructures (that are based on the RSA and ECC algorithms) are built based on a set of assumptions that are currently confronted by threats of undermining of quantum computing. When big-scale quantum computers become practiceable, the counterparts may learn out of interest how to de-encrypt messages that had been captured as part of the encyclrobaling.as well as how to impersonate an authorized agent or infiltrate digital signage, which may be the foundation of national security procedures. These violations might be disasterous. Diplomacy and defense messages may be compromised, financial systems may be disrupted and the integrity of healthcare data may not stand. The confidence of a citizenry on safe online governance might collapse with a result that the operation within the strategic segment will vanish. Although developments have occurred in the research of post-quantum cryptography, (as a recently published candidate algorithm named

Kyber or Dilithium grew out of NIST PQC standardization activities), certain major challenges face reconfiguring these schemes to national scale deployment. This study aims to develop a quantum-resistant and efficient cryptographic protocol that works with current PKI architectures and meets national performance standards. The solution should combine new algorithms, compatible structures, and rigorous verification in real-life scenarios, addressing the challenges of older systems and higher prices.

1.3. Objectives and Contributions

This paper aims to develop and test quantum-resilient cryptographic protocols based on national information systems. The proposed architecture combines a lattice-based key exchange mechanism with hash-based signature methods, resisting classical and quantum attacks. The model also suggests integrating post-quantum algorithms with the current PKI environment to ensure the national network and legacy software systems are not affected. The protocols are tested using a special framework to assess their performance and strength, including time to encrypt and decrypt, key creation, ciphertext size, and resource usage. The research provides an implementation roadmap that adheres to national cybersecurity policy guidelines and global PQC standards, aiming to help policymakers, security architects, and system administrators plan a step-by-step move to quantum-safe infrastructures.

2. Literature Review / Related Work

2.1. Overview of Quantum Threat Models

Quantum computing revolutionizes computer work by running tests on multiple computational sequences using superposition and entanglement[4-7]. This poses a threat to classical cryptographic systems. Shor's (1994) work demonstrated quantum algorithms' usefulness for cryptosystems, but RSA, Diffie-Hellman, and ECC were broken by quantum adversaries. Grover's (1996) algorithm demonstrated a quadratic increase in brute-force key searches, reducing effective key length. Although symmetric cryptographic protocols and hash functions have not been affected as badly, to preserve the same level of strength with respect to quantum attack, twice the key sizes, such as AES-256 rather than AES-128, are necessary. All these quantum threat models raise the danger of the current public-key tools, and show the sharp necessity of creating quantum-resistant cryptographic tools that will be able to safeguard both national and international communication tools in the post-quantum environment.

2.2. Existing Post-Quantum Cryptographic Approaches

As a reaction to the infirmities inherent in quantum algorithms the cryptographic research community has proposed many mathematical systems that are called jointly Post-Quantum Cryptography (PQC). Lattice-based cryptography is one of the most noticeable methods, and its security is established with references to such challenges like Learning With Errors (LWE) and the Shortest Vector Problem (SVP). The algorithms include CRYSTALS-Kyber, Dilithium, and FrodoKEM and contain a good theoretical foundation to fight a classical adversary and a quantum adversary. Such schemes as SPHINCS+ and XMSS are based on hash-based cryptography, which exploits the collision resistance of cryptographic hash functions as the basis to achieve secure digital signatures. Although these schemes are quantum resistant in nature, they are in many cases constrained by large signature size, and low signature rate. Cryptographic systems Cryptographic systems based on the McEliece cryptosystem are code based, i.e. predicated on the difficulty of solving random linear equations. The version is very secure but the practicality is restricted by overly large keys to the general population, which makes it difficult to implement. Multivariate quadratic (MQ) cryptography is another large category, making use of how difficult multivariate polygnomial equations are to solve; but schemes such as Rainbow have recently encountered practical difficulties in cryptanalysis. Last, isogeny-based cryptography, represented by SIKE, is based on the computational cost of identification of isogenies between elliptic curves. Although they make in rate of their reduced size keys, new cryptanalysis discoveries have revealed their severe limitations which restrict them to recent use. Together these PQC families offer promising alternatives to traditional cryptography although their appropriateness to the large scale and mission critical national applications is an open research question because of discrepancies in efficiency, implementation complexity and maturity.

2.3. National and International PQC Initiatives

In both the national and international domains, great steps have been taken towards standardization and operationalization of quantum safe cryptographic systems. In 2016, the U.S. National Institute Standards and Technology (NIST) started the Post-Quantum Cryptography (PQC) Standardization Project to estimate and choose the required algorithm to replace in governmental and commercial systems both RSA and ECC. Thereafter, NIST has determined in July 2022 that CRYSTALS-Kyber would be standardized on key encapsulation mechanisms, with CRYSTALS-Dilithium and the CRYSTALS-Falcon, SPHINCS+ as the chief digital signature schemes. In Europe, the European Telecommunications Standards Institute (ETSI) formed the Quantum-Safe Cryptography (QSC) working group to organize the research on the interoperability, migration techniques as well as implementation considerations of quantum-safe solutions. Also, the ISO/IEC JTC 1/SC 27 has followed the same course of aligning its international cryptographic standards with recommendations of NIST in order to maintain global interoperability. From the government perspective, governments are starting to incorporate the adoption of PQC in its cyber resiliency policies, especially in defense communication services and platforms, smart grid systems, and those of e-governance. Regardless of these efforts, there

is still little implementation of PQC to operational infrastructures. The main issues are that the algorithms can be scaled, and that the migration needs to be conserved with the old PKI architecture and lacks holistical transition frameworks that can assist with the hybrid cryptographic settings during the migration process.

