Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Applications of Quantum Computing in Cybersecurity and Cryptographic Systems

C Swathi[1], Repaka Karunasree[2], Prasanna Mathi[3]

[1]Assistant Professor, Department of CSE, Aurora Deemed to be University, Hyderabad
[2]Assistant Professor, Department of CSE, Aurora Deemed to be University, Hyderabad
[3]Assistant Professor, Department of CSE, Princeton Institute of Engineering and Technology for Women, Hyderabad

Abstract

Quantum computing is introducing a significant transformation in cybersecurity by creating both new security capabilities and new threats to established cryptographic systems. Large-scale fault-tolerant quantum computers could undermine widely deployed public-key cryptographic mechanisms through quantum algorithms such as Shor's algorithm, while Grover's algorithm provides a quadratic search advantage that affects the security analysis of symmetric cryptography. At the same time, quantum technologies offer defensive mechanisms including quantum key distribution, quantum random number generation, quantum-safe authentication, and advanced security architectures. Post-Quantum Cryptography (PQC) has therefore emerged as an essential strategy for protecting conventional communication systems against future quantum attacks. In August 2024, NIST finalized three principal PQC standards: ML-KEM, ML-DSA, and SLH-DSA, and in March 2025 selected HQC as an additional key-establishment algorithm for standardization. This article examines the applications of quantum computing in cybersecurity and cryptographic systems, emphasizing quantum threats, cryptanalysis, quantum key distribution, quantum-safe cryptography, secure communications, intrusion detection, random number generation, and migration strategies. Graph-ready comparative datasets are provided for cryptographic vulnerability, cybersecurity applications, implementation challenges, and quantum-resistant protection mechanisms. The analysis shows that quantum computing should be considered simultaneously as a future attack capability and as a technology that can contribute to stronger security architectures.

Correspondence

C. Swathi

Assistant Professor, Department of CSE, Aurora Deemed to be University, Hyderabad

- Received Date: 30 Aug 2026
- Accepted Date: 20 Sep 2026
- Publication Date: 26 Sep 2026

Introduction

Cybersecurity depends heavily on cryptographic mechanisms that protect the confidentiality, integrity, authenticity, and non-repudiation of digital information. Public-key algorithms such as RSA, Diffie–Hellman, and elliptic-curve cryptography support key establishment, digital signatures, certificate infrastructures, secure web communication, virtual private networks, software authentication, and many other security services. Symmetric algorithms such as AES are used extensively for high-speed data encryption, while cryptographic hash functions support integrity checking and authentication protocols. The security of these systems depends on mathematical problems and computational assumptions that are considered difficult for conventional computers. The development of sufficiently capable quantum computers could change these assumptions substantially. [1–3]

Quantum computers use quantum bits and operations based on quantum-mechanical principles. Unlike classical bits, quantum states can represent superpositions of computational states, and multi-qubit systems can exploit entanglement and interference. These properties do not make every computation faster, but they enable specific algorithms with computational properties different from those of classical algorithms. For cybersecurity, the most important consequence is the ability of quantum algorithms to affect cryptographic problems based on integer factorization and discrete logarithms. Shor's algorithm provides a polynomial-time quantum approach to these problems, which means that sufficiently large fault-tolerant quantum computers could threaten the foundations of RSA, Diffie–Hellman, and elliptic-curve public-key systems. [1,4]

Symmetric cryptography faces a different quantum effect. Grover's algorithm provides a quadratic reduction in the number of operations needed for unstructured search. Consequently, the effective security margin of a symmetric key can be reduced when considering a sufficiently powerful quantum adversary. NIST notes, however, that practical quantum attacks based on Grover's algorithm face substantial hardware and parallelization limitations. Therefore, the quantum impact on AES is fundamentally different from the direct vulnerability of widely

Citation: Swathi C, Repaka K, Mathi P. Applications of Quantum Computing in Cybersecurity and Cryptographic Systems. GJEIIR. 2026;6(6):234.

used public-key systems to Shor's algorithm. Current guidance continues to support AES key sizes, with AES-256 providing a particularly large security margin against generic quantum search attacks. [5]

The cybersecurity implications extend beyond cryptographic key recovery. A future quantum adversary could potentially decrypt captured encrypted communications after obtaining the necessary private keys, which motivates concern about "harvest now, decrypt later" strategies for information that must remain confidential for many years. Long-lived government, healthcare, financial, defense, research, and industrial information may therefore require protection before cryptographically relevant quantum computers become available. The resulting migration problem is substantial because public-key cryptography is embedded across certificates, operating systems, network protocols, hardware devices, software libraries, cloud services, identity systems, and industrial infrastructure. [2,6]

