Name: Taiba Khan

Course Title: Introduction to Computing (IT-104-B01)

Date: 15-06-2025

Title: Post Quantum Cryptography

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/wp-content/uploads/2023/08/George-Mason-University-Honor-Code-2023-2024-final-version-SaveasPDF.pdf and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ web site."

Post Quantum Cryptography (PQC)

1.Introduction

As we move into the digital age, everything is only secure if it's up to date cryptographically. Cryptography is the foundation of safe communication. It protects everything from daily personal messages to secrets concerning national security. Existing and traditional systems of cryptography such as RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellmann have been around for decades and stand up to attacks by classical computers. They enjoy widespread trust on our internet, banking, government, and healthcare systems. However, as useful as quantum computing has the potential to be, it disrupts decades of established systems of digital security.

1.1 Quantum Cryptography

Quantum Computers operate by fundamentally different, and better, rules than classical computers. Computers operate on bits, with a bit being either on or off, or 1 or 0. Quantum computers operate on quantum bits, or qubits, and leverage things like superposition and quantized entanglement to solve problems typical computers cannot solve, or to solve problems that would take a typical computer billions of years to solve. Quantum computers are not there yet, but they will be able to break widely used algorithms that traditional computers are inefficiently simulating. A particular algorithm named Shor's algorithm was developed in 1994. Shor's algorithm is a quantum algorithm specifically designed to factor large integers exponentially faster than the fastest known classical algorithms. Exponentially faster ultimately directly affects RSA and ECC, which are the two main cryptographic pillars of authentication and security of the internet. Another algorithm called Grover's algorithm can greatly reduce the effective security of symmetric key algorithms and therefore requires longer symmetric key lengths to adequately secure things.

1.2.Post-Quantum Cryptography

In light of the potential threats posed by quantum computing, researchers and cryptographers are taking action now to create a new set of cryptographic algorithms that are secure from quantum attacks. Researchers refer to this area as Post-Quantum Cryptography (PQC), while it is also referred to as quantum-resistant or quantum-safe cryptography. Unlike quantum cryptography, which is built on the principles of quantum mechanics, PQC is based on classical problems that we believe to be hard for classical and quantum computers to solve, and can work on classical computing (lattice-based, multivariate polynomial, code-based, and hash-based digital signatures). PQC is not just an academic exercise. Any sensitive data that is encrypted today, such as government classified information, medical records, and corporate sensitive information could be captured today and stored for when quantum computers become powerful enough to decrypt, or "harvest now, decrypt later." PQC standards develop better urgency to develop and adopt (Bernstein, Buchmann, & Dahmen, 2009).

After years of testing and working with academics, government agencies, and the private sector, NIST finally announced its first batch of standardized PQC algorithms in 2022, which was a huge milestone in efforts to safely prepare the future digital ecosystem for the coming post-quantum paradigm. As we move toward a post-quantum world brought upon by quantum computing, ensuring post-quantum cryptographic would not be an option, but in reality, a necessity. Organizations, governments, and individuals need to start preparing today by learning, and testing the available algorithms under the post-quantum umbrella, and eventually transitioning to a post-quantum secure infrastructure. Post-Quantum Cryptography lies in the intersection of urgent need and cutting-edge technology and represents the next frontier in securing our digital domains in light of the challenges posed by quantum computing.

The purpose of this study is to delve into the domain of Post-Quantum Cryptography (PQC), looking closely at its use case, its mathematical basis, and whether it is useful in the advancement of a digitally inclusive method of information security. It will look at the different types of algorithms growing, such as lattice-based algorithms, hash-based algorithms, code-based schemes, as well as review the efforts, standards, and protocols put forward by worldwide institutions such as NIST. It will also speak to the various technical and operational challenges of moving from classical to post-quantum systems. Overall, this paper attempts to show the immense importance that PQC will have to global information security in what will eventually be a quantum computer world

2.Development of Post-Quantum Cryptography (PQC)

is emerging as a crucial advancement in information technology, driven by the looming threat quantum computers pose to current cryptographic systems like RSA, Diffie-Hellman, and ECC. These traditional systems rely on mathematical problems difficult for classical computers but vulnerable to quantum algorithms such as Shor's Algorithm, which could compromise digital security.

In response, researchers began exploring quantum-resistant algorithms in the early 2000s, culminating in NIST's 2016 initiative to standardize PQC algorithms. These approaches are designed around problems quantum computers struggle to solve efficiently.