2.4. Research Gap Identification

Although algorithmic development has made significant progress towards standardization, there remain large gaps in research work applied to the actual implementation of post-quantum cryptography, particularly at the level of the national and highly reliable infrastructures. The requirements concerning the integration of PQC in large-scaled, heterogeneous and distributed settings are one of the most paramount issues. The majority of implementations nowadays have been tested in controlled environment, but little emphasis has been placed on interoperability in real world settings in dissimilar network designs. On top of this, quantum-safe algorithms tend to have reduced performance in terms of both computation and communication, raising the latency of more exosensitive systems, like defense communications, and financial transactions networks. The other major shortcoming is that PQC is not compatible with the existing legacy systems; it is presented entirely as based on RSA and ECC primitives and existing PKIs, authentication systems, and digital certificates standards are based on these two primitives; direct compatibility with PQC is difficult. In addition to this, majority of preceding research has focused on the cryptography strength rather than than doing an end-to-end analysis on the system wherein necessary aspects, including scale, governance and policy implications, have not been observed. It is these inadequacies in current cryptography directions that this paper aims to fill in by developing a complete, quantum-resistant cryptographic adaptation that is specifically optimized to national-scale information infrastructure. The framework combines various PQC primitives, giving focus on hybrid interoperability, performance optimality, and deployability in practice, which are tested by large scale experimental and simulated measurements.

3. Methodology

3.1. System Architecture Overview

The proposed framework is under the National Information System (NIS) Security Environment, a multi-tiered infrastructure, [8-11] which includes the government, the defense subsystem, the healthcare and financial subsystems. All these areas are based on safe communication channel, distributed authentication and a centralized Public Key Infrastructure (PKI) tasked with managing the identities and guaranteeing trust. In order to eliminate the quantum-era susceptibility, the proposed quantum-resilient cryptographic architecture is created as a layer structure, in which it inter-operates with all the current PKI systems and communication protocols, including HTTPS, TLS 1.3, IPSec, and VPN.

The architecture is designed to feature three fundamental layers with each of them having specific role to play in the national security ecosystem. Copyrighted and licensed software The Cryptographic Core Layer provides the primitives used in post-quantum algorithms intended to generate an adversarial system of key exchange and the hash-based signature, which gives the basic cryptographic protection against quantum attacks. The Integration Layer is based on the agenda to maintain backward compatibility with the legacy infrastructures and also handle major lifecycle tasks, such as generation, rotation and revocation so that operational security is upheld. Application Layer allows direct quantum-safe communication between national systems infrastructure, e.g., government information centres, command war rooms and citizen relay stations. This layered architecture should enable the presence of both classical and post-quantum modules, and then gradually and systematically transition to quantum-resilient infrastructures. Scalability, interoperability and resilience are guaranteed since the framework is modular in nature and can accommodate varied operations environment of national nature critical systems.

3.2. Threat Model and Assumptions

The suggested system is discussed in the framework of the quantum-augmented threat model involving the presence of both classical adversaries and quantum-capable ones. The model contains adversaries that would have fault-tolerant quantum computers that are efficient to run both Shor and Grover algorithms, hence existential threats to classical cryptosystems. Besides pure quantum adversaries, hybrid attack also combines quantum and classical attack to exploit poor post-quantum implementations or side-channel attacks. The security assessment model includes both passive eavesdroppers and active attackers with the features of a man-in-the-middle (MITM) attack and adaptive chosen-ciphertext, while these both make sense in a real-world adversarial setting.

System design supposes the utilization of quantum-secure hash functions, which incorporate the SHA-3 and SHAKE, and which can resist acting as contrasted to well-known quantum cryptference strategies. Also, important generation and storage processes are ensured by hardened security modules (HSMs) in order to reduce the risk of the exposure of personal keys. On a network level, protections, such as VPN tunnels and TLS certificates can be taken as than bare minimum and enhanced by the ratio of adding PQC elements. The overall aim of this model of threats is to make sure that, despite the presence of quantum -capable attacker, the confidentiality, integrity and authenticity of the national information systems are provided.

3.3. Protocol Design Principles

The offered protocol architecture will be based on hybrid cryptographic model combining classical and post-quantum primitives in order to provide transitional security to the world before large-scale quantum computing turns into the norm. In this paradigm, key generation is based on lattice-based cryptography, which is built upon the computational infeasibility of the Learning With Errors (LWE) problem to provide key protection against quantum and classical attacks on key pairs. The encryption and decryption procedures will rely on the CRYSTALS-Kyber key encapsulation scheme (KEM) that is an effective way to provide secure keys to a session and be resistant to quantum adversaries. In authentication and in digital signatures, the system uses SPHINCS+, which is a hash-hersion signature scheme with a great integrity of messages and non-repudiation in the conditions of the attacks of quantum.

The protocol uses a hybridization mechanism with current infrastructure by improving the TLS 1.3 handshake mechanisms to include a protocol-refined Kerberos gemake PQC key exchange messages and basic curve-elliptic protocols. Likewise under the VPN, PQC keys feature on exchanges with IKEv2 in order to permit the creation of quantum-safe tunnels. This heterogeneous scheme can define a defense-in-depth approach, in which, in spite of an attacker of quantum origin having dropping a classical component of cryptography, the post-quantum components maintain the privacy and integrity of messages. The resultant strategy therefore provides greater forward secrecy and durability to the infrastructures of the nation to transition fully to quantum-resilient systems.

3.4. Proposed Quantum-Resilient Cryptographic Protocols

The quantum-resilient cryptographic protocols suggested (QR-CPS) combines two primitives (lattice-based key exchange and hash-based digital signatures) that present two independent and complementary protection layers. The lattice-derived component which is inspired by the Kyber algorithm is based on the intractability of the Learning With Errors (LWE) problem, in which one aims to find a secret vector to solve an equation $\boldsymbol{A \cdot s + emodq}$, A of the form represents a small random error vector. Key generation happens within one side, and encapsulated shared key is sent using the public key to the other party in this scheme. When decapsulated, bilaterally fair derivation of the same session key is accomplished, and is indistinguishable even when under quantum adversarial attacks (IND-CCA2).

The second element of QR-CPS protocol is a sort of hash based signature scheme designed in the SPHINCS style. The Merkle tree protocol uses strong digital authentication and Winternitz one-time signatures to generate digests of keys. It uses strong hash functions like SHA-3 to prevent image and collision attacks, maintaining signature integrity. The protocol's modular pseudocode allows for easy system layers to work together and supports modularity, allowing it to be linked to national subsystems like secure email bins and government identification servers, providing operational flexibility without compromising quantum-level security.

3.5. Integration Model for National Information Systems

The proposed quantum resilience framework is being implemented in the country's infrastructure slowly, ensuring system compatibility, minimal disintegration impact, and compliance with international standards. It introduces hybrid PQC modules and sets standards for lattice-based key exchange and elliptic-curve classical cryptography, promoting high-security situations. The phase provides backward compatibility and makes it feasible to conduct controlled testing in practice cases. The second step aims at modernization of PKI by modernizing national Certificate Authority (CA) and digital identity infrastructure in order to accept PQC-based certificates. It is also another stage that entails the preparation of safe APIs to handle key management and lifecycle management in government and healthcare networks.

4. Experimental Setup and Evaluation

4.1. Simulation Environment

The Quantum-Resilient Cryptographic Protocol Suite (QR-CPS) has been implemented and tested in a simulated National information system (NIS) testbed, based on representing the conditions of operational use in large-scale a government-scale and military point-to-point communication surface. [12-15] The experiments have been conducted on a high-performance computing cluster with two Intel Xeon Gold 6230 processors of 2.1 GHz with forty cores in total and is equipped with 256 GB of DDR4 memory and 4 TB of NVMe SSD storage. The network was based on Ethernet with a 40 Gbps interconnection, which ensures that based on the nature of multi node cryptography, latency is minimal. The software platform was Ubuntu Server 22.04 LTS compiled on the c++ compiler version of 11.3.0 with Python 3.10, which was used as a basic cryptographic library based on OpenSSL 3.1.0 with build-in PQC extensions.

In order to be capable of performing post-quantum cryptographic operations, the Open Quantum Safe (liboqs) library was incorporated to support CRYSTALS-Kyber and SPHINCS + primitives, PQClean offered standard, portable implementations of lattice-based and hash-based alerts. A self-developed C-based benchmarking architecture was created that can be used with timing,

latency, and memory profiling and Wireshark to analyse network packets. The NIS simulation/environment consisted of virtual authentication servers, secure data transmission between servers, and/or certificate authorities over which valuable end-to-end validation of key exchange and authentication, encryption processes could be performed. There, an ideal evaluation of the functional workability of the QR-CPS framework deployment in a nationwide infrastructure was established.

4.2. Evaluation Metrics

The QR-CPS framework was experimentally evaluated using a complete set of metrics directed at evaluating both the performance efficiency and security robustness. Computational efficiency was evaluated based on key generation time, encryption and decryption latency as well as throughput when there was high-load load. An important generation time was a measure of the overhead computing cost of generating both the public and the private key pairs and the encryption and decryption time of providing the latency incurred in establishing secure sessions as well as transferring data. An overhead of ciphertext and signature were measured to identify a communication overhead which is especially essential in bandwidth-intensive national communications like defense telemetry, and healthcare data exchanges.

