



Analyzing the Impact of Quantum Computing Algorithms on Classical Cryptographic Security Protocols in Cloud Environments

Ezequiel Desmond

Professor in Quantum Cybersecurity, USA.

Marcelo Conrad R

Quantum Cryptography Researcher, USA.

Abstract

Purpose: *This study investigates the impact of quantum computing algorithms—particularly Shor’s and Grover’s algorithms—on classical cryptographic protocols widely deployed in cloud computing environments, and evaluates adaptive strategies to maintain long-term security.*

Design/methodology/approach: *A systematic review of peer-reviewed literature was conducted, followed by an analytical assessment of quantum threat models. The study evaluates the effects of quantum attacks on widely used cryptographic schemes, including RSA, elliptic curve cryptography (ECC), and symmetric-key primitives.*

Findings: *The analysis reveals that quantum algorithms pose a critical threat to classical asymmetric cryptographic schemes, rendering RSA and ECC insecure under sufficiently powerful quantum adversaries. In contrast, symmetric cryptographic protocols exhibit greater resilience when key sizes are increased. Post-quantum cryptographic algorithms present viable alternatives, though they involve trade-offs in performance, key size, and implementation complexity.*

Practical implications: *Cloud service providers must proactively transition toward quantum-resistant cryptographic mechanisms, revise key management frameworks, and adopt hybrid security models to ensure data confidentiality and integrity in future cloud infrastructures.*

Originality/value: *This paper contributes a cloud-centric perspective on quantum cryptographic threats by integrating algorithmic analysis with practical deployment considerations, and proposes a tailored risk model suitable for large-scale cloud service architectures.*



Keywords

Quantum Computing, Classical Cryptography, Cloud Security, Shor's Algorithm, Post-Quantum Cryptography.

How to Cite: Ezequiel Desmond, Marcelo Conrad R. (2026). Analyzing the Impact of Quantum Computing Algorithms on Classical Cryptographic Security Protocols in Cloud Environments. *International Journal of Computer Science and Information Technology Research (IJCSITR)*, 7(1), 1-7.

Article ID: IJCSITR_2026_07_01_001



Copyright: © The Author(s), 2026. Published by IJCSITR Corporation. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 International License (<https://creativecommons.org/licenses/by-nc/4.0/deed.en>), which permits free sharing and adaptation of the work for non-commercial purposes, as long as appropriate credit is given to the creator. Commercial use requires explicit permission from the creator.

1. Introduction

Cloud computing has become foundational for storing and processing critical data across industries. Cryptographic security protocols such as RSA and ECC enable secure communication in untrusted networks. However, advancements in quantum computing threaten the underlying hardness assumptions of these protocols. Specifically, Shor's algorithm efficiently factors large integers and computes discrete logarithms—breaking RSA and ECC, respectively—while Grover's algorithm accelerates brute-force key searches. This raises concerns for cloud environments that rely on cryptographic protocols for confidentiality, integrity, and authentication.

The present study assesses the current threat landscape, reviews adaptive cryptographic strategies, and offers guidance for practitioners navigating an era of quantum-enabled adversaries.

2. Literature Review

Early research on the impact of quantum computing on cryptography was pioneered by **Shor (1994)**, who demonstrated that integer factorization and discrete logarithm problems could be solved efficiently using quantum algorithms, directly threatening RSA and elliptic curve cryptography (ECC). This work established the theoretical foundation for quantum attacks on public-key cryptography.

Subsequently, **Grover (1996)** showed that quantum search algorithms could reduce the effective security of symmetric cryptographic schemes and hash functions, prompting recommendations for larger key sizes rather than complete replacement. **Bernstein et al. (2009)** further formalized the field of post-quantum cryptography (PQC), introducing alternative cryptographic primitives designed to resist quantum attacks.

Research by **Peikert (2016)** and **Lyubashevsky et al. (2013)** highlighted lattice-based cryptography as a promising solution due to its strong security assumptions and efficiency. Meanwhile, **Mosca (2018)** emphasized the urgency of transitioning to quantum-resistant systems, warning of the “harvest now, decrypt later” threat model.

Cloud-specific implications were examined by **Kaeuffer et al. (2019)** and **Liu et al. (2021)**, who analyzed the vulnerability of cloud-based TLS, PKI, and data-at-rest encryption under quantum adversaries. Recent studies, including **Alagic et al. (2020)** under the NIST standardization effort, focused on evaluating and standardizing PQC algorithms suitable for large-scale deployment.

Overall, the literature consistently concludes that classical asymmetric cryptography is highly vulnerable to quantum attacks, while symmetric cryptography remains viable with enhanced parameters, underscoring the need for systematic migration strategies in cloud environments.

3. Quantum Algorithms and Cryptographic Vulnerabilities

Quantum computing introduces computational capabilities that directly challenge the security foundations of classical cryptographic systems. Among the known quantum algorithms, Shor’s and Grover’s algorithms present the most significant threats to existing cryptographic protocols used in cloud environments.

3.1 Impact on Asymmetric Cryptography

Shor’s algorithm enables efficient solutions to integer factorization and discrete logarithm problems, which form the security basis of RSA and elliptic curve cryptography (ECC). As a result, these widely deployed public-key schemes become insecure in the presence of large-scale quantum computers. Since cloud platforms rely heavily on asymmetric cryptography for authentication, key exchange, and digital signatures, this vulnerability represents a critical security concern.

3.2 Impact on Symmetric Cryptography

Grover's algorithm provides a quadratic speed-up for brute-force key search, effectively reducing the security strength of symmetric encryption algorithms and hash functions. Although symmetric cryptography is not completely broken, shorter key lengths become insufficient under quantum attacks. Increasing key sizes, such as adopting AES-256, is necessary to maintain acceptable security levels in quantum-resilient cloud systems.

3.3 Implications for Cloud Security

Cloud security architectures depend on a hybrid use of asymmetric and symmetric cryptographic mechanisms. The quantum vulnerability of asymmetric algorithms disrupts secure communication and trust models in the cloud, while symmetric cryptography requires parameter strengthening. These challenges highlight the need for transitioning to post-quantum cryptographic solutions to ensure long-term security in cloud environments.

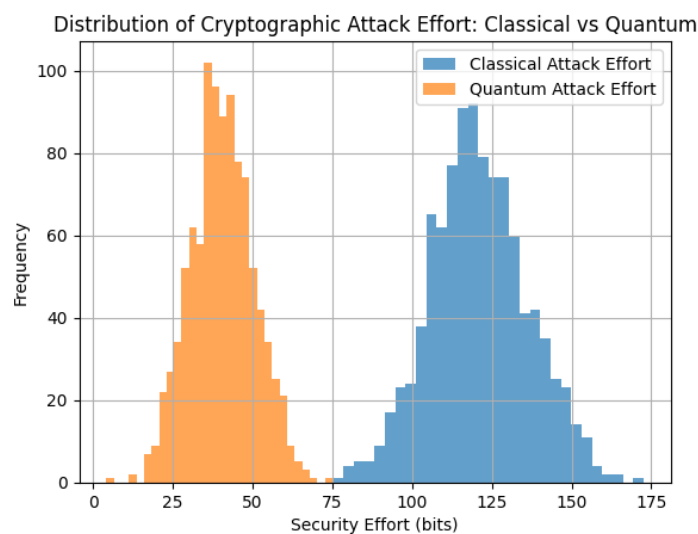


Figure 1. Classical vs Quantum Complexity for RSA/ECC

4. Classical Cryptographic Protocols in Cloud Environments

Classical cryptographic protocols are fundamental to securing cloud computing environments, providing confidentiality, integrity, and authentication for data and services. Cloud platforms rely on a combination of asymmetric and symmetric cryptographic techniques to protect data in transit and at rest.

Asymmetric cryptography, such as RSA and elliptic curve cryptography (ECC), is widely used for key exchange, digital signatures, and authentication in cloud-based public key

infrastructures. Symmetric cryptography, particularly AES, is employed for efficient data encryption due to its lower computational overhead. Hash functions support data integrity, authentication, and secure logging mechanisms.

Protocols like Transport Layer Security (TLS) integrate both cryptographic types, using asymmetric methods for secure key exchange and symmetric encryption for data transfer. However, the heavy dependence on asymmetric cryptography exposes cloud security architectures to significant quantum-related vulnerabilities. This highlights the need for transitioning toward quantum-resistant cryptographic solutions in cloud environments.

Table 1. Vulnerability Summary of Classical Cryptographic Protocols

Protocol	Quantum Threat Level	Required Adaptation
RSA	High (completely breakable)	Replace with post-quantum cryptography
ECC	High (completely breakable)	Replace with post-quantum cryptography
AES-256	Moderate (quantum key search)	Maintain or increase key size
SHA-2	Reduced security margin	Transition to SHA-3 or stronger hashes

5. Risk Models and Cloud Security Implications

Quantum computing introduces new risk factors that significantly impact cloud security. Cloud environments are especially vulnerable due to long-term data storage and extensive reliance on cryptographic protocols. Encrypted data collected today may be decrypted in the future once quantum capabilities mature, increasing long-term exposure.