1. Lattice-Based Cryptography

One of the most promising areas in PQC, it uses hard problems like Learning With Errors (LWE) and the Shortest Vector Problem (SVP). Algorithms such as **CRYSTALS-Kyber** (encryption) and **CRYSTALS-Dilithium** (signatures) offer strong security, efficiency, and are already adopted in modern systems.

2. Code-Based Cryptography

Relying on the difficulty of decoding linear error-correcting codes, **Classic McEliece** remains a strong contender due to its long-standing resistance to cryptanalysis. However, its large public key sizes (hundreds of KB to several MB) limit its use in bandwidth-constrained systems.

3. Hash-Based Cryptography

Using hash functions like SHA-256, this method supports quantum-resistant digital signatures. **SPHINCS+** is a prominent example, valued for its simplicity and security. However, large signature sizes and slower performance can hinder real-time use.

4. Multivariate Polynomial Cryptography

This area involves solving multivariate quadratic equations, a hard problem for all computers. Though **Rainbow** showed promise in digital signatures, recent cryptanalytic attacks have exposed vulnerabilities, making it a less reliable option for now.

5. Isogeny-Based Cryptography

Built on finding isogenies between elliptic curves, this approach is notable for small key sizes, ideal for bandwidth-limited applications. However, the recent break of **SIKE** highlights the fragility of newer schemes and the need for further research.

(Aggarwal et al., 2017).

3.Applications of PQC

Post-Quantum Cryptography has a prominent role in the future across many applications where secure communication for data protection is paramount.

3.1. Securing Internet Communications

While the internet might rely on protocols like TLS (Transport Layer Security) and SSL (Secure Sockets Layer), to protect data exchange between browsers and web servers, PQC is crucial for upgrading these protocols to withstand quantum threats. Email encryption systems such as PGP (Pretty Good Privacy) and secure messaging platforms (e.g., Signal, WhatsApp) also depend on cryptographic keys vulnerable to quantum attacks. Potential benefits for securing internet communication are:

- Future-proof online security: PQC ensures that even if encrypted internet traffic is captured today, it cannot be decrypted later by quantum computers.
- Continuous trust: Maintains the integrity and authenticity of web servers and digital certificates.
- Compliance: Helps organizations meet future cybersecurity standards that require quantum-safe encryption.

3.2. Cloud Data Protection

Cloud computing services (like AWS, Google Cloud, Microsoft Azure) host everything from private documents to national databases. With users increasingly depending on remote servers, PQC becomes essential in encrypting stored data, communications, and backups against quantum decryption. Potential benefits are:

- End-to-end encryption: Ensures that even cloud providers cannot access user data without authorization.

- Data durability: Protects long-term stored data (e.g., medical records or contracts) from being compromised in the future.
- Secure migration: Facilitates safe cloud migration for sensitive enterprises like healthcare, legal, and financial services (Mosca, 2018).

3.3. Financial Systems and Online Banking

Digital banking and financial transactions are heavily dependent on public key cryptography for login security, secure money transfers, and transaction signing. From ATM operations to mobile banking apps and global payment systems like SWIFT, PQC must replace existing cryptographic tools to safeguard assets. It has some potential benefits, that are:

- Fraud prevention: Quantum-safe encryption makes it significantly harder for attackers to forge transactions or manipulate banking data.
- Secure fintech growth: Enables safer use of innovative financial technologies, including digital wallets and online investment platforms.
- Transaction authenticity: Ensures that signatures remain valid and verifiable even decades later (Chen et al., 2016).

4.Legal, Social and Ethical Issues Associated with PQC

4.1.Legal Issues:

As quantum computing threatens to break existing encryption systems, the legal landscape surrounding Post-Quantum Cryptography (PQC) is becoming increasingly complex. Key concerns include intellectual property (IP) rights, where many PQC algorithms are patented or contain proprietary components, creating risks of unintentional infringement and deterring open development. Developers and organizations often face uncertainty around licensing costs and usage rights, prompting calls for greater transparency during the standardization process. At the same time, varying global regulatory responses are complicating compliance. While sectors like finance, healthcare, and defense are beginning to incorporate PQC into legal frameworks, many others lack clear mandates. This raises liability issues for delayed adoption and highlights the need for coordinated, sector-wide regulations to ensure timely and uniform PQC implementation.

