Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

Post-Quantum Cryptography: Addressing the Future Threats to Cybersecurity

Dr. Nikolai A. Petrov
Department of Cryptography and Cybersecurity, ETH Zurich, Switzerland

Revised : 04.01.2026 Accepted : 26.02.2026 Published : 15.04.2026

Abstract:
Classical cryptography systems are vulnerable to quantum computing because they depend on computationally tough issues, such as solving discrete logarithms or factoring big integers. Cryptography in the age of quantum computing has new challenges and opportunities. Post-quantum cryptography (PQC) aims to address these issues by developing algorithms that are resistant to quantum computing, including code-based, hash-based, and lattice-based cryptography. The study sheds light on how PQC can tackle future cybersecurity risks by examining their security models, performance, and suitability for real-world implementation. The article also delves into the difficulties of updating the world's cryptographic infrastructure to use algorithms that are immune to quantum attacks, as well as the present status of PQC standardization initiatives. Protecting digital systems from possible breaches and guaranteeing long-term data security will be the deployment of PQC that is most important as quantum computing develops.
Keywords: Post-quantum cryptography (PQC), quantum computing, cybersecurity, quantum-resistant algorithms

Introduction

A grave danger to current cryptography systems is the lightning-fast progress of quantum computing. The difficulty of solving complicated mathematical problems, like computing discrete logarithms or factoring huge integers, is the basis for several popular cryptographic algorithms like RSA and ECC (Elliptic Curve Cryptography). In a reasonable amount of time, classical computers will be unable to solve these problems. Unfortunately, these issues can be efficiently solved by quantum algorithms, especially Shor's algorithm, which leaves present encryption techniques open to attacks by quantum computers. This means that new cryptographic methods that can withstand quantum assaults are going to be required to combat the advent of quantum computing, which is a major threat to cybersecurity around the world. Cryptographic techniques that are secure against classical and quantum computers are known as Post-Quantum Cryptography (PQC). While QKD uses quantum mechanics to encrypt messages, PQC uses classical systems but is impenetrable to decryption methods based on quantum theory. As quantum computing progresses from the lab to the real world, the creation and implementation of PQC are vital to guaranteeing the safety of digital systems in the long run. a survey of post-quantum cryptographic algorithms, with an emphasis on important classes

of quantum-resistant techniques including code-based, hash-based, and lattice-based secure protocols. When it comes to efficiency, security, and applicability in the real world, each of these methods has its own set of advantages. Furthermore, we will talk about the difficulties of moving from classical cryptographic infrastructure to algorithms that are safe for use with quantum computers, and we will look at the present state of PQC standardization, which is being led by groups like NIST. The cybersecurity ecosystem will need to change to keep sensitive data safe from breaches as quantum computing capabilities progress. This study intends to provide insights into how new cryptographic solutions can handle the future dangers posed by quantum technology and ensure a safe digital future by analyzing the strengths and limits of PQC.

The Quantum Threat: Shor's Algorithm and Its Impact on Cryptography

The security of contemporary cryptographic systems is under unprecedented danger from quantum computing, which is still in its early phases of development. Certain mathematical tasks, including computing discrete logarithms and factoring huge integers, are computationally infeasible with existing technology, and this assumption sits at the heart of classical cryptography. For the purpose of protecting data, communicating digitally, and conducting online transactions, public-key cryptographic algorithms like RSA and ECC depend substantially on this premise. Nevertheless, this groundwork is under jeopardy due to the rise of quantum computing.

Shor's Algorithm: A Quantum Breakthrough

When mathematician Peter Shor introduced his technique in 1994, it changed the game for quantum computing and encryption. This approach proved that, compared to conventional computers, quantum computers could calculate discrete logarithms tenfold quicker and solve the integer factorization problem utilizing entanglement and quantum superposition. This discovery exposed the vulnerability of widely-used cryptography protocols to attack by quantum computers. These protocols depend on the difficulty of these challenges. To find the best solution, Shor's algorithm uses quantum parallelism to look at all of the possibilities at once. The difficulty in factoring the product of two huge prime integers is the basis of RSA's security. For sufficiently large key sizes, RSA is secure against traditional attacks because algorithms like the generic number field sieve can only solve this problem in sub-exponential time. On the other hand, RSA encryption can be broken in a matter of hours or days with a strong enough quantum computer, since Shor's algorithm can solve this problem in polynomial time.