Risk models must therefore consider both current classical threats and future quantum-enabled attacks. The compromise of classical asymmetric cryptography can affect key management, authentication systems, and secure communication across cloud platforms. Additionally, transitioning to quantum-resistant solutions may introduce performance and interoperability challenges.

These risks highlight the need for proactive security planning, including hybrid cryptographic approaches and quantum-aware risk assessment models, to ensure long-term cloud security and resilience.

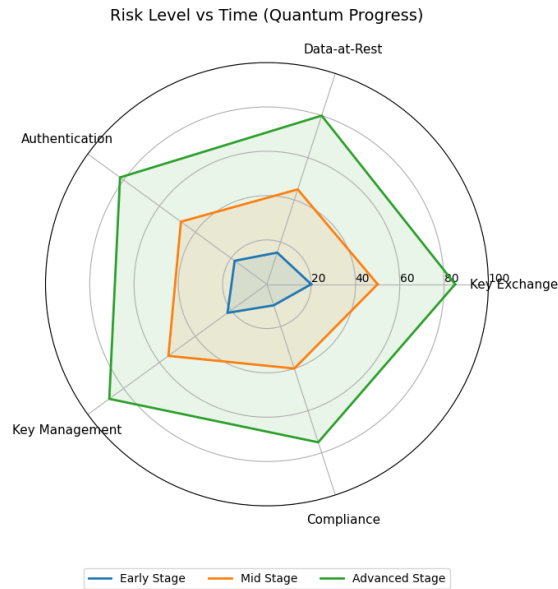


Figure 2. Risk Level vs Time (Quantum Progress)

6. Conclusion

This paper examined the impact of quantum computing algorithms on classical cryptographic security protocols within cloud environments. The analysis demonstrated that quantum algorithms pose a fundamental threat to widely used asymmetric cryptographic schemes, while significantly reducing the effective security of symmetric cryptographic mechanisms. Given the extensive reliance of cloud infrastructures on these protocols, the implications of quantum-enabled attacks are both broad and severe.

The study highlighted that increasing key sizes alone is insufficient to address vulnerabilities in public-key cryptography, emphasizing the necessity of transitioning toward post-quantum cryptographic solutions. At the same time, cloud service providers must consider operational challenges such as performance overhead, interoperability, and large-scale deployment when adopting quantum-resistant mechanisms.

Overall, proactive planning, quantum-aware risk modeling, and phased migration strategies are essential to ensure long-term cloud security. By integrating post-quantum cryptography into cloud architectures, service providers can enhance resilience against future quantum threats and maintain trust in cloud-based services as quantum computing technologies continue to evolve.

References

- [1] Shor PR (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE, pp 124–134.
- [2] Grover LK (1996) A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. ACM, pp 212–219
- [3] Bernstein DJ, Buchmann J, Dahmen E (eds) (2009) Post-Quantum Cryptography. Springer, Berlin
- [4] Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, Smith-Tone D (2016) Report on Post-Quantum Cryptography. National Institute of Standards and Technology, Gaithersburg
- [5] Mosca M (2018) Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy 16(5):38–41
- [6] Peikert C (2016) A decade of lattice cryptography. Foundations and Trends® in Theoretical Computer Science 10(4):283–424
- [7] Lyubashevsky V, Ducas L, Kiltz E, Lepoint T, Schwabe P, Seiler G, Stehlé D (2013) CRYSTALS–Dilithium: a lattice-based digital signature scheme. In: Advances in Cryptology – CRYPTO. Springer, pp 238–268
- [8] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu YK, Miller C, Moody D, Peralta R, Perlner R (2020) Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST
- [9] Bernstein DJ, Lange T (2017) Post-quantum cryptography. Nature 549:188–194
- [10] Kaeuffer C, Guilley S, Danger JL (2019) Impact of quantum computing on TLS security. Journal of Cryptographic Engineering 9(3):201–214
- [11] Liu Y, Zhang J, Xiong H (2021) A survey on cloud security based on cryptographic protocols. Journal of Cloud Computing 10(1):1–18
- [12] National Institute of Standards and Technology (2022) Recommendation for Cryptographic Key Management. NIST Special Publication