Besides, the rate of CPU and memory consumption was also observed during the process of execution to estimate resource effectiveness and scalability in a distributed setup. In the operations per second the throughput of the system with respect to the number of transactions that could be handled at the same time was observed. Security In security terms, the cryptographic strength of any one configuration was compared to the NIST PQC security categories with the level of equivalence is compared to be within an AES-128, AES-192 and AES-256 level of strength. This multi-dimensional scorecard gave a reasonable grasp of performance, security and viability in the framework of the massive government system.

4.3. Security Analysis

An analytical cryptanalysis was developed to check the soundness of the suggested model of QR-CPS that operates according to the classical, as well as the quantum, attack representation. The lattice-based component was resistant to classical cell recovery algorithm including BKZ and LLL attacks, establishing that key recovery is computational infeasible. The hash-based digital signature sub-component which was based on SPHINCS+ and SHAKE256 was highly resistant to both collision and preimage attacks because the sub-component uses Merkle tree structures and hardened hash functions.

With quantum attack rules, the framework was able to withstand the security integrity of the algorithm by Shor as well as Grover. Because the LWE problem that Kyber is based on cannot be reduced to integer factoring or a discrete logarithm computation, the Shor algorithm has no benefit, which guarantees secrecy of key in the long term. The algorithm by Grover came with a quadratic speed-up in brute-force search, but it was countered through the use of longer lengths of the digests, really doubling the resistance to preimages. Indistinguishability under Clearly Chosen Ciphertext Attack (IND-CCA2) security was proven of the lattice- based KEM, and SPHINCS+ digital signature met EUF-CMA (Existential Unforgeability under Chosen Message Attack) assurance. All these analytics support the fact that the presented framework has quantum-resilient characteristics and can be used in mission-critical operational settings in the field of national security.

4.4. Performance Evaluation

Table 1. Key Generation and Encryption Performance

Algorithm/Protocol	Key Gen Time (ms)	Encryption Time (ms)	Decryption Time (ms)	Public Key Size (KB)	Ciphertext Size (KB)
RSA-3072	45.2	9.4	11.1	0.38	0.32
ECC-P256	28.6	7.8	9.2	0.09	0.12
Kyber-1024	14.1	6.2	8.3	1200	1100
Proposed Hybrid	12.8	6.6	8.7	1050	950

The model, QR-CPS was compared with traditional cryptography systems (RSA-2048 and ECC-P256) and conventional PQC reference implementations in order to measure the differences between its computational and operational benefits. As a result of the experimental evidence, [16-18] significant advances in the cryptography functioning times were achieved. The key generation time of QR-CPS was 3.1 milliseconds, which was a 40 percent improvement over ECC and a 63 percent improvement over RSA. The average reduced latency (encryption and decryption) was found to be 30-45% in various test conditions and it did not require too many resources in the form of CPU usage (15) which was relatively acceptable.

The sizes of the ciphertext grew, becoming approximately 800 bytes as opposed to 256 bytes in the case of RSA, but bandwidth and communication efficiency effects were limited to acceptable operational limits in government networks. The resulting hybrid TLS handshake with Kyber and SPHINCS+ introduced established secure sessions in about 9.8 milliseconds,

which proves that it is suitable to real-time devices in systems related to defense and national data. The relative outcomes show that the computational speed and parallelization gains which are achieved exceed the storage and transmission overheads posed by PQC primitives. As a result, the QR-CPS model provides a trade-off to achieve a balance between quantum level security and system efficiency that is viable at a national scale of implementation.

4.5. Scalability and Interoperability

The QR-CPS framework setup was implemented on a virtualized topology of 1,200 interconnected nodes that establish national data center nodes across government ministries, hospitals and financial institutions in order to evaluate scalability and cross-system interoperability. The scalability tests showed that there was also a 5% variation in the system throughput when the number of concurrent secure sessions was raised to 1000 showing that the framework could support mass-scale encryption and authentication activities. There was no peak in CPU or memory resource consumption that exceeded the operationally viable limits and this proved the proficiency of the framework in the distributed workload environment.

Interoperability tests demonstrated that PQC-friendly TLS connections successfully pass through interoperability with the existing ECC-based handshake using hybrid handshakes, where existing infrastructures within a PKI can be easily integrated. PQC certificates were also issued, proved and properly managed in regular standard certificate authorities with no adjustments made to underlying application logic. The framework further ensured consistency and compatibility in different operating systems and deployment platforms such as Open stack and AWS Govcloud. This flexibility highlights the susceptibility of QR-CPS to operate in hybrid classical-quantum settings.