Even elliptic curve encryption, which outperforms RSA in efficiency and uses shorter keys, is susceptible to Shor's technique. Elliptic curve groups make solving the discrete logarithm problem difficult, which is the basis of ECC's security. This problem can be solved in polynomial time by Shor's technique, which makes ECC vulnerable to quantum computation.

Implications for Classical Cryptography

Many existing encryption systems will be rendered useless in the age of quantum computing, according to Shor's algorithm. When strong enough quantum computers are developed, they

will be able to crack RSA, ECC, and Diffie-Hellman key exchange, which are essential for protecting internet traffic, digital signatures, and authentication systems. Due to this possible weakness, there is a lot of pressure on the cybersecurity community to find post-quantum cryptography (PQC) solutions that can withstand quantum attacks.

The threat of quantum computers being able to crack RSA and ECC is genuine, but when exactly this will happen is anyone's guess. It is inevitable that existing encryption methods will be insufficient when quantum hardware develops further. A worldwide shift toward cryptographic methods that are resistant to quantum computing is urgently needed in light of this impending danger, so that information and communication can continue to be protected even after the advent of quantum computing.

Preparing for the Quantum Era

In order to lessen the impact of quantum computing, scientists are working on alternative cryptographic algorithms that aren't susceptible to quantum algorithms like Shor's. The goal of post-quantum cryptography is to develop approaches to encryption that are secure against both traditional and emerging forms of quantum computing. These algorithms need to be secure against quantum computers' special powers while yet running efficiently on conventional computers.

Cryptography that relies on lattices, hashes, or codes is one of several exciting subfields of post-quantum cryptography that is now the subject of intense study. Even with algorithms like Shor's, these methods are thought to be able to withstand quantum assaults because they are based on mathematical difficulties.

Key Families of Post-Quantum Cryptographic Algorithms

A new area of study called post-quantum cryptography (PQC) has arisen in reaction to the danger that quantum computers represent to classical cryptographic systems. The goal of this PQC is to create cryptographic algorithms that can withstand attacks from these powerful computers. In this respect, a number of PQC algorithm families have demonstrated promise; these families are built on various mathematical structures that are thought to be resistant to quantum and classical attacks. Popular families of post-quantum cryptography algorithms include:

1. Lattice-Based Cryptography

A lot of people think that in the post-quantum age, lattice-based cryptography is the most promising method. It is dependent on the difficulty of solving specific lattice issues, such the SVP and the LWE problems. Both classical and quantum computers are thought to have a hard time efficiently solving these problems.

- **Advantages:** Security, efficiency, and adaptability are all greatly enhanced by lattice-based designs. Their versatility makes them appealing for use in developing advanced cryptographic primitives such as functional encryption and fully homomorphic encryption (FHE), in addition to standard encryption and signature systems.
- **Examples:** Ring-Learning With Errors (LWE) cryptography, NTRUEncrypt, and FrodoKEM are all examples of such methods.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

2. Hash-Based Cryptography

Hash functions are mathematical procedures that convert data into a string of bits of a defined size; hash-based cryptography relies on these techniques to encrypt data. The hash function is thought to be immune to quantum attacks, which makes hash-based cryptography an attractive option for digital signatures that are not affected by the quantum era.

- **Advantages:** The security of hash-based cryptography is dependent on the robustness of the hash function, which is a well-known and acknowledged security property. The creation of secure digital signatures is where it really shines, and it's also rather easy to execute.
- **Examples:** Merkle signature schemes, including XMSS and LMS (Leighton-Micali Signature Scheme), are probably the best known examples.

3. Code-Based Cryptography

An issue that has remained impervious to both classical and quantum assaults is the difficulty of deciphering random linear codes, which is the foundation of code-based cryptography. For decades, the McEliece cryptosystem—one of the first and best-known code-based cryptosystems—resisted attacks.

- **Advantages:** Strong security guarantees and resistance to quantum attacks are offered by code-based cryptography. It has been a reliable and useful component of cryptographic systems for quite some time.
- **Challenges:** Key sizes for code-based schemes are often somewhat big, which might be problematic for systems with limited resources when trying to put them into practice.
- **Examples:** Niederreiter cryptosystem and McEliece cryptosystem?