Quantum technologies can also be used defensively. Quantum Key Distribution uses quantum states to establish secret keys between legitimate parties and can provide security properties based on quantum physics. Quantum Random Number Generators exploit quantum measurement processes to produce random numbers that can support cryptographic applications. Quantum communication networks may provide new mechanisms for secure information exchange, while quantum technologies can also contribute to authentication, secure computation, and security monitoring. These technologies should not, however, be treated as automatic replacements for conventional security mechanisms because practical QKD systems introduce requirements involving specialized hardware, trusted components, network availability, authentication, and implementation security. [7,8]

A major defensive strategy is Post-Quantum Cryptography, which develops classical cryptographic algorithms designed to resist attacks from both classical and quantum computers. NIST finalized FIPS 203, FIPS 204, and FIPS 205 in August 2024, defining ML-KEM for key establishment, ML-DSA for digital signatures, and SLH-DSA as a hash-based digital-signature standard. In March 2025, NIST selected HQC as an additional key-establishment algorithm for standardization, intended as a backup to ML-KEM and based on a different mathematical construction. These developments mark a transition from theoretical preparation toward practical migration and deployment. [6,9]

Literature Review

The relationship between quantum computing and cryptography was established prominently by Shor's 1994 quantum algorithm for factoring and discrete logarithms. The importance of this development comes from the role that these mathematical problems play in public-key cryptography. RSA relies on the difficulty of factoring large composite integers, while Diffie–Hellman-type systems and elliptic-curve systems rely on discrete-logarithm assumptions. A sufficiently capable fault-tolerant quantum computer running an appropriate implementation of Shor's algorithm could solve these problems much more efficiently than known classical methods. Consequently, public-key cryptography represents one of the most significant long-term cybersecurity consequences of quantum computing. [1,4]

Grover's 1996 quantum search algorithm created a second major connection between quantum computing and cryptographic analysis. In contrast to Shor's direct impact on public-key mathematical foundations, Grover affects brute-force searches over large key spaces. The theoretical quadratic improvement means that doubling the classical key length can approximately restore a comparable generic quantum search margin under an idealized model. Practical implementation remains considerably more demanding, particularly because quantum attacks require large numbers of logical operations and effective control over quantum hardware. NIST therefore distinguishes the quantum threat to symmetric cryptography from the much more disruptive threat to public-key cryptosystems. [5]

Quantum Key Distribution has developed as a major research area in quantum cybersecurity. The BB84 protocol and subsequent QKD methods demonstrate how quantum states can be used for secret-key establishment while allowing certain forms of eavesdropping to be detectable through changes in observed quantum statistics. More advanced research has investigated device-independent QKD, satellite-based distribution, quantum repeaters, integrated photonic components, and multi-user quantum networks. Nevertheless, QKD is not equivalent to an end-to-end secure communication system by itself. Authentication, classical network infrastructure, implementation security, key management, and device trust remain necessary. Practical QKD networks also experience distance, loss, cost, and denial-of-service considerations. [7,10]

Quantum random number generation represents another important application. Cryptographic security depends strongly on high-quality randomness for keys, initialization vectors, nonces, salts, and security protocols. Classical pseudorandom generators can provide excellent security when correctly designed and seeded, but quantum random-number generators can derive randomness from fundamentally probabilistic quantum processes. Research has investigated optical, photonic, semiconductor, and integrated implementations capable of producing random bit streams. The security and usefulness of such systems depend on entropy estimation, device characterization, post-processing, and protection against implementation-level attacks rather than merely asserting that the underlying physical process is quantum. [8]

Post-Quantum Cryptography has consequently become the main practical migration strategy for protecting conventional information systems. PQC algorithms do not require a quantum communication channel. Instead, they are designed around mathematical problems believed to remain difficult for quantum computers. NIST's 2024 standards include lattice-based ML-KEM for key establishment, lattice-based ML-DSA for digital signatures, and hash-based SLH-DSA for digital signatures. In 2025, HQC was selected for standardization as a second KEM based on error-correcting codes, providing mathematical diversity in the event that weaknesses emerge in another algorithm family. [6,9,11]

The migration literature emphasizes that post-quantum transition is not simply a matter of replacing one cryptographic library with another. Organizations must first identify where vulnerable public-key algorithms are used, including applications, certificates, firmware, communication protocols, hardware modules, cloud systems, and embedded devices. Cryptographic agility is therefore becoming an important engineering principle. Systems should be designed so that algorithms and parameters can be updated without redesigning the complete application. Hybrid cryptographic mechanisms, in which classical and post-quantum schemes are used together during transition, have also been investigated to reduce migration risk and provide resilience against weaknesses in either component. [6,12]

Recent systematic research has expanded the discussion toