IJCSIT
International Journal of Computer Science & Information Technology
ISSN: XXXX-XXXX / Volume 1 Issue 2 April-June 2025 / Page No: 14-24
Paper Id: IJCSIT-V1I2P103

Original Article

Post-Quantum Cryptography Algorithms and Implementation Challenges

Erdwin Owuma Ngwawe[1], Tsitsi Zengeya[2]

[1,2]Department of Computer Science,National University of Science and Technology, zimbabwe.

Received Date: 07 February 2025 Revised Date: 09 March 2025 Accepted Date: 07 April 2025

***Abstract**: Quantum computer poses a very high threat to the current cryptographic measures we are practicing to protect our digital infrastructure. In particular, the best known public-key algorithms (such as RSA for encryption, and ECDSA for digital signatures), are broken by a quantum computer using Shor's algorithm. But quantum algorithms like Shor's algorithm don't care. This security grows even worse as quantum computing advances. Yet, we need to find cryptography which does not get broken out-of-the-box when quantum computers arrive. Post-Quantum Cryptography (PQC) is encryption that can use quantum, but it must be secure against the attack of a quantum computer and also must be safe with classical computer. This study is a significant contribution to broaching the algorithmic frameworks used in Post-Quantum Cryptography (PQC), including lattice-based, code based, multivariate and hash-based methods.*

***Keywords:** Case Studies, Commercial Enclaves, Energy Efficiency And Sustainability Cryptographic Security Key Exchange Digital Signatures Lattice-Based Cryptography Quantum Computing Post-Quantum Cryptography Cryptographic Algorithms.*

I. INTRODUCTION

In these days, the cryptography systems are very essential in saving the communications from arbitrating, protecting your privacy and trust in online transactions. These are the modern encryption methods that form part of this digital infrastructure. -- These are the algorithms that check online banking is secure and that no one can listen into military communications. Public key systems are implemented to secure information in many different ways, two of which are RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography). These systems provide for a parity distributed burden contingent upon how convoluted certain mathematical issues and are totally open-source in nature. To explain, RSA is based on factoring large integers and elliptic curve cryptography (ECC) on discrete logarithms over an elliptic curve. These are problems that, classically, we cannot solve in a reasonable time, as computationally inconceivable to classical computers, therefore preserving the security of foundational cryptographic techniques.

By definition, this underlying assumption is true; however, the rate of change in quantum computing is so accelerated that their efforts have instantly turned into a rearview mirror exercise. Computers That Use the Rules of Quantum Mechanics to Do Math: Quantum computers do math using qubits (quantum bits) and concepts as superposition or entanglement. This is not to be confused with binary data as used in classic computers. These characteristics is what makes quantum computers orders of magnitude faster than classical computers for certain types of problems. Shor's Algorithm was introduced in 1994. It can factor integers and compute discrete logarithms faster than coppersmith algorithm This suggests RSA, DSA and ECC could be broken relatively easily with a powerful quantum computer. Among secure communication protocols could be named SSL/TLS, PGP, or even blockchain. Here are only some of the most important pieces in those sets of rules.

The danger that quantum attacks might be used in opposition to current encryption structures is increasing. Progress is swift in quantum hardware and error correction, but there are no large quantum computers that we can use to break today's encryption methods. Many experts say they could make it a reality — at least in the next 20 to 30 years. Digital systems, including those used by the government and healthcare sectors, as well as critical infrastructure need to remain secure for a very long time so transition to quantum resilient alternatives needs to start immediately.

This research leans toward the field of post-quantum cryptography (PQC)— cryptographic designs that are secure against both classical and quantum attacks. This is meant to be a detailed study of all the base PQC types: — hash based, code based, multivariate and lattice based frameworks etc. It also discusses the problems that arise when attempting to use these algorithms in practical systems, including key sizes, performance, compatibility and protection from side-channel attacks. These are the concepts we must understand if we are going to make a world resilient against quantum threats.

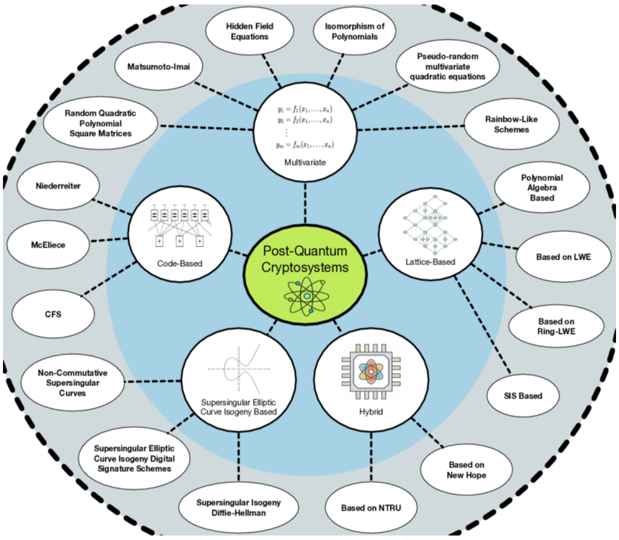
Hidden Field Equations
Isomorphism of Polynomials
Matsumoto-Imai
Pseudo-random multivariate quadratic equations
Random Quadratic Polynomial Square Matrices
$y_1 = f_1(x_1,\ldots,x_n)$
$y_2 = f_2(x_1,\ldots,x_n)$
$\vdots$
$y_m = f_m(x_1,\ldots,x_n)$
Multivariate
Rainbow-Like Schemes
Niederreiter
Polynomial Algebra Based
McEliece
Code-Based
Post-Quantum Cryptosystems
Lattice-Based
Based on LWE
CFS
Based on Ring-LWE
Non-Commutative Supersingular Curves
Supersingular Elliptic Curve Isogeny Based
Hybrid
SIS Based
Supersingular Elliptic Curve Isogeny Digital Signature Schemes
Based on New Hope
Supersingular Isogeny Diffie-Hellman
Based on NTRU

Figure 1: Most Relevant Types and Implementations of Post-Quantum Public-Key Cryptosystems and Digital Signature Schemes

II. CLASSICAL CRYPTO AND THE QUANTUM THREAT

RSA (Rivest–Shamir–Adleman) is one of the most widely used public-key cryptographic systems, relying on the mathematical difficulty of factoring large prime numbers. It has long been a cornerstone of secure communication, powering email encryption, digital signatures, and web authentication. Today, RSA typically employs 2048- or 3072-bit keys to ensure security. However, the arrival of quantum computing poses a significant threat to RSA and similar systems. Elliptic Curve Cryptography (ECC), which is more efficient than RSA due to its use of elliptic curve point multiplication and the discrete logarithm problem, offers strong security with smaller keys—making it ideal for constrained environments like mobile and IoT devices. DSA (Digital Signature Algorithm), another prominent public-key method, relies on discrete logarithms and is used widely for secure software verification and email signing. Yet, like RSA and ECC, DSA is vulnerable to quantum algorithms such as Shor's.

Shor's algorithm represents a major quantum threat, as it can efficiently factor large integers and compute discrete logarithms—rendering RSA, ECC, and DSA obsolete in the face of a sufficiently powerful quantum computer. Grover's algorithm, while less devastating, still offers a quadratic speed-up against symmetric encryption, effectively halving the effective key size. For example, Grover reduces AES-256's security to that of AES-128, meaning symmetric systems will need to double key lengths or otherwise harden to maintain the same level of protection. The quantum threat is not only future-facing; adversaries may already be harvesting encrypted data with the intent to decrypt it once quantum capabilities become practical—a dangerous "store now, decrypt later" threat model that elevates immediate risk, especially in sensitive sectors like government or healthcare.

The broader infrastructure implications of quantum computing are severe. Protocols such as HTTPS, VPNs, and digital signatures—all reliant on RSA and ECC—would become ineffective, jeopardizing global cybersecurity. With quantum machines capable of reducing years of cryptanalysis to hours, traditional cryptography could collapse swiftly and entirely. Symmetric encryption methods like AES and hash functions like SHA-2 show more resilience but still require adjustments to remain secure in a quantum era. In response to this looming crisis, the global cryptographic community has pivoted toward the development and standardization of post-quantum cryptography (PQC)—algorithms designed to resist both classical and quantum attacks.

Post-quantum cryptographic algorithms are built on hard mathematical problems not yet efficiently solvable by quantum algorithms like Shor's or Grover's. Among the most promising families is lattice-based cryptography, which relies on problems like Learning With Errors (LWE) and Shortest Vector Problem (SVP). Algorithms such as Kyber (for key encapsulation) and Dilithium (for digital signatures) are leading contenders, offering robust security and efficient implementation, though with larger key and ciphertext sizes. Code-based cryptography, exemplified by McEliece encryption, has shown decades of resilience but is challenged by enormous key sizes. Multivariate polynomial cryptography—once promising due to its speed—has seen key candidates like Rainbow fall to cryptanalysis. Hash-based signature schemes like SPHINCS+ and XMSS offer strong post-quantum security with minimal assumptions but are hindered by large signature sizes and implementation complexity.

The National Institute of Standards and Technology (NIST) initiated the PQC standardization process in 2016, driving a competitive and transparent effort to evaluate and endorse quantum-resistant cryptographic algorithms. Through multiple rounds of scrutiny, performance testing, and academic analysis, NIST selected a first set of finalists in July 2022: Kyber for encryption, and Dilithium, Falcon, and SPHINCS+ for digital signatures. These selections balanced performance, key sizes, security assumptions, and implementation feasibility. The standardization process continues, seeking a diverse suite of algorithms based on different mathematical foundations to mitigate unknown vulnerabilities. This ongoing effort is essential to ensuring a smooth and secure transition to a post-quantum future where cryptography can withstand the immense power of quantum adversaries.

III. IMPLEMENTATION CHALLENGES IN POST-QUANTUM CRYPTOGRAPHY

Challenge	Description	Impact	Mitigation Strategies
Large Key and Signature Sizes	Many PQC algorithms (e.g., McEliece, Dilithium) use large keys and ciphertexts, often several kilobytes in size.	Difficult to implement on IoT, embedded devices; increases bandwidth and storage overhead.	Use algorithms with smaller parameters (e.g., Kyber); apply data compression where feasible.
Performance Overhead	PQC schemes may be slower or require more memory and CPU cycles than RSA or ECC, especially without hardware acceleration.	Latency in real-time applications; more power and CPU consumption in constrained devices.	Use AVX2, SIMD, FPGA, or GPU acceleration; optimize software implementations.
Integration with Existing Protocols	TLS, SSH, and other protocols are built for classical crypto and may not support new PQC schemes natively.	Incompatibility with legacy systems; risk of deployment delays or failure.	Employ hybrid cryptography; update protocol standards (e.g., TLS 1.3 with PQC support).

Secure algorithms are much easier to aim for Post-Quantum Security. Developers have to fix all these problems at the system level with nearby-commodity protocols that work together using as little resources and clean maintainable cryptography. Business can then prepare for a secured transition to the post-quantum world by identifying and rectifying these traceability issues early on.

III. SOFTWARE AND HARDWARE IMPLEMENTATIONS

A. Open-Source Software Libraries

There is good reason why there are many open-source post-quantum cryptography tools available for anyone to explore, read, and contribute. The Open Quantum Safe (OQS) project is probably the most popular one. It makes the liboqs library. Liboqs is a C-based library that provides implementations for many of the algorithms that NIST has either selected or is considering. It is fully compatible with modern cryptographic libraries like OpenSSL, so that developers can use and deploy their post-quantum proposals in applications they are used to.

PQClean is a separate large codebase written to create clean, portable, and extractably verifiable versions of various post-quantum algorithms—many of which were NIST PQC standardization candidates. Simple and correct is the dream of anyone wishing to audit, formally verify or study in academia using PQClean.

B. Real-World Software Integration

The libraries serve more than just for school. People use them to benchmark stuff, merge protocols, test on interoperablily et al in real world. Such protocols like TLS and SSH allow researchers and system admins to test performance, overhead as well usability under real-world conditions. As well, they are providing people enormous toolkit for using both archaic (traditional) and modern methodologies for testing hybrid solutions.

C. Hardware Implementations

Software libraries can be capable of such but to speed things up and use way less power, especially in small places you are going to need this sort of hardware-accelerated approach. Some PQC schemes, particularly lattice-based algorithms such as Kyber and Dilithium, are starting to be implemented in FPGA (Field-Programmable Gate Array) or ASIC (Application-Specific Integrated Circuit) form by researchers and engineers. Hardware implementations can reduce latency (and in many cases power use) by orders of magnitude, and hence are particularly well-suited for portable or rapid systems.

D. Security in Hardware Designs

Solid hardware solutions for where things can be improved but there is a big question about keeping things secure. A side-channel approach could target PQC processes with power analysis, electromagnetic leakage or timing attacks. Safe hardware designs have things like constant-time execution, signal masking and noise injection to keep people safe. These improvements are incredibly important for practical applications of PQC in e.g. smart cards, mobile devices and embedded control systems.

E. Embeded Systems in IOTs and PQC

This can cause problems using PQC on embedded systems, IoT devices etc. These devices generally have limited memory, CPU and battery resources - meaning they can't support very large keys or resource-intensive processing. To address this, engineers are working on low-footprint variants as well as lightweight hardware modules that can work with such devices without compromising cryptographic capabilities.

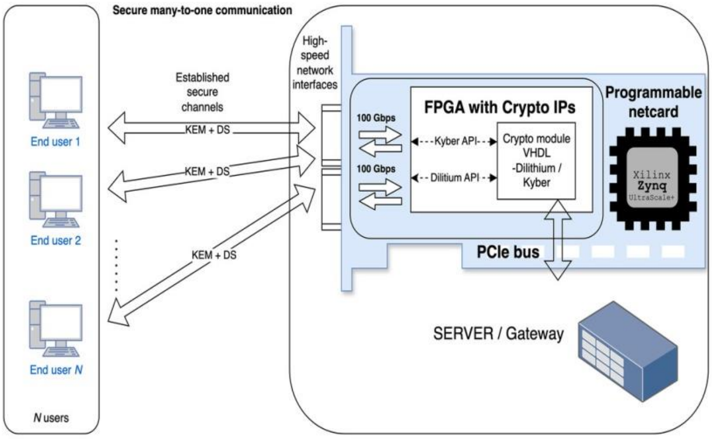

Figure 2 : FPGA-Based PQC Controller for Embedded Systems

IV. REAL-WORLD APPLICATIONS

However, PQC is no longer only a theoretical requirement but also a class of technology that it is being seeded and fielded. Experimental Deployments by a Few Organizations such as Google and Cloudflare of PQC-Ready TLS The results also show that secure internet communications using PQC will soon be possible. VPN: Have also been employing PQC Secure Email and File Transfer protocols ups and downs LIRE. In the case of digital signatures, which are necessary for software deployment and verification to prove the authenticity of a document, these will also need to change to quantum-safe methods in order to be valid over the long-term. Unfortunately, in the blockchain world (which is quite a special world), content on cryptos and smart contracts are common which often need elliptic curve cryptography never mind post-quantum.

This challenge becomes much more evident for the Internet Of Things (IoT) involving billions of interconnected devices with limited computation power. Devices have to be provided with an upgrade suitable for lightweight PQC schemes such as Kyber512 in order to maintain a balance between performance and security. There is interest in the broader automotive and healthcare sectors to utilize PQC to protect embedded systems, medical devices, and vehicle-to-infrastructure communications.

Preparing for post-quantum cryptography (PQC) is a nuanced and multi-stage process that requires significant planning, testing, and standardization. Since most of the cryptography that is widely integrated in today's systems is conventional, an immediate and extensive migration to post-quantum schemes is unfeasible. Hybrid cryptography — a popular method used to bridge the gap during this transition is hybrid cryptography, which joins quantum-resistant versions of classical cryptographic algorithms like RSA or ECC as alternatives in the same protocol (or applications). Hybrid schemes work on the basis of layered security such that even when a quantum adversary breaks one algorithm,usually classical, then based on their capability there is whole another (quantum-safe) here which ensures to keep the confidential and authenticity of communication intact.

Among the first proof-of-concept implementations of hybrid cryptography was Google's CECPQ2 experiment, where a lattice-based post-quantum algorithm (HRSS) was integrated with X25519 key exchange in TLS 1.3. We deployed our setup to a subset of Chrome browsers and Google servers to evaluate real-word performance, compatibility, and stability of hybrid key exchanges. And it was a successful one--one that, if anything, encouraged the use of such hybrid approaches on a larger scale. Today the hybrid key exchange is getting attention to be used in more general protocols (like TLS, SSH, IPsec or secure messaging platforms) which are required to have very strong forward secrecy and long-term confidentiality.

On the other hand, hybrid cryptography is more secure, but adds helpful layers of complexity. E.g., it enlarges the key exchange, certificate chain, and handshake messages, etc. which might result in scalability issues especially for bandwidth-limited or latency-sensitive environments. This increased computational overhead as well as the overhead of transmitting data affects mobile applications, real-time communications, and IoT systems. Developers have to walk a fine line between the advantages of hybridization and the performance penalties this imposes. While compression techniques, efficient protocol design or selective hybridization (only during initial key exchange for instance) might provide adequate mitigations in some use cases.

As if this were not enough, interoperability is a great worry. Hybrid schemes are not always supported by legacy systems, and the integration of classical with post-quantum parts needs to be handled backward-compatible and transparent. Its presence of multiple cryptographic primitives (if not well designed and standardized and audited) could cause unexpected security vulnerabilities such as multiple key validation issues or even signature mismatching. Best practices for secure hybrid integration will evolve along with the standards that are emerging around these principles; organisations should stay in line with guidelines coalescing across standardisation bodies such as NIST, ETSI and IETF interested in creating seamless, non-disruptive protocol paths to a migration path benefiting state-of-the-art lessons provided by all leading cloud providers.

Besides the technical improvements, the PQC video presented Organizational Readiness: evaluating infrastructure for potential challenges with cryptography, teaching security staff about PQC, and standing up testbeds to test hybrid implementations in real-world scenarios. BoringSSL, OpenSSL and liboqs are open-source libraries that can now be used to create hybrid configurations, allowing early adopters to test compatibility with the implementations and transition their production stacks to different or multiple post-quantum algorithms. In summary, hybrid cryptography is not just the path to post quantum but a mature security model on its own that enables organizations to prepare their communications for the future while avoiding wholesale disruption today. The transition can only be met with success through broad cooperation of academia, industry and government in concert defining interoperable, secure and efficient hybrid solutions.

At a foundational level, the security of these post-quantum cryptographic (PQC) algorithms is based on the presumed difficulty of certain mathematical problems that are thought to be both computationally intractable for classical computers and quantum computers. Among them, lattice-based cryptography (especially those based on the Learning With Errors and Module-LWE problems) has taken the lead. These problems are widely believed to be at least as hard for quantum adversaries, and have survived intense scrutiny during the NIST standardization process. These are the foundations that schemes like Kyber and Dilithium build upon, and while no practical quantum attacks have been shown yet, the long-term security of these schemes depends on further cryptanalysis and better understanding of what quantum systems are capable of.

Another contender is code-based cryptography, of which the McEliece encryption scheme is one well-studied example. McEliece is a classic that has been around for four decades and has not yet succumbed to crushing attempts of cryptanalysis. This longevity adds some gravity to the claim, given that the underlying problem, decoding random linear codes, is known to be NP-hard. Code-based schemes are practical to deploy, but their limitations such as too large public key size (more than several hundred kilobytes) make them not suitable for many real-world applications due to storage and transmission issues.

SPHINCS+ and XMSS are hash-based signature schemes that are provably secure in the random oracle model. Such schemes are not based on hard algebraic problems and provide black-box proofs in the standard model, provided that the used hash function is secure. They are limited only in terms of performance and signature size requirements, but not at a foundational security level.

In summary, Final Thoughts though these PQC schemes seem to have reasonable security profiles, they are still in the early stages of development. As powerful as it may be, data centers greater than a few hundred qubits remain firmly in the future and much remains to be done to move from carefully crafted small demonstrations on exacting silicon chips in cryogenic environments into one that can operate at scale. alpha-1.constantcontact I believe we need continuous analysis, real-world testing for putative ultralarge quantum computers prior to certification and vigilance in monitoring new quantum algorithm developments if confidence in post-quantum era cryptographic standards is to be maintained.

V. LEGAL, POLICY, AND REGULATORY CONSIDERATIONS

Any wider adoption of the technology is likely to be delayed by a raft of legal, policy and regulatory challenges. National and international regulators are making PQC law enforcement the exact same for all critical business and infrastructure networks. The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) was produced by the United States National Security Agency (NSA). That would require those national security systems to be using post-quantum secure algorithms by the mid-2030s. Funded through the National Institute of Standards and Technology (NIST), this project on global PQC standards. The norm for policy frameworks in the US and many other countries

We particularly get comments from people in the PQC space, The European Union Agency for Cybersecurity (ENISA) and spoken to them about how important quantum is, and they are working a lot on how to secure this [...]. Japanese CRYPTREC project is also investigating on whether and how safely the performance of PQC systems can be measured The powers that be, are concerned about more than just technical problems. They are even crafting legislation, regulations to enforce it, and risk management strategies in order to be prepared for a post-quantum future.

If you are writing rules, consider IP Cyprer rights — even more so in this day and age. Patents guard several of the alternate versions to the PQC algorithm, which may render them more difficult to come by and also more expensive if adopted especially for individuals in groups with a low budget or open-source programmes. If that is the case, it is no wonder so many strive to obtain algorithms that are royalty-free and open-licensed. These can be more effectively implemented as standard and are also easier to be used by people around the world. Increasingly, governments and standards bodies are mandating cryptographic algorithms. They want them open, inter-operable, and unambiguous in law. This is to ensure that during the long term both the public and private sectors benefitted from algorithms.

In the process, coordination among governments, industry and academia would be necessary to effectively and safely navigate the legal and regulatory landscape of PQC adoption.

In order for PQC to be secure and legal, governments, companies and universities have had to work together.

Reduce The Key, Ciphertext, and Signature Sizes as Much as Possible While Maintaining Security. Ensure your ideas work well in extremely low-power devices (e.g. RFID, IoT sensors, or low-power embedded systems).

You need to develop the capability for changing or using different PQC algorithms, even older ones, as well and you must be able to do this without much trouble if the situation demands a less quantum secure algorithm or another threat model, i.e. more speed (NTRUEncrypt folds in 7 other fields) or specific field characteristics because of size restrictions like LWE needs. It will allow things to progress when new information becomes available.

