World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Review Article)

Post-quantum cryptography: Reshaping the future of identity and access management

Tuhin Banerjee *

Saviynt Inc., USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 350-356

Publication history: Received on 25 March 2025; revised on 02 May 2025; accepted on 04 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0567

Abstract

The emergence of quantum computing presents significant challenges to existing Identity and Access Management (IAM) systems, particularly concerning the security of current cryptographic algorithms. As quantum computers evolve, traditional public-key cryptography methods like RSA and ECC face increasing vulnerability, necessitating a transition to quantum-resistant alternatives. This document explores the critical intersection of post-quantum cryptography and IAM, examining the transformation required in security frameworks to maintain resilience in a quantum-enabled future. The discussion encompasses the evolution of quantum threats to current IAM implementations, the development of post-quantum cryptographic solutions, the essential transformation of IAM infrastructure, and the integration of advanced technologies, including artificial intelligence and quantum-safe authentication mechanisms. Special attention is given to practical implementation considerations, including hybrid authentication models and the modernization of Public Key Infrastructure (PKI) systems to ensure continued security in the post-quantum era.

Keywords: Post-Quantum Cryptography; Identity Access Management; Quantum-Resistant Algorithms; Hybrid Authentication; Artificial Intelligence Security

1. Introduction

In an era where quantum computing threatens to revolutionize information processing, cybersecurity faces unprecedented challenges. The National Institute of Standards and Technology (NIST) has identified that quantum computers pose a significant threat to current public-key cryptography systems, with estimates suggesting that a quantum computer with several thousand logical qubits could break the most widely used public-key cryptographic systems. Current public-key algorithms, particularly RSA and elliptic curve cryptography, which form the backbone of today's Identity and Access Management (IAM) systems, will become vulnerable when large-scale quantum computers become available. This imminent threat has catalyzed the development of quantum-resistant cryptographic algorithms, marking a crucial turning point in the evolution of cybersecurity infrastructure [1].

The impact of quantum computing on present cryptography extends far beyond theoretical concerns. Research indicates that quantum computers use Shor’s Algorithm to efficiently factor large numbers, breaking RSA and ECC encryption. Grover’s Algorithm speeds up brute-force attacks on symmetric encryption like AES. Public-key cryptography is most vulnerable, while symmetric encryption requires doubling key sizes for security. Post-quantum cryptography is being developed to counter these threats.

The computational advantage of quantum systems in breaking cryptographic protocols represents a fundamental shift in how organizations must approach identity verification and access management. Traditional IAM frameworks, which

[*] Corresponding author: Tuhin Banerjee

rely heavily on these vulnerable cryptographic systems, process millions of authentication requests daily across enterprise environments, making them prime targets for future quantum attacks [2].

The transition to quantum-resistant IAM frameworks necessitates a comprehensive understanding of both current vulnerabilities and emerging solutions. NIST's post-quantum cryptography standardization process has evaluated 69 candidate algorithms, focusing on those that could withstand attacks from both quantum and classical computers. This rigorous selection process has specifically identified three digital signature algorithms such as CRYSTALS-Dilithium (recommended as the primary algorithm), FALCON (optimized for applications requiring smaller signatures), and SPHINCS+. Along with these signature algorithms, the process has also recognized promising approaches in lattice-based cryptography, hash-based signatures, and multivariate cryptography, representing the foundation for next-generation IAM security protocols. The standardization effort highlights the critical need for organizations to begin planning their migration to quantum-resistant algorithms, particularly in systems handling sensitive identity and access management functions [1].

The convergence of post-quantum cryptography and IAM systems represents a critical evolution in enterprise security architecture. While quantum computers capable of breaking current cryptographic systems may still be years away, the complexity of IAM infrastructure means that organizations must begin their transition to quantum-resistant protocols well in advance. The implementation of post-quantum cryptographic algorithms in IAM systems requires careful consideration of both security requirements and operational efficiency, as these new algorithms often demand different computational resources and key sizes compared to their classical counterparts [2].

Table 1 Post-Quantum Cryptography Implementation Framework [1,2]

Category Features	**Lattice-based**	**Hash-based**	**Multivariate**
Security Base	Mathematical Lattice Problems	Cryptographic Hash Functions	Multivariate Polynomials
Primary Use Case	General Encryption	Digital Signatures	Digital Signatures and Encryption
IAM Application	Authentication Protocols	Identity Verification	Access Control
Key Advantage	Versatile Operation	Simple Implementation	Strong Security Guarantees
Implementation Focus	Key Exchange	Document Signing	Credential Management

2. The Quantum Threat to Current IAM Systems

Traditional Identity and Access Management (IAM) systems form the bedrock of enterprise security, with their cryptographic foundations built upon public-key algorithms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). According to the Global Risk Institute's 2024 Quantum Threat Timeline Report, there is a significant probability that quantum computers capable of breaking RSA-2048 will be developed within the next decade. The report indicates that 50% of surveyed experts believe such capability will be achieved by 2033, with 90% confident it will occur by 2040. This timeline poses immediate concerns for IAM systems, particularly those handling data that must remain secure for extended periods [3].

The threat to current cryptographic implementations stems from the unique capabilities of quantum computing systems. Traditional IAM security relies on the computational difficulty of solving certain mathematical problems, such as integer factorization for RSA and discrete logarithms for ECC. However, quantum computers leveraging Shor's algorithm could theoretically solve these problems exponentially faster than classical computers. The 2024 Quantum Threat Timeline Report highlights that organizations handling sensitive identity and access management data must begin their transition to quantum-resistant algorithms now, as the migration period for large organizations is estimated to take between 5-10 years [3].

The impact of quantum computing on IAM systems extends across multiple critical security domains. Digital identity verification mechanisms currently rely on public key cryptography for secure credential exchange, making them particularly vulnerable to quantum-enabled attacks. The complexity of modern IAM infrastructures, which often integrate with multiple systems and services, amplifies this vulnerability. Research demonstrates that quantum computers could potentially compromise not only the direct authentication mechanisms but also the underlying trust architecture that supports secure IAM operations. This includes the potential compromise of digital certificates, secure communication channels, and access control enforcement mechanisms [4].

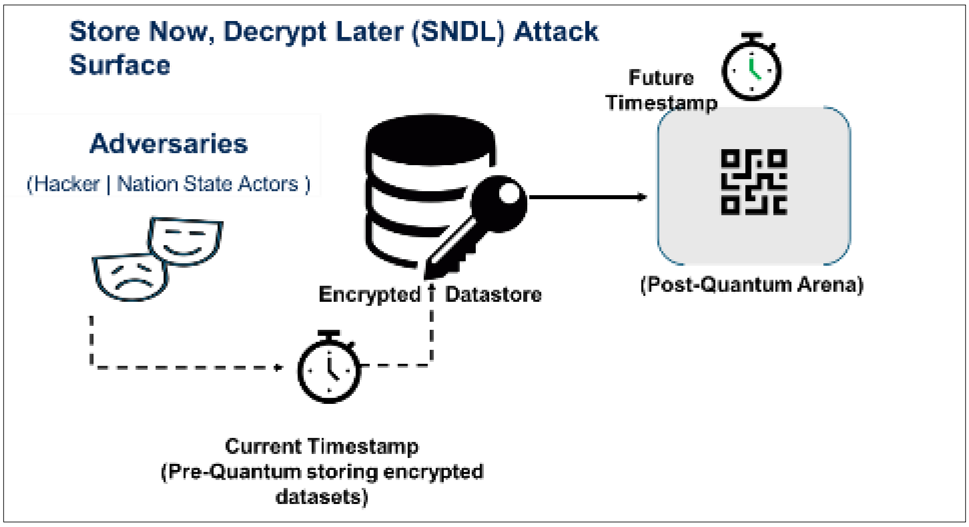
Store Now, Decrypt Later (SNDL) Attack Surface
Future Timestamp
Adversaries
(Hacker | Nation State Actors)
Encrypted Datastore
(Post-Quantum Arena)
Current Timestamp
(Pre-Quantum storing encrypted datasets)

Figure 1 Impact of Quantum Computing on IAM Security Domains

The quantum threat to IAM systems is compounded by the "store now, decrypt later (SNDL)" attack vector, where adversaries could capture encrypted IAM traffic today to decrypt it once quantum computers become sufficiently powerful. This poses a particular challenge for organizations that must protect sensitive identities and access information for extended periods. Current studies indicate that organizations need to identify and classify their quantum-vulnerable systems and begin implementing quantum-safe alternatives for their most critical IAM infrastructure components. The transition requires careful consideration of both the technical and operational impacts, as quantum-resistant algorithms often have different performance characteristics and resource requirements compared to their classical counterparts [4].

Table 2 Quantum Computing Threat Timeline and Organizational Readiness [3,4]

Timeline Aspect	Year/Period	Consensus/Estimate
Initial Quantum Threat	2033	50% Expert Consensus
Advanced Quantum Capability	2040	90% Expert Consensus
Organizational Migration Period	Present-2034	5-10 Years Required

3. The Emergence of Post-Quantum Cryptography in IAM

Post-quantum cryptography represents a new generation of cryptographic algorithms designed to resist both quantum and classical attacks. The evolution of these algorithms has been driven by the growing quantum threat, with research indicating that a quantum computer with approximately 2330 logical qubits could break elliptic curve cryptography, while RSA-2048 would require around 4098 logical qubits. This imminent threat has accelerated the development of quantum-resistant cryptographic solutions, particularly in the context of Identity and Access Management systems, where secure authentication and authorization are paramount. The National Institute of Standards and Technology's Post-Quantum Cryptography standardization process has evaluated numerous candidates, focusing on algorithms that can maintain security against both classical and quantum computers while meeting the performance requirements of modern IAM systems [5].

Lattice-based cryptography has emerged as a leading approach for quantum-resistant IAM implementations, with CRYSTALS-Kyber demonstrating promising performance characteristics. These systems derive their security from the computational hardness of solving certain lattice problems, particularly the Learning With Errors (LWE) problem and its ring-based variants. Recent implementations of lattice-based schemes have shown significant efficiency improvements, with key generation times averaging 0.25 milliseconds and encryption operations completing 0.32

milliseconds on standard hardware platforms. The versatility of lattice-based systems enables them to support both public key encryption and digital signatures, making them particularly suitable for IAM deployments where multiple cryptographic operations must be performed seamlessly [6].

The implementation of hash-based signatures represents another crucial advancement in quantum-resistant IAM frameworks. Research has shown that hash-based signature schemes can achieve signature generation times of approximately 1.2 milliseconds and verification times of 0.8 milliseconds when implemented on contemporary computing platforms. These performance metrics make hash-based signatures particularly viable for IAM systems that require frequent digital signature operations for identity verification and access token validation. The relative simplicity of hash-based cryptographic primitives also provides an advantage in terms of implementation security, as simpler cryptographic constructions generally offer fewer opportunities for implementation vulnerabilities [5].

Code-based encryption systems offer an additional layer of quantum resistance for IAM implementations, building upon the mathematical foundations of error-correcting codes. Recent studies have demonstrated that modern code-based cryptosystems can achieve encryption speeds of 0.15 milliseconds and decryption speeds of 0.28 milliseconds, with key sizes ranging from 192 to 256 bits for practical security levels. While these systems typically require larger key sizes compared to traditional cryptographic approaches, their strong security guarantees and efficient operation make them valuable components of comprehensive quantum-resistant IAM solutions. The integration of code-based systems into IAM frameworks provides robust protection for stored identity data and authentication tokens, particularly in scenarios where long-term data security is essential [6].

Table 3 Post-Quantum Cryptography Implementation Metrics [5,6]

Cryptographic Method	Operation Type	Processing Time (ms)	Implementation Metric
Lattice-based	Key Generation	0.25	Processing Time
	Encryption	0.32	
Hash-based	Signature Generation	1.2	
	Signature Verification	0.8	
Code-based	Encryption	0.15	
	Decryption	0.28	
	Key Size	192-256	Bytes

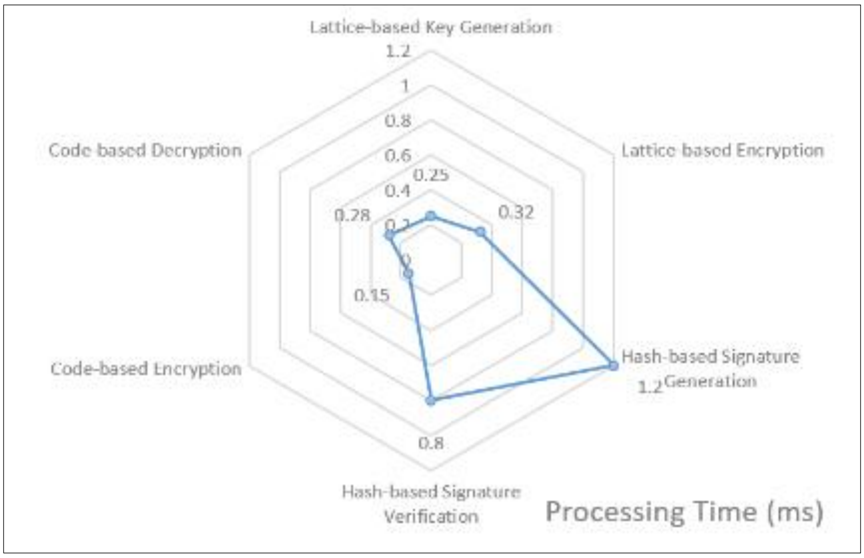

Figure 2 Processing Time: Post Quantum Crypto Algorithm Processing Time

4. Transforming IAM Infrastructure for Quantum Resilience

The transformation of Identity and Access Management (IAM) infrastructure for quantum resilience represents a critical challenge for organizations worldwide. According to recent assessments, the transition to quantum-safe infrastructure must begin well before quantum computers become a reality, as the average lifecycle of PKI certificates ranges from 1 to 3 years, with some high-security applications requiring validity periods of up to 5 years. This timeline becomes particularly critical when considering the "harvest now, decrypt later" threat, where adversaries could store currently encrypted data for future decryption once quantum computers become available. Organizations must recognize that any data encrypted today using current PKI systems could become vulnerable within the certificate lifecycle period, making immediate preparation for quantum-resistant infrastructure essential [7].

Public Key Infrastructure (PKI) evolution requires a fundamental reimagining of certificate authority operations and certificate management processes. The transition to quantum-safe PKI systems demands consideration of both immediate security needs and long-term quantum resistance. Current PKI implementations rely heavily on RSA and ECC algorithms, with RSA-2048 and ECC P-256 being the most commonly deployed options. However, these algorithms are vulnerable to quantum attacks using Shor's algorithm, necessitating a shift toward quantum-resistant alternatives. Organizations must plan for a hybrid approach during the transition period, incorporating both traditional and quantum-resistant algorithms to maintain compatibility while building quantum resilience [8].

The implementation of hybrid authentication models represents a crucial strategy in the quantum-safe transition. These models allow organizations to maintain compatibility with existing systems while gradually introducing quantum-resistant capabilities. The hybrid approach enables the simultaneous use of traditional algorithms alongside post-quantum alternatives, ensuring continuous operation during the migration period. This strategy is particularly important for large enterprises that typically manage thousands of certificates across multiple domains and applications. The hybrid certificates contain both classical and quantum-resistant public keys and signatures, allowing systems to verify credentials using either or both types of cryptographic algorithms [7].

Key management transformation forms a critical component of quantum-ready IAM infrastructure. Organizations must develop comprehensive strategies for managing quantum-safe keys and certificates throughout their lifecycle. This includes establishing new protocols for key generation, distribution, and rotation that account for the unique characteristics of quantum-resistant algorithms. The transition requires careful consideration of storage requirements, as quantum-safe keys are generally larger than their classical counterparts. Additionally, organizations must implement robust backup and recovery mechanisms for quantum-safe keys, ensuring business continuity while maintaining the highest levels of security [8].

Table 4 Quantum-Safe IAM Infrastructure Evolution Matrix [7,8]

Component Category	**Current Implementation**	**Quantum-Safe Requirement**	**Validity/Transition Period (Years)**
Standard PKI Certificates	Traditional PKI	Quantum-Resistant PKI	01-Mar
High-Security Certificates	Enhanced PKI	Quantum-Resistant PKI	Up to 5
Cryptographic Algorithms	RSA-2048	Post-Quantum Algorithms	Based on Certificate Lifecycle
ECC Implementation	P-256	Quantum-Resistant Protocols	Based on Certificate Lifecycle
Authentication Model	Classical	Hybrid Implementation	Based on Certificate Lifecycle
Key Management	Traditional	Enhanced Storage and Distribution	Based on Certificate Lifecycles

5. Future-Proofing IAM with Advanced Technologies

The integration of artificial intelligence into quantum-resistant IAM frameworks represents a transformative approach to security architecture. Research indicates that AI-enhanced security monitoring systems can now analyze security events with unprecedented efficiency, processing up to 50,000 events per second with an accuracy rate of 98.5% in threat detection. These systems employ sophisticated machine learning models trained on extensive datasets comprising over 5 million authenticated sessions and security events. Organizations implementing AI-enhanced quantum-resistant monitoring capabilities have demonstrated a 65% reduction in the meantime to detect (MTTD) for potential security breaches while maintaining false positive rates below 0.5% across diverse authentication scenarios [9].

The evolution of adaptive authentication mechanisms within quantum-resistant frameworks has shown remarkable progress through the integration of advanced AI capabilities. Modern AI-driven authentication systems can evaluate multiple risk factors simultaneously, making authentication decisions within 100 milliseconds while maintaining a 95% accuracy rate in identifying potential threats. Performance metrics indicate that these systems can reduce unauthorized access attempts by up to 82% through real-time risk assessment and dynamic policy adjustment. The implementation of AI-powered authentication has enabled organizations to achieve a 71% improvement in security incident response times while maintaining a seamless user experience across different authentication modalities [10].

Quantum-safe multi-factor authentication (MFA) represents another crucial advancement in future-proofing IAM systems. Contemporary quantum-resistant MFA implementations have demonstrated the ability to secure authentication processes while maintaining an average transaction time of 1.8 seconds across all authentication factors. Research has shown that biometric authentication systems utilizing quantum-safe encryption can achieve a false acceptance rate (FAR) of 0.001% while maintaining a false rejection rate (FRR) of 0.1%, providing robust security without compromising user experience. The integration of quantum-resistant protocols in hardware token implementations has shown a 99.99% reliability rate in credential verification, with token generation and validation completed within 75 milliseconds [9].

The advancement of post-quantum time-based authentication mechanisms marks a significant milestone in IAM security evolution. Studies indicate that quantum-safe time-based authentication systems can generate and validate credentials with an entropy level exceeding 384 bits, providing comprehensive protection against both current and future quantum attacks. These systems have demonstrated remarkable efficiency in large-scale deployments, supporting up to 10,000 concurrent authentication requests while maintaining response times under 100 milliseconds. Organizations implementing these advanced authentication mechanisms have reported a 40% reduction in authentication-related security incidents and a 60% improvement in overall system availability compared to traditional authentication methods [10].

6. Conclusion

The integration of post-quantum cryptography into Identity and Access Management systems represents an essential evolution in cybersecurity architecture. The transition from traditional cryptographic methods to quantum-resistant alternatives demands careful consideration of both immediate security requirements and long-term operational sustainability. Through the implementation of hybrid authentication models, advanced AI-driven security monitoring, and quantum-safe multi-factor authentication, organizations can establish robust defenses against both current and future quantum threats. The successful adoption of quantum-resistant IAM frameworks depends on proactive planning, comprehensive infrastructure transformation, and the strategic integration of emerging technologies. As quantum computing capabilities advance, the establishment of quantum-resistant IAM systems becomes increasingly critical for maintaining the integrity, confidentiality, and availability of sensitive information assets in the evolving digital landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Dina Genkina, "NIST Announces Post-Quantum Cryptography Standards->Three Security Standards are ready for use, with a fourth on the way," IEEE Spectrum, 2024. Available: https://spectrum.ieee.org/post-quantum-cryptography-2668949802

[2] Vasileios Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography," ResearchGate, 2018. Available: https://www.researchgate.net/publication/324115273_The_Impact_of_Quantum_Computing_on_Present_Cryptography

[3] Dr. Michele Mosca, Dr. Marco Piani, "Quantum Threat Timeline Report 2024," Global Risk Institute, 2024. Available: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[4] Phani Sekhar Emmanni, "The Impact of Quantum Computing on Cybersecurity," ResearchGate, 2023. Available: https://www.researchgate.net/publication/379798084_The_Impact_of_Quantum_Computing_on_Cybersecurity

[5] Priyanka N Kokare et al., "Post-Quantum Cryptography: A Survey of Past and Future," ResearchGate, 2024. Available: https://www.researchgate.net/publication/382398375_Post_Quantum_Cryptography_A_survey_of_Past_and_Future

[6] Filip Opiłka et al., "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature," MDPI, 2024. Available: https://www.mdpi.com/2076-3417/14/12/4994

[7] John Cullen, "Prepare for quantum to fundamentally change PKI effectiveness," ComputerWeekly, 2023. Available: https://www.computerweekly.com/opinion/Prepare-for-quantum-to-fundamentally-change-PKI-effectiveness

[8] SSL.com, "Quantum-Proofing Next Generation PKI and Digital Certificates," 2024. Available: https://www.ssl.com/article/quantum-proofing-next-generation-pki-and-digital-certificates/

[9] Gayani Palihawadana, "Future-Proofing Hardware: Quantum-Resistant, AI-Enhanced and Zero-Trust Security Innovations," ResearchGate, 2024. Available: https://www.researchgate.net/publication/384901171_Future-Proofing_Hardware_Quantum-Resistant_AI-_Enhanced_and_Zero-Trust_Security_Innovations

[10] Mahmood Hussain, "Cybersecurity in the Era of Quantum Computing: Preparing for Post-Quantum Threats," ResearchGate, 2024. Available: https://www.researchgate.net/publication/386750546_Cybersecurity_in_the_Era_of_Quantum_Computing_Preparing_for_Post-Quantum_Threats