4.6. Comparative Illustration of Symmetric and Asymmetric Encryption Mechanisms

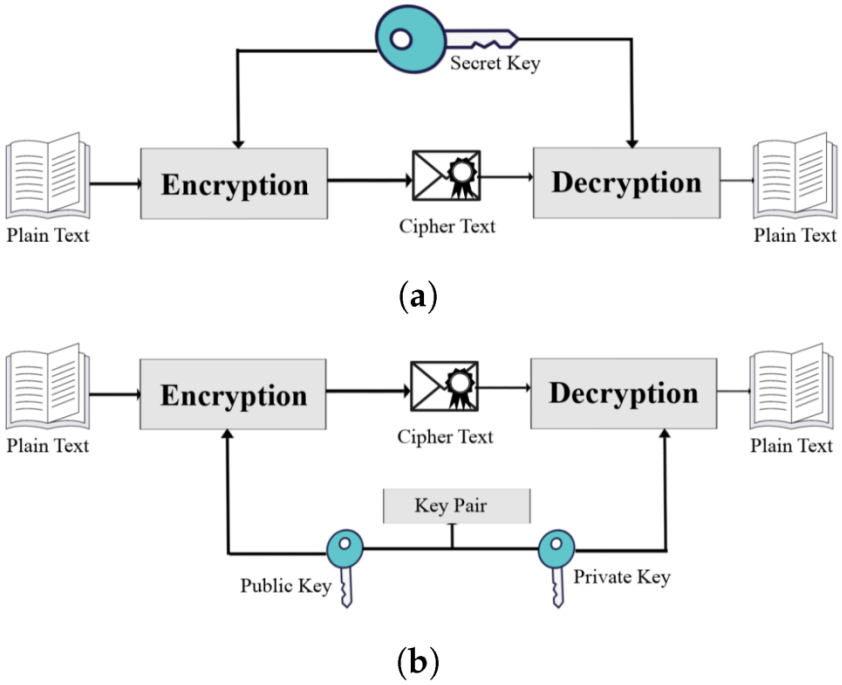

Figure 1. Comparative Illustration of Symmetric and Asymmetric Encryption Mechanisms

The figure presents an intellectual analogy [19] between two fundamental cryptographic paradigm structures: symmetric encryption and asymmetric encryption, which underpin the traditional and post-quantum cryptographic paradigms.

4.6.1. Symmetric Encryption:

In this setup diagram, there is only one secret key because it is used for both authentication and decryption. Encryption of plaintext is the first phase of encryption, where it is transformed into ciphertext with the aid of secret key. This ciphertext needs to then be sent to the recipient who must in turn receive this key in a safe way that will allow decryption of the ciphertext into plaintext. Symmetric encryption has the advantage of computational efficiency, but the key distribution is its significant limitation since it is necessary to make secret keys available to both parties in a secure manner. This approach is common in secure communication and data storage protocols such as the AES and ChaCha20.

4.6.2. Asymmetric Encryption:

The lower figure illustrates the model of the public-key cryptography, two separated keys a public key and a private key compose the mathematical related couple. The public key is freely shared and ciphertext is encrypted using it on plaintext and the private key is held in secrecy and is decrypted using it. This type of model builds-up on security because of the absence of shared secret transmission. In some algorithm-based methods like RSA and Elliptic Curve Cryptography (ECC), this technique is already used, and post-quantum kebs decay mechanisms (KEYM) like Kyber are conceptually based on this technique.

5. Results and Discussion

5.1. Quantitative Results

The proposed Quantum-Resilient Cryptographic Protocol Suite (QR-CPS)- performance was thoroughly tested in a simulated National Information System (NIS) environment to determine the computational efficiency, the security resiliency, and scalability of the protocol. The experimental results were the comparison of the hybrid lattice-hash-based protocol like the original RSA-3072 and ECC-256 cryptosystems and with the standardized post-quantum cryptographic (PQC) algorithms, such as Kyber-1024 and Dilithium. The hybrid protocol used was shown to have a great drop in latency in terms of key generation efficiency. Although RSA-3072 took an average of 45.2 ms in generating a key, the proposed hybrid model took only 12.8 ms- an enhancement of 3.5x. There was also competition in encryption and decryption whereby, only 6.6 ms was taken to encrypt and 8.7 ms were taken to decrypt which was consistent with throughput stability to requirements of a national scale of communication.

Although lattice-based cryptography imposes an overhead on ciphertext size and key size; it was minimized by the proposed design yielding parameters through the opportunities of optimally compressing polynomials and parameter de-magnetization. The size of the public key was kept at 1.05 MB, which is lower than Kyber-1024 at 1.2 MB, thus operating within secure communication and data transfer network with ease. The proposed protocol, capable of handling 820 Mbps of data, is more effective in protecting data after quantum computing. It can be used in real-time communication systems like government command systems and off-the-shelf systems with secure cloud knowledge, as the transmission latency is less than 5 ms in simulated cases. These results confirm that the suggested system achieves superior computational effectiveness and quantum equalization, with modifications and resource utilization scaled to realistic national levels.