Additionally, PQC is subject to export controls due to its dual-use nature—applicable in both civilian and military domains—making international collaboration difficult. Laws such as the U.S. Export Administration Regulations (EAR) and similar policies in other nations tightly regulate the export and development of cryptographic tools. National security concerns can further restrict PQC research, especially in defense contexts, resulting in geopolitical tensions and uneven global access. Moreover, legal recognition of PQC standards is still evolving. While organizations like NIST, ISO, and ETSI are working on standardizing quantum-resistant algorithms, the absence of finalized standards creates hesitation for widespread adoption. This delay increases the risk of "harvest now, decrypt later" attacks, underscoring the urgency for legal systems to adapt and support secure, future-proof communication infrastructure.

4.2.Social Issues:

While Post-Quantum Cryptography (PQC) offers vital advancements in digital security, its implementation brings significant social challenges. One major concern is **accessibility and digital inequality**—developing countries, small businesses, and underfunded institutions may lack the resources, technical infrastructure, and expertise needed to adopt PQC, widening the global security gap. This “quantum divide” risks leaving vulnerable populations further exposed to cyber threats. Compounding this is the general **lack of public awareness**—many people do not understand quantum computing or the need for PQC, leading to either resistance to change or misplaced confidence in outdated encryption. Public education campaigns, curriculum integration, and industry outreach are essential to foster widespread understanding and support for the transition.

Trust in institutions is another central issue. Public skepticism grows if PQC adoption appears exclusive to governments and tech giants, reinforcing fears about privacy loss and increased surveillance. Transparent communication and inclusive policymaking are critical to ensuring PQC is seen as a tool for protecting, not undermining, civil liberties. Additionally, **global inclusion** remains a challenge, with most PQC research and standardization driven by a few advanced nations. To avoid reinforcing global tech inequality, international collaboration and equitable participation in PQC development must be prioritized.

Lastly, PQC could be **misused by bad actors**, such as terrorists or cybercriminals, who might exploit its resilience to hide activities from law enforcement. While some propose backdoors for "lawful access," doing so undermines the very purpose of PQC. Balancing privacy rights with public safety remains an ongoing ethical dilemma in the secure digital future PQC aims to support.

4.3.Ethical Issues

Post-Quantum Cryptography (PQC) introduces critical ethical challenges alongside its security benefits. One major concern is the **potential misuse by malicious actors**, such as terrorists or cybercriminals, who could exploit quantum-resistant encryption to conceal harmful activities, making lawful surveillance extremely difficult. This raises a dilemma between upholding individual privacy and ensuring public safety. At the same time, **inequitable access and**

participation in PQC development—dominated by wealthier nations and institutions—threatens to deepen global cyber disparities. Developing countries and low-resourced organizations may lack the means to adopt PQC, leaving them exposed to future quantum threats and excluded from shaping the standards that will govern global security.

Further ethical issues stem from **lack of transparency and rushed implementation**. Organizations may upgrade systems without informing users, bypassing informed consent and risking trust. Rolling out PQC without adequate testing can also create false security and new vulnerabilities. Moreover, while PQC is intended to enhance privacy, there is concern that some governments may exploit the quantum threat to justify increased digital surveillance or demand backdoors, undermining civil liberties. For PQC to be ethically implemented, it must balance innovation with caution, promote equitable access, and protect privacy without enabling state overreach (European Telecommunications Standards Institute [ETSI], 2020).

5.Security Aspects and Challenges of Post-Quantum Cryptography

As quantum computers rapidly advance, they threaten the foundation of classical cryptographic systems like RSA and ECC, which could be rendered obsolete by quantum algorithms such as Shor's. The most immediate risk is the **"harvest now, decrypt later"** scenario, where adversaries collect encrypted data now with the intention of decrypting it in the future using quantum capabilities. Post-Quantum Cryptography (PQC) aims to counter this threat by developing quantum-resistant algorithms, but the field is still maturing, and many proposed solutions are undergoing evaluation. This introduces concerns around **immature algorithms**, which may contain unknown vulnerabilities or may not yet be tested across diverse real-world threat models. Deploying such algorithms prematurely could result in weak protection or wasted implementation efforts.

Even when PQC algorithms are theoretically secure, **implementation vulnerabilities** pose significant risks. These include programming flaws, improper key management, and weak random number generation—problems that become more likely with PQC due to larger keys and more complex operations, which increase the codebase and potential error surface. Furthermore, PQC schemes are particularly vulnerable to **side-channel and timing attacks**, where attackers glean secret information through indirect means like power consumption or execution time. Many PQC algorithms, especially lattice- and code-based schemes, are not constant-time by default, which can unintentionally leak sensitive data. Addressing these challenges requires careful implementation, ongoing review, and secure hardware and software integration to ensure PQC fulfills its promise of future-proof digital protection (Rösler, Mainka, & Schwenk, 2018).