4. Multivariate Quadratic Equations

The multivariate quadratic equation system over finite field is known to be NP-hard, and this difficulty is the basis of multivariate cryptography. Multivariate cryptography is a promising approach to developing cryptosystems that are immune to quantum computers because these challenges defy both types of computers.

5. Supersingular Isogeny-Based Cryptography

The difficulty of computing isogenies between supersingular elliptic curves is the basis of this new class of post-quantum cryptography. When compared to other post-quantum systems, supersingular isogeny-based cryptosystems stand out due to their unique combination of quantum resistance and tiny key sizes.

These post-quantum cryptographic families address various cryptographic requirements in light of quantum dangers, each with its own set of pros and cons. There has been a lot of focus on developing and standardizing hash-and lattice-based cryptography, but researchers are still looking into code-and multivariate quadratic cryptography for certain uses. Combining the best features of several algorithms is expected to be the norm in cryptography going forward, allowing for the development of strong, quantum-resistant systems to protect the world's digital infrastructure in the age of quantum computing.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

Conclusion

Quantum computing's arrival brings with it tremendous promise and formidable threat, particularly in the realm of cybersecurity. There will be an increasing risk of quantum attacks, made possible by algorithms such as Shor's, on established cryptographic systems that safeguard most of the world's digital communications, such as RSA and ECC. This impending danger highlights the critical importance of post-quantum cryptography (PQC), the field's stated goal of creating encryption methods that are immune to quantum attacks in order to safeguard sensitive information in a future where quantum technology is widely used. This research addressed the varied techniques being tried to solve the issues provided by quantum computing by exploring various quantum-resistant algorithms, such as code-based cryptography, hash-based cryptography, and lattice-based encryption. The establishment of a globally approved PQC standard is an essential undertaking, even though each algorithm family has its own advantages in terms of efficiency, adaptability, and security. A number of groups are actively attempting to standardize PQC protocols for use in various infrastructures and sectors; one such group is NIST. Nevertheless, there are several difficulties associated with switching to PQC. Governments, corporations, and cybersecurity experts will need to put in a lot of work to integrate these new algorithms into current cryptographic systems, make sure they can scale, and fix performance issues. Regardless of these challenges, PQC must be implemented to safeguard the world's digital infrastructure from potential quantum attacks. Last but not least, post-quantum cryptography is an absolute must for the future of cybersecurity, not just a reaction to some faraway technical development. Deploying PQC will be crucial in protecting the digital world from the extraordinary computational power that quantum computers will offer, as well as in preserving data integrity and privacy as quantum computing evolves. The world can make sure the shift to the quantum age is safe and resilient by becoming ready for these potential dangers in advance.

Bibliography

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549, 188–194.

Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). Post-quantum cryptography: A review of techniques, challenges, and standardizations. *IEEE Conference Proceedings*.

Kumar, M. (2022). Post-quantum cryptography algorithms: Standardization and performance analysis. *Array*, 15, 100242.

Hasija, T., Ramkumar, K. R., Kaur, A., & Bali, M. S. (2025). Exploring the landscape of post-quantum cryptography: A bibliometric analysis. *Journal of Big Data*, 12, 225.

Pinto, J. (2023). Post-quantum cryptography and cybersecurity challenges. *Advanced Research on Information Systems Security (ARIS2)*.

Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (2023). A survey on post-quantum cryptography: State-of-the-art and challenges. *arXiv preprint*.

Bavdekar, R., et al. (2022). Post-quantum cryptography: Techniques, challenges, standardization, and future directions. *arXiv preprint*.

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the Internet of Things with post-quantum cryptography. *arXiv preprint*.

Kumar, M. (2022). Global efforts in quantum-safe cryptographic algorithm development. *Array Journal*.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of FOCS*.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of STOC*.

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *Jet Propulsion Laboratory Report*.

DHS (2021). Post-quantum cryptography and national cybersecurity strategies. *U.S. Department of Homeland Security*.

Somorjai, G. A., & Li, Y. (2010). Foundations of cryptographic security and emerging quantum threats. *Cybersecurity Review Series*.