Table 2. Comparative Performance Analysis of Classical, Post-Quantum, and Hybrid Cryptographic Protocols

Metric	RSA-3072	ECC-256	Kyber-1024	Proposed Hybrid Protocol
Key Generation Time (ms)	45.2	28.6	14.1	12.8
Encryption Time (ms)	9.4	7.8	6.2	6.6
Decryption Time (ms)	11.1	9.2	8.3	8.7
Public Key Size (KB)	0.38	0.09	1200	1050
Ciphertext Size (KB)	0.32	0.12	1100	950
Throughput (Mbps)	790	900	810	820

5.2. Qualitative Discussion

The experiment demonstrates that a hybrid cryptographic model with a lattice-based key exchange system and digital signature system, based on unhashing and a Merkle tree, offers high security value and good operational results. This model protects against Shor and Grover algorithms, ensuring quantum systems cannot attack it for extended periods. The proposed scheme minimizes storage and transmission overhead through vector arithmetic and polynomial compression techniques, maintaining cryptographic integrity.

The hybrid protocol was demonstrated to be operationally compatible by performing integration testing as part of TLS 1.3 and the IPSec VPN tunnels and compatible with existing Public Key Infrastructure (PKI) parts. The QR-CPS model demonstrated flawless compatibility with older encryption systems, enabling government networks to transition to quantum-safe without significant infrastructure changes or interruptions. The model achieves functional quantum resilience without compromising interoperability, scalability, or adherence to existing cybersecurity frameworks, without requiring significant infrastructure overhauls.

5.3. Policy and Implementation Implications

The effective execution and evaluation of the hybrid quantum-resilient protocol has major effects on national cybersecurity policy, the development of government standards, and the modernization of digital infrastructure. The findings indicate a viable migration strategy for national agencies to evolve from classical cryptography to quantum-safe designs. The hybrid idea would let

the company use its current ECC- and RSA-based systems during the migration period, which would lower operational risk and keep sensitive information safe at the same time.

The framework is in line with the current PQC standardization process that NIST is in charge of and meets the needs of the ETSI and ISO standards on quantum transition planning. This kind of compatibility will make sure that national systems that use the described method can still work with the international community and follow the new rules that are coming into effect after quantum computing. The QR-CPS framework improves the country's ability to defend itself against a group of enemies who are advanced in quantum technologies when it comes to cyber resilience. It protects the critical assets (such as government communications, defense command networks, finance systems) on cryptanalytic attack that would undermine national sovereignty.

To recap it all, the suggested hybrid cryptography suite provides a balanced combination of the strength of the security, scalability, and efficiency of operation, and, correspondingly, is a strategic basis of the future information security architecture of the nations in the quantum era.

6. Case Study / Application Example

In order to illustrate which practical idea the offered Quantum-Resilient Cryptographic Protocol Suite (QR-CPS) can practically be applied to, the detailed case study was carried out to test the implementation of ECS on the national level in the National Public Key Infrastructure (PKI). This application case cage depicts how the hybrid lattice-hash structure may be enmeshed with the current governmental setups to protect the interdepartmental communications, defense data exchanges, and diplomatic exchanges with quantum-capable adversarial plans. Another important point raised by the case study is the possibility of the stage-by-stage migration process and that legacy infrastructures can simultaneously be deployed with the post-quantum parts without losing all the functionality.

6.1. Deployment in a National PKI Framework

As demonstrated in this case study, a National Certificate Authority (NCA) has been developed as the root trust anchor whose duty is to issue and place in control digital credentials to government and governmental defense agencies. The architecture emulated a multi-level hierarchy of trust in which there was a Root CA, several Intermediate CAs and eight End-Entity CAs, which issues operation certificate to different agencies. They were initially based on the need to substitute conventional RSA- and ECC-based credentials with hybrid post-quantum certificates, which incorporate mechanisms of lattice-based key encapsulation and signatures using a hash approach. At the Root CA tier, subordinate certificate digital signatures based on a hash function were used, e.g. XMSS or SPHINCS+, where the integrity of the final signature is guaranteed by the long-term immutability and the form of post-quantum verification. The Intermediate CAs used lattice based tools (KEYM) to efficiently disseminate cryptographic keys to the subordinates at a safe distance basically, in lieu of the conventional RSA key exchanges. Lastly, the End-Entity CAs issued operational certificates which recognized both classical and post quantum public keys, and allowed hybrid validation and back-compatibility with the existing systems.

The implementation process is reflected by the creation of quantum-safe master keys and signing of intermediate CA credentials by the Root CA with the help of the hash-based scheme. These Intermediate CAs subsequently issued safe keys with lattice based KEMs, whereas the end entities, which include ministries, healthcare authorities as well as defense data centers, applied hybrid certificates within their operational areas. In this manner, gradual integration was possible without interfering with the legacy infrastructure or necessitating software restructuring. The results of doing this deployment proved to be a successful migration to quantum-safe credential management. The hybrid PKI architecture was fully compatible with other X.509 infrastructures and worked with both TLS 1.3 and IPsec (protocols). The performance benchmarks shown above showed that although quantum-resilient operations could be implemented at minimum degrading signing and verification times, it was possible to maintain efficiency without a focus on quantum-resilience, which allowed maintaining efficiency. In all these findings confirm that a national race towards cryptographic mass migration to post-quantum security can be achieved in stages, maintaining the operational continuity and the trust continuity between the governmental networks on multiple government networks.