5.2.Challenges in Deployment and Adoption

Post-Quantum Cryptography (PQC), while offering strong protection against future quantum threats, introduces technical and operational challenges. Most PQC algorithms come with larger key sizes, ciphertexts, and signatures, increasing **performance and resource overhead**, especially in constrained environments like IoT and mobile systems. This can slow adoption and lead to insecure workarounds. Moreover, integrating PQC with existing systems presents **interoperability and backward compatibility** issues, requiring secure migration paths and hybrid systems that support both classical and quantum-safe algorithms. This added complexity can create new vulnerabilities. **Standardization and trust** are also critical: while NIST has selected leading candidates like CRYSTALS-Kyber and CRYSTALS-Dilithium, global consensus and cautious adoption are necessary to avoid repeating past cryptographic failures.

To manage these challenges, several **mitigation strategies** are in place. **Hybrid cryptographic models** blend classical and quantum-safe algorithms for layered protection. Ongoing

standardization efforts, especially NIST's, ensure rigorous peer review and selection of robust algorithms. Developers are actively working on **side-channel resistance** by improving constant-time implementations and using hardened hardware. Organizations are encouraged to conduct thorough **testing and simulation** through pilot deployments and attack modeling to identify vulnerabilities. Finally, **public awareness and training** are crucial—educating developers, security professionals, and administrators ensures PQC is implemented correctly and securely, fostering trust and smooth integration into future digital infrastructure.

6.Conclusion

Post-Quantum Cryptography (PQC) is a leading new way forward in cybersecurity in relation to a much more pressing need to protect digital communication against the high level of future quantum computer decrypting strength. Traditional cryptographic systems such as RSA and ECC can only be utilized for a limited time before falling prey to quantum advancements. You cannot stop the quantum computer from evolving, but you can offer a means of defense proactively with PQC. PQC provides encryption and digital signature schemes that are believed to be resistant to quantum decryption. The field of PQC is not just a transition to new technology, but a major transition in how we view data protection at a global scale. Throughout this dissertation, we have reviewed PQC, discussing its history and the importance of PQC. We examined PQC from several perspectives including lattice-based approaches, code-based approaches, multivariate approaches, hash-based approaches, and isogeny-based cryptographic systems, each providing their own individual strengths, individual weaknesses, and potential weaknesses that need continuous cryptanalysis, peer review, and development. We also discussed the myriad of potential use cases across various industries—financial services, military communication, healthcare, cloud computing, and blockchain—where PQC can prioritize privacy and trust in a digital world going forward.

Despite the promise of quantum-safe cryptography, hurdles remain along the route to PQC. There are potential security vulnerabilities pertaining to side-channel funds, as well as issues with implementations and underdeveloped algorithms, which are significant concerns. The ethical implications of PQC can be difficult to navigate: it can enhance our privacy and data ownership, but also can be used for good or ill. Similarly, it has the potential to further the digital divide between advanced countries and developing countries. The legal considerations surrounding PQC can also be scrambled: beyond intellectual property, is regulatory, and standardization issues. As this space continues to develop, integrating ethical, legal and security aspects of PQC will be better served by integrative ethics. Ethical frameworks can help inform responsible development and distribution of PQC technologies. Legal parameters can help with compliance, while also being flexible enough to highlight the importance of innovation in a manner that respect privacy. Security factors will require continuous review processes to establish breaches not only from quantum, but open new areas of vulnerability through uninformed developments as implementations are developed and deployed.

In closing, Post-Quantum Cryptography is much more than a response to quantum computing; it presents a challenge to rethink and reaffirm our underlying commitment to cybersecurity, privacy, and digital ethics. By cultivating an open, transparent, and collaborative PQC process, we can imagine a future in which our information is secure, our systems resilient, and our digital rights as individuals are respected in the face of the advancements of quantum computing.

References

1.Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009).

Post-quantum cryptography. Springer. https://doi.org/10.1007/978-3-540-88702-7

Accessed on: June 14, 2025

This scholarly book is one of the earliest and most influential texts addressing the foundations of Post-Quantum Cryptography (PQC). It explores various quantum-resistant algorithms such as lattice-based, multivariate, and code-based cryptography, providing a technical introduction suitable for researchers and graduate students. As an edited volume by leading cryptographers, it maintains high academic standards and provides peer-reviewed, technically sound content. The reliability of the book is enhanced by its publication through Springer and its citation in numerous subsequent works on PQC. It is a crucial source for understanding the early theoretical developments and mathematical frameworks underlying PQC.