Building & Evaluating Post-Quantum Homomorphic Encryption, Private Set Intersection, Secure Multi-Party Computation: Create and evaluate versions of homomorphic encryption (HE), secure multiparty computing (MPC) and private set intersection that are resistant to attacks by quantum computers.

Quantum-Safe Zero-Knowledge Proofs: Implement concise proofs based on post-quantum research (in the fashion of SNARK or STARK) which are zero-knowledge. It even enables decentralized ID systems, verifiable computation, and safe data authentication.

Quantum Digital Identity and Authentication→PQC primitives to build decentralize/federate identity networks and ledger credentials (signature, key exchange, revocation). This will allow the Trust Anchors to remain healthy for an extended period of time.

Secure and Auditable Firmware & Software Updates: Discover ways of code signing and patch dissemination which are secure against quantum adversaries, as well as maintain their validity and integrity over the long-haul. And the fact that a piece of equipment as simple as a blood test reader is completely unsafe because attackers can control the device to get alerts sent directly from your body ("harvest now, decrypt later") is just one example.

New Networks (6G for example) : Learn how to embed PQC in future communication protocols, like 6G requires security solutions which work well together because latency is very low, connections are numerous and edge intelligence done on them.

Investing in Change — Blockchain and Cross-Ledger Interoperability: This article Address the question "how would quantum computing shape future distributed ledger technologies." Include quantum-safe consensus, wallets and keys, and atomic swaps between different blockchains.

See the by-effectiveness you can get with PQC — or initiate QKD deployments for layered systems that use both information-theoretic and computational quantum resistance in a variety of deployment scenarios. This technique is called Quantum Key Distribution (QKD) hybridization.

Improve Co-Optimized Implementations: Develop better and more cryptographically secure co-optimized implementations targeting the trade-off curve between cryptographic security and physical limits – e.g., side-channel resistance, energy-efficiency, quality random numbers generation on ASIC/FPGAs.

Automatic Verification and Formals: Develop formal verification toolchains, to generate automated proofs for PQC implementations to minimize human mistakes, keep them in the right state always, and ensure they are protected against implementation attacks of certain kinds.

Study of Entropy and Randomness: Develop methods for capturing, conditioning, and quantifying entropy that are more secure and reliable in the presence of quantum attacks. This is because the primitives used in PQC generally require much higher-quality randomness to generate keys and obscure data.

Migration and Lifecycle Management Models - Build good transitioning tools with deprecation pathways, key rotation procedures, and risk assessments to aid firms transitioning from classical to post-quantum systems.

Future Resilience Against Quantum Advances - Periodically revisit core hardness assumptions to ensure they are prepared for any unexpected quantum breakthroughs, as well as incorporate diversity to mitigate potential risks from new trends in cataclysmic cryptanalysis.

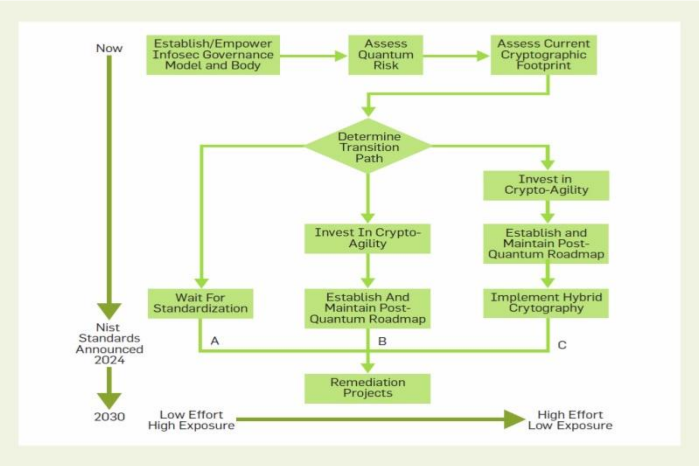
Now
Establish/Empower Infosec Governance Model and Body
Assess Quantum Risk
Assess Current Cryptographic Footprint
Determine Transition Path
Invest in Crypto-Agility
Invest In Crypto-Agility
Establish and Maintain Post-Quantum Roadmap
Wait For Standardization
Establish And Maintain Post-Quantum Roadmap
Implement Hybrid Crytography
Nist Standards Announced 2024
A
B
C
Remediation Projects
2030
Low Effort High Exposure
High Effort Low Exposure

Figure 3 : Organizational Pqc Assessment & Mitigation Flowchart

VI. A BRIEF GUIDE THROUGH THE POTENTIAL QUANTUM DOOM OF TRADITIONAL CRYPTOSYSTEMS

Some might say that quantum computing is an existential threat to traditional cryptographic systems, especially considering the essential role played by RSA, ECC and DSA for global digital security. These algorithms are based on mathematical problems (e.g., integer factorization and discrete logarithms) that—in contrast to calculations of classical computers —requires an immense amount of work. On the other hand, Shor´s algorithm, a quantum algorithm presented in the 1990s can address these problems from an exponential point of view and therefore would break current encryption methods. There is an increased urgency for quantum-resistant or enhanced cryptographic systems as quantum computing transitions from conceptual to practical. Public-key cryptosystems are completely exposed to quantum threats, while symmetric algorithms remain partially resilient through adjustments (e.g., key-size doubling). In practical sense, this could compromise a huge number of things, ultimately all the way from secure web browsing (HTTPS), over digital signatures and VPNs to encrypted-email or blockchain-transactions. This poses an even greater threat with what's known as a "harvest now, decrypt later" scenario where adversaries can obtain encrypted data today and expect to be able to break it open in the future when quantum hardware matures. That is why there will be a need to move towards new cryptographic methods which are able to withstand quantum (or post-quantum) attacks. These PQC algorithms are created using lattice-based, hash-based, code-based, and multivariate polynomial mathematic problems that are anticipated to be secure enough for the quantum era. They include a group of algorithms that NIST recently standardized, based on their strong performance and quantum- and classical-computer security – for example key encapsulation with Kyber and digital signatures with Dilithium. This is not a straightforward operation, and it is more than the exchange of one system for another; it requires complex developments in both software and hardware, but also legislative adjustments and general public know-how. The US Government (among others globally) is already planning for a post-quantum future with NSA’s CNSA 2.0 and NIST’s PQC project, so public and private sectors need to start this migration. The quantum threat has, in other words, obtained a status less of an academic fear than as a pending deadline, and hesitation poses a severe risk to critical data and systems. Not adopting PQC today is a concerning proposition -- both in terms of current security and forward-looking infrastructure investments that will need to be operational for many decades.