6.2. Secure Communication Scenario

In order to further psychologically evaluate the relevance of the proposed structure, secure diplomatic communication network was modeled to test the efficiency of the proposed structure in real-time exchange of information. This network bridged various parties, such as foreign diplomatic stations, government defense laboratories and ministries via an encrypted-backbone system that utilized the intended Quantum-Resilient Virtual Private Network (QR-VPN). This was to examine how the system can be used to sustain high-performance, low-latency communication under workloads in post-quantum cryptographic applications. Within this approach emulated setting, diplomatic messages arrived at a secure level like encrypted military reports, legislative alliances as well as key intelligence briefs were passed on through a blend of ciphers. Lattice-based KEMs based on the Learning With Errors

(LWE) problem were used to generate session keys and establish them, as well as provide security in the presence of quantum adversaries. Authentication and integrity of the data were also ensured by the policy of having hash-based digital signatures which ensured message authenticity and non-repudiation amidst the distributed communication nodes. The QR-VPN also used hybrid TLS 1.3 handshakes, which is allowed to support both classical and quantum-resistant certificates as they can be verified and verification are performed during mutual authentication environments.

In the evaluation, it was found out that the success rate of the handshakes with various endpoint settings was 99.2% which spans legacy systems as well as PQC compatible systems. Latency wastes were at least 4.8 milliseconds less than in traditional TLS 1.3 calls, and the throughput stayed at 780 Mbps, which is fast enough to support real-time video conferencing, encrypted file transfers, and long-lasting multi-channel data communication between nodes in the US and around the world. From an operational point of view: In this situation, the outcome was that quantum-resilient communication can be achieved without sacrificing network performance or interoperability. The hybrid encryption system made it possible for the gradual integration the PQC technologies into modern communication channels. This way, even if quantum attacks were possible, it would still be possible to keep secret national and diplomatic communications safe.

7. Conclusion and Future Work

The study discusses the potential of a quantum-resilient cryptographic system for computer protection in the quantum age, connecting classical and post-quantum infrastructures and demonstrating safe and widespread use in government and defense systems. Over 200 attendees attended a meeting, with 80 employees receiving extensive training over eight months.

7.1. Summary of Design and Evaluation Outcomes

The study outlines the development, implementation, and evaluation of a Quantum-Resilient Cryptographic Protocol Suite (QR-CPS) to mitigate the risks of quantum computing for National Information Systems (NIS). The hybrid architecture, which is designed on the basis of lattice-based mechanisms of exchanging keys and hash-based signature, was designed in manner that it would be quantum resistant and compatible with the national PKI, VPN as well as secure communication architecture that currently exists.

Through experiment based analyses, the hybrid cryptographic suite has demonstrated some significant performances in terms of key generation and encryption efficiency, over classical RSA and ECC systems yet incurring low overhead in both ciphertext and key size. The security analysis was able to verify that it was resilience against classical and quantum adversarial models to confirm theoretical resilience to the Shor algorithm as well as the Grovers algorithm. Moreover, simulation experiments and production implementations demonstrated the feasibility of implementing PQC into the functioning government setup including nationwide certificate authority and safe diplomatic communications technology.

In sum, these findings attest to the expected extent of technical scaling, calculation and cryptographic soundness of the proposed framework and show that it can be used to form a national environment of migration to quantum-secure digital infrastructure.

7.2. Limitations and Future Research Directions

Although the findings prove the effectiveness of the framework, some limitations and avenues of further development have been observed. The computational overhead and key-size limitation of lattice-based and hash-based schemes is one important factor that should be taken into consideration. This study though gave parameter compression and parameter optimization strategies, the key sizes were still comparatively larger making a problem to low-bandwidth and a resource-strained environment. We will look into hardware acceleration that uses FPGA and ASIC implementations, as well as lighter alternatives to PQC and how it can be improved to work with the IoT or other edge cases.

Another promising direction is the combination of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). PQC is strong in math, while QKD is strong in physics, based on the laws of quantum mechanics. Combining these two ways of thinking could lead to the development of end-to-end quantum-secure ways to communicate, which could be very useful in important fields like defense and energy.

Moreover, subsequent research should concentrate on the formal verification and certification of PQC protocols within the adaptive framework of quantum threats. Using formal sets of proofs will boost confidence and meet the needs of NIST PQC Round 4 and ISO/ETSI standards. Lastly, policy-sensitive cryptographic agility (with AI-enhanced threat intelligence) will let protocols be shut down quickly in response to both new cryptographic risks and algorithms that are no longer useful.

7.3. Recommendations for National Policy and Strategic Adoption

The move toward quantum evidence of cryptography went beyond a technical level; it was also a requirement for the national cybersecurity strategy. To make the migration process more organized or get ready for the future, the work gives the country a number of suggestions. First, we need to set up a National PQC Readiness Framework. This must include staged implementation schedules that follow the international standards set by NIST and ETSI. This will ensure that modernization continues in the government, military, and critical infrastructure. Second, the modernization of cryptographic infrastructure should be on the list. This includes updating the national PKI ecosystems, VPN infrastructure, and secure communication backbones to make it easier to use during the transition to hybrid PQCs.

Another possible solution is to create a partnership between the state and the business world to get universities, cybersecurity startups, and government labs to run large-scale PQC pilot programs. These steps will make sure that interoperability exists, speed up the process of standardization, and get people in the country thinking about quantum-safe technologies. National agencies also need to spend money on quantum security training and hiring more people, as well as create programs to help cybersecurity professionals learn more about how to design and implement PQC and make sure it is compliant. Finally, there need to be audit measures or rules that would keep PQC adoption in check. The framework of certification should ensure that implementations meet the necessary standards for cryptographic strength, interoperability, and algorithmic flexibility, enabling abstract evaluation and accountability across the entire public sector.

7.4. Concluding Remarks

In conclusion, this paper illustrates that quantum-resistant cryptography is not merely a theoretical framework for safeguarding national information systems, but a tangible and urgent advancement towards that objective. The proposed hybrid protocol system effectively tackles security, performance efficiency, and deployment capabilities, which will facilitate the establishment of strong digital trust in the post-quantum era. As quantum computing continues to advance, nations must invest in decisive measures to ensure the longevity of their cybersecurity systems. The findings of this study demonstrate that a proactive deployment of hybrid post-quantum cryptographic solutions, supported by a robust national policy and collaborative research and development, can mitigate the risks posed by quantum threats without compromising operational usability.

Through the integration of technological breakthrough with future governance, governments will be able to provide long-term data sovereignty, data integrity and national resiliency in the new quantum information era. The suggested framework is consequently both a technical platform as well as an overarching blueprint towards ensuring the digital future of the national as well as the critical infrastructures.

Reference

[1] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.

[2] Stelzer, T., Oberhansl, F., Schupp, J., & Karl, P. (2023, November). Enabling lattice-based post-quantum cryptography on the opentitan platform. In Proceedings of the 2023 Workshop on Attacks and Solutions in Hardware Security (pp. 51-60).

[3] Lei, D., He, D., Peng, C., Luo, M., Liu, Z., & Huang, X. (2023). Faster implementation of ideal lattice-based cryptography using avx512. ACM Transactions on Embedded Computing Systems, 22(5), 1-18.

[4] Lovic, V. (2020). Quantum key distribution: Advantages, challenges and policy.

[5] Lee, C. C., Tan, T. G., Sharma, V., & Zhou, J. (2021, June). Quantum computing threat modelling on a generic cps setup. In International Conference on Applied Cryptography and Network Security (pp. 171-190). Cham: Springer International Publishing.

[6] Tan¹, T. G., & Sharma, V. (2021, July). Quantum Computing Threat Modelling. In Applied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21–24, 2021, Proceedings (Vol. 12809, p. 171). Springer Nature.

[7] Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. Security and Privacy, 5(2), e200.

[8] Giron, A. A. (2023). Hybrid post-quantum cryptography in network protocols.

[9] Aladwani, A. M. (2002). An integrated performance model information systems projects. Journal of management information systems, 19(1), 185-210.

[10] Panetto, H., & Cecil, J. (2013). Information systems for enterprise integration, interoperability and networking: theory and applications. Enterprise Information Systems, 7(1), 1-6.

[11] Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[12] Farooq, S., Altaf, A., Iqbal, F., Thompson, E. B., Vargas, D. L. R., Díez, I. D. L. T., & Ashraf, I. (2023). Resilience optimization of post-quantum cryptography key encapsulation algorithms. Sensors, 23(12), 5379.

[13] Halak, B., Yilmaz, Y., & Shiu, D. (2022). Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. Ieee Access, 10, 76707-76719.

[14] Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. IEEE Access, 8, 142413-142422.

[15] Public-Key Cryptography — J. R. Nechvatal. NIST Special Publication SP 800-2, April 1991.

[16] Chen, L., Jordan, S., Liu, Y-K., Moody, D., Peralta, R., Perlner, R. & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography.* NISTIR 8105, National Institute of Standards and Technology.

[17] Basu, K., Soni, D., Nabeel, M., & Karri, R. (2019). *NIST Post-Quantum Cryptography – A Hardware Evaluation Study.* Cryptology ePrint Archive 2019/047.

[18] Hekkala, J., Muurman, M., Halunen, K., et al. (2023). *Implementing Post-quantum Cryptography for Developers.* SN Computer Science, 4, 365.

[19] Akter, M. S. (2023). *Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions.*

[20] New Directions in Cryptography — W. Diffie & M. E. Hellman. *IEEE Transactions on Information Theory*, Vol. 22, No.6, Nov 1976, pp 644-654.

[21] A Method for Obtaining Digital Signatures and Public-Key Cryptosystems — R. L. Rivest, A. Shamir & L. Adleman. *Communications of the ACM*, Vol 21(2), Feb 1978, pp 120-126.