2.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. https://doi.org/10.6028/NIST.IR.8105

Accessed on: June 14, 2025

This technical report by NIST provides a comprehensive overview of why PQC is necessary, focusing on the quantum threats to RSA and ECC algorithms. It discusses various post-quantum approaches and outlines criteria for selecting secure alternatives. As a U.S. government publication by one of the most respected institutions in cybersecurity, this source is highly credible and free of commercial bias. It is often used in academic, industrial, and policy discussions and supports ongoing standardization efforts. This source is foundational to understanding the government's role in preparing for post-quantum threats.

3. **Mosca, M. (2018).**

Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSEC.2018.053761606

Accessed on: June 14, 2025 (Database: IEEE Xplore – https://ieeexplore.ieee.org)

This journal article raises awareness about the urgency of migrating to quantum-resistant systems and addresses strategic challenges in cybersecurity. Written by Dr. Michele Mosca, a well-known expert in quantum information science, the article blends both technical and strategic insights. It is a reliable and peer-reviewed source published in a reputable IEEE journal. Its concise yet impactful analysis makes it especially useful for understanding the broader implications of PQC adoption and the need for timely global action. The source is highly credible due to its peer-reviewed nature and alignment with ongoing international cryptography efforts.

4. European Telecommunications Standards Institute (ETSI). (2020).

Quantum safe cryptography and security (ETSI White Paper No. 8, Updated).

https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

Accessed on: June 14, 2025

This white paper from ETSI provides industry-focused insight into PQC, including risk management, application in telecom systems, and standardization initiatives. It targets stakeholders from both private and public sectors and reflects a consensus-driven approach to quantum-safe security. As a publication from a leading international standards organization, it is authoritative and regularly cited in industry discussions. The content is up-to-date and includes practical challenges, making it relevant for applied research and implementation studies. It complements more academic sources by providing real-world applicability and regulatory considerations.

5. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017).

Quantum attacks on classical cryptographic protocols. *Nature Communications, 8*, Article 609.

https://doi.org/10.1038/s41467-017-02340-5

Accessed on: June 14, 2025

6.Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., & Perlner, R. (2022).

Submission to FIPS 203: CRYSTALS-Kyber (Module-Lattice-Based Key-Encapsulation Mechanism). National Institute of Standards and Technology.

https://csrc.nist.gov/publications/detail/fips/203/draft

Accessed on: June 14, 2025

This draft Federal Information Processing Standard (FIPS) document details the CRYSTALS-Kyber algorithm selected by NIST as the primary standard for post-quantum key exchange. It is highly technical and aimed at cryptographic implementers and policy makers. The document is an authoritative U.S. government source, making it extremely reliable and crucial for technical compliance research. It outlines the rationale, structure, and security properties of Kyber, which is the cornerstone of upcoming cryptographic transitions. This source is essential for any technical analysis of PQC standards.

7.Rösler, P., Mainka, C., & Schwenk, J. (2018).

More is less: On the end-to-end security of group chats in Signal, WhatsApp, and Threema. *Proceedings of the IEEE European Symposium on Security and Privacy*, 415–429.

https://doi.org/10.1109/EuroSP.2018.00036

Accessed on: June 14, 2025 (Database: IEEE Xplore – https://ieeexplore.ieee.org)

While not entirely focused on PQC, this peer-reviewed paper discusses vulnerabilities in popular messaging apps using end-to-end encryption. The findings offer useful context when exploring how post-quantum algorithms can improve these systems. The paper is highly reliable, written by respected security researchers and published at a major IEEE conference. It highlights potential application areas for PQC in group communication. This indirect connection helps broaden the understanding of PQC's real-world impact on daily-used technologies.

Appendix A: Use of ChatGPT

This appendix describes how ChatGPT was used to create this research study. The main contributions and prompts are listed below:

1.Brainstorming for the Topic:

- Prompt: "Suggest some technologies in information technology that are under development"
- Response: " ChatGPT gave a list of technologies including, generative AI, edge AI and 5G Integration, AI-powered cybersecurity, post quantum cryptography and Web3 blockchains innovations. Post quantum cryptography was selected for the research."

2.Outline:

- Prompt: " Provide an outline on the topic Post Quantum Cryptography for research study."
- Response: "Sections that were suggested were examined and modified for the paper's outline.

3. Suggestions for the Section Headings

- Prompt: “ Can you summarize the significance and possibilities of quantum cryptography in a paper's section headings?”
- Response: “ Provided a detailed draft with key points to add in the research paper.”