VII. HOW TO HANDLE THE PERFORMANCE AND COMPATIBILITY ISSUES

On one hand, we have the obvious need for post-quantum cryptography (PQC) but actually implementing and managing a set of these algorithms is fraught with significant technical challenges on all levels. Large keys and signatures in many PQC schemes are one of the biggest challenges. For example,... McEliece system based on codes is securely quantum-resistant but has public keys of a few hundred kilobytes, making it impractical for resource-restricted storage and bandwidth devices. Likewise, the authors observed that although lattice-based schemes like Kyber and Dilithium are less expensive in terms of communication, they require even larger amounts of memory and computational power compared to traditional systems like RSA or ECC. This is particularly problematic for embedded systems, IoT devices, etc, which must universally ignore calculations due to the restriction of computational resources within those low power environments. Another impediment is performance—PQC algorithms are usually more CPU/memory-intensive affecting realtime application latency/throughput. Current mitigations include hardware acceleration using AVX2, and efforts are underway to integrate with FGPAs and GPUs; however, these options require extensive investment in reengineering for wide deployment. We also face the challenge of compatibility with existing protocols. Secure communication protocols like TLS and SSH which are building blocks of the internet have not incorporated post quantum primitives. Hybrid Cryptography: an Antidote to Post-Quantum Crises — or Just a Painkiller? Hybrid cryptography, in which two algorithms (one from classical and one from PQC) work together, is aimed at this interim solution. This enables us to establish secure communication channels while remaining backwards-compatible with older systems. This pattern has been vindicated by things like CECPQ2, the hybrid key exchange that Google shipped in both Chrome and their servers. That being said, hybrid schemes are not without their own problems: they often bloat message sizes, overcomplicate the handshake process and introduce additional protocol overhead that could have a performance cost. Developers also need to protect against a number of side-channel attacks, such as power analysis or timing attacks that could defeat even quantum-safe algorithms if not adequately mitigated. Liboqs and PQClean are open-source tools that provide clean, testable implementations of PQC algorithms, which can be used in benchmarking. Most of these libraries are crunching numbers for PQC benchmarking and assessing the feasibility to deploy them within real systems. In sum, the PQC provides a strong theoretical accouterment for ensuring data in the quantum age, but practical realization will require solutions to several circuitous puzzles in software, hardware and protocol design. It needs cryptographers, developers, and a collective international agreement on creating an undeniable cryptographic future.

VIII. FROM THEORY TO PRACTICE — REAL-WORLD INTEGRATION OF POST QUANTUM CRYPTOGRAPHY IN CRITICAL INFRASTRUCTURE

Real-world systems are in the process of transitioning from theoretical resilience to practical implementation by integrating post-quantum cryptography (PQC). Quantum computing has pushed the envelop of traditional encryption as quantum capabilities come ever closer to breaking basic cryptographic. Many industries, including healthcare, finance, telecommunications and defense are racing to deploy new post-quantum cryptographic toolkits that can provide a safe and secure path to adapt in a rapidly changing data security landscape. Several major technology companies—including Google, Microsoft, and Cloudflare—have placed early bets on running pilot programs to assess the performance of PQC algorithms in production contexts, notably, within the TLS protocol for secure internet communication. While these early deployments are proving that PQC is feasible, they also showcase the challenges of real-world adoption. For example, enabling PQC in embedded systems like IoT devices and smart medical implants involves different constraints because of limitations which are due to hardware and energy efficiency. Engineers are creating lightweight versions and slim hardware modules that will solve that without involving risks in the security aspect. Vehicle-to-everything (V2X) communications in automotive systems and avionics are being investigated to ensure that sensitive data and control signals are not at risk from these coming quantum threats. Even the healthcare system is now trying out PQC for medical data transmission, patient records and connected devices. But real-world integration is not only about industry alone. Governments, and military infrastructures in particular, are beginning to employ PQC protocols which tended to use hybrid cryptographic schemes with the outright switchovers of public-key schemes affixed by these entities. Open-source cryptographic libraries such as BoringSSL, OpenSSL and liboqs are key to this work, allowing the team to prototyping quickly, test interoperability and prepare for deployment. Yet, the co-ordination must also encompass legal/regulatory and economic considerations as well. Most PQC algorithms are patented, so open-licensed alternatives need to be fostered for them to see adoption on a large scale. Secondly, while the cryptographic landscape changes physical policy frameworks must not be allowed to go out of date. To avoid these risks, regulatory bodies in regions like NIST, ETSI or ENISA are already developing standards and best practices to allow for a smooth and secure transition. PQC cannot just be dropped into place; it has to be implemented, tested and kept updated with contributions from an interdisciplinary team. Instead, developers need to be aware of interoperability challenges, user experience degradation, update-cycle lag and system strain if safeguar:s are not implemented properly into the wider landscape of a cloud-native context. In addition to finding the correct cryptographic algorithm (exactly how is still up in the air), post-quantum cryptography will also need to be supported across legacy infrastructures, which will complicate things. With collaborative effort, PQC implemented as part of the very infrastructure of our digital world securing communications, safeguarding identities and preserving trust for future generations.

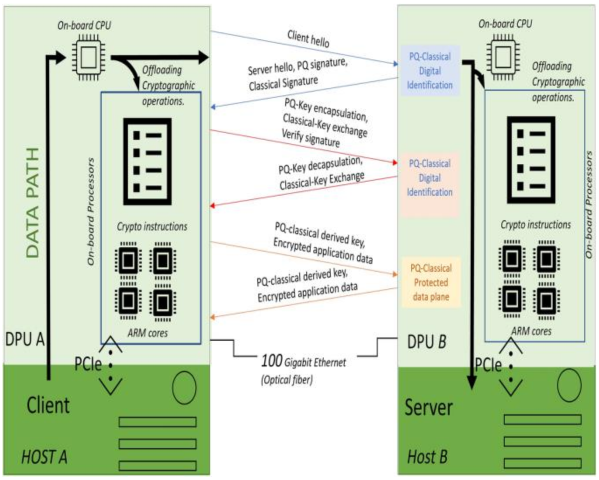
On-board CPU
Offloading Cryptographic operations.
DATA PATH
On-board Processors
Crypto instructions
ARM cores
DPU A
PCIe
Client
HOST A
Client hello
Server hello, PQ signature, Classical Signature
PQ-Key encapsulation, Classical-Key exchange Verify signature
PQ-Key decapsulation, Classical-Key Exchange
PQ-classical derived key, Encrypted application data
PQ-classical derived key, Encrypted application data
100 Gigabit Ethernet (Optical fiber)
PQ-Classical Digital Identification
PQ-Classical Digital Identification
PQ-Classical Protected data plane
On-board CPU
Offloading Cryptographic operations.
On-board Processors
Crypto instructions
ARM cores
DPU B
PCIe
Server
Host B

Figure 4 : Real-World Integration of Post-Quantum Cryptography in Critical Infrastructure

IX. CONCLUSION

Post-quantum cryptography (PQC) is a critical research area in current-day cryptography due to the rapid advancements being made in quantum computers, which can render current public-key cryptographic methods obsolete. Classical algorithms use problems that are relatively hard for classical computers to solve as well, like the RSA, DSA and ECC ones. But Shor's quantum algorithms can. With the emergence of quantum technology from theory to real-world applications, the need for cryptographic systems that can evolve at pace with these developments has emerged. PQC is a theoretical advance and more a principle improvement for our secure architecture.

Much work has gone into finding cryptographic primitives that are unbreakable to a quantum computer. Quite a few different algorithms could possibly work using lattices, codes, multivariate data (hashes) and isogeny. These are both good and bad for different reasons. Lattice-based approaches are becoming increasingly popular for being fast, versatile and making conservative security assumptions. While code-based algorithms such as McEliece have been unbreakable for quite some time, they suffer from key sizesissues. SPHINCS+ and hash-based signatures are, in theory, rather secure. They do also have a massive signature and other issues in eve though. These changes are the reason why NIST started the PQC standardization process. They have a method for safe algorithm selection due to rigorous cryptanalysis, performance testing and ease-of-use.

It is improving but it will not be easy nor soon for everyone to start using PQC. It is still had to get both the software and native hardware to operate. Examples of these are taking up more memory, being difficult to attach to other systems, and increasing the risk of side-channel attacks. There exist protocols like TLS, SSH and IPsec as well which need to be changed or rebuilt, so that they operate in an encryption mode that is either somewhat post-quantum or completely post-quantum. You guys have to balance security and performance for the production environment, and that requires a lot of tuning before you go live. This specifically holds true for scenarios where there is low space like IoT, Mobile devices or be it Embedded System. In principle, it is even more important that they have safe implementations that always run in constant time even if they are targeted in person. We have libraries for building and evaluating fpga/asic architectures, and an active community behind liboqs and PQClean taking care the systems will be goodII.

At the same time, the transition to quantum-safe infrastructures as a whole should also be supported by robust legal and policy frameworks. Agencies like the National Security Agency (NSA), European Network and Information Security Agency (ENISA) or Japanese Cryptography Research and Development Center (CRYPTREC) are only some of the government, cybersecurity institutions that will likely provide support later in the process to transition to post-quantum standards. The internet, your bank money, and shining buildings are not the best we have. This is what our world really is! It happens that these technologies are hidden behind beautiful appearances onStopWarIfNeeded Therefore it is important for governments to cooperate. Someone should be able to find and use intellectual rights, open standards, and export limits easily without being bogged down by legal concerns that could hinder uptake or innovation. And everyone in the sector can easily pick up open-source, royalty-free algorithms – making trust more widespread around the globe.

According to their policy prescriptions, the public and private sectors must cooperate much more closely to ensure a safe "energy transition. In this way, going forward with classical and quantum-safe algorithm will help in Hybrid cryptography installations. It adds Quantum Resistance on end-of-life systems, they help to keep them up running. In this world, Google gets the CECPQ2 project of Quipper and starts using these real-world encryption applications as other encrypted messaging apps and VPN services are already doing. However, it is a pretty big engineering lift and this needs to be solved so that hybrid models can handle speeds, complexity and sizes of handshakes.

Future work will likely involve further perfecting the algorithms computationally, to make them more compact and efficient while ensuring they do not clash with upcoming technologies. PQC is becoming very relevant for 6G high-speed communications, digital ID systems, some blockchain and zero-knowledge proof initiatives to name a few including quantum safe secure multiparty computation. There is a lot to be done in terms of money, developing new algorithms and thoroughly testing that they operate safely, such as training together with the world to secure these areas.

Essentially, post-quantum encryption upends much of the way we go about keeping our data safe. It requires collaboration between disciplines, novelty on a regular basis and patience for the long game. As quantum computing evolves we will have to update our digital systems to make sure they stay secure. And that we must begin to deploy PQC now in order to protect the privacy, integrity and availability of the digital infrastructure of tomorrow. This is so critical for the future of secure communication.

X. REFRENCES

[1] Shor, P. W. (1994). Quantum Computation: Discrete Logarithms & Factoring In Proc. 35th FOCS.

[2] Grover, L. K. (1996). Quantum mechanical description of an algorithm for database search. In 28th Annual ACM Symposium on Theory of Computing.

[3] Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) (2009). Post-Quantum Cryptography. Springer.

[4] NIST. (2022). Post-Quantum Cryptography Standardization Project. https://csrc.nist.gov/Projects/post-quantum-cryptography

[5] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2016). Post-Quantum Key Exchange – A New Hope. USENIX Security.

[6] Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Whyte, W. (2018). CRYSTALS-Kyber. IEEE European Symposium on Security and Privacy.

[7] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P. & Stehlé, D. (2018). CRYSTALS-Dilithium. IEEE Euro S&P.

[8] Bernstein, D. J., et al. (2009). Security of the McEliece cryptosystem and its variants; PQCrypto.

[9] Hülsing, A., et al. (2013). SPHINCS: Practical stateless hash-based signatures. EUROCRYPT.

[10] Open Quantum Safe Project. https://openquantumsafe.org

[11] NSA. (2022). CNSA Suite 2.0. https://www.nsa.gov

[12] ENISA. (2021). New Current Benchmark Review on Post-Quantum Cryptography.

[13] Lyubashevsky, V., Peikert, C., and Regev, O. (2010). New constructions for ideal lattices and application to learning with errors over rings. EUROCRYPT.

[14] Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends® in Theoretical Computer Science.

[15] Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

[16] Chen, L., et al. (2016). Report on Post-Quantum Cryptography. NISTIR 8105.

[17] NIST. (2022). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism: ML-KEM (Draft).

[18] NIST. (2022). FIPS 204: Module-Lattice-Based Digital Signature Algorithm: ML-DSA (Draft).

[19] NIST. (2023). FIPS 205 - Stateless Hash-Based Digital Signature Algorithm: SLH-DSA (Draft).

[20] Aranha, D. F., Paterson, K. G. (2016). On the Security of Hybrid Key Exchange Protocols. ASIACRYPT.

[21] Campagna, M. et al. (2020). Hybrid Post-Quantum TLS. IETF Draft.

[22] Schwabe, P., Stoffelen, K. (2016). All the AES you need. Selected Areas in Cryptography.

[23] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A Ring-based Public Key Cryptosystem. ANTS.

[24] Courtois, N. T. (2001). Secure and Efficient Zero-Knowledge Authentication. PKC.

[25] Beullens, W. (2021). Rainbow Shattered in a Weekend. Cryptology ePrint Archive.

[26] Regev, O. (2005). Lattices, Learning with Errors, Random Linear Codes and Cryptography. STOC.

[27] Goldreich, O., Goldwasser, S., & Halevi, S. (1997). Lattice reduction problems and public-key cryptosystems. CRYPTO.

[28] Hoffstein, J., Howgrave-Graham, N. (2003). NTRUEncrypt: Alive after all these years. PQCrypto.

[29] Sendrier, N. (2011). Cryptography from Code: Current State and Perspectives. IEEE Security & Privacy.

[30] Hülsing, A., Rijneveld, J., Schwabe, P. SPHINCS+. Submission to NIST PQC.

[31] ETSI. (2020). Quantum Safe Cryptography and Security. ETSI TR 103 619.

[32] Steinfeld, R., et al. (2012). Secure against keyword guessing attacks. PKC.

[33] PQClean GitHub Repository. https://github.com/PQClean/PQClean

[34] Bindel, N., et al. (2021). Hybrid Key Encapsulation Mechanisms. IACR.

[35] Hülsing, A., Butin, D. (2018). XMSS: Extended Hash-Based Signatures. RFC 8391.

[36] Chen, M. S., et al. (2020). Quantum cryptanalysis: Progress and challenges. ACM Computing Surveys.

[37] Derler, A., Krenn, S., Slamanig, D. (2018). Post-quantum zero-knowledge proofs. PQCrypto.

[38] Misoczki, R., et al. (2013). MDPC-McEliece: New McEliece Variants. ISIT.

[39] Albrecht, M. R., et al. (2017). LWE, NTRU, and SIS Problems: Estimates. Cryptology ePrint Archive.

[40] Overbeck, R., Sendrier, N. (eds.) (2009). Code-based cryptography. In Post-Quantum Cryptography.

[41] Bernstein, D. J., Lange, T., Niederhagen, R. (2011). Dual EC: A Standardized Backdoor. CHES.

[42] D'Anvers, J. P., et al. (2021). SABER: Module-LWR Based Key Exchange. PQCrypto.

[43] Kales, D., et al. (2020). Secure MPC with Post-Quantum Guarantees. IEEE S&P.

[44] Boneh, D., Kim, S. (2019). Quantum Resilient Zero-Knowledge Systems. ePrint Archive.

[45] Naehrig, M., et al. (2011). Can Homomorphic Encryption be Practical? ACM Cloud.

[46] Chen, H., et al. (2019). On Deploying Quantum-Resistant Authentication. IEEE Comm. Mag.

[47] Fluhrer, S. (2017). Quantum-safe key encapsulation in TLS. Internet-Draft.

[48] Lindner, R., Peikert, C. (2011). Better key sizes for LWE-based encryption. CT-RSA.

[49] Lepoint, T., Naehrig, M. (2014). A Comparison of Homomorphic Encryption Schemes. EUROCRYPT.

[50] IETF Crypto Forum Research Group. (2023). Quantum-Ready Internet Protocols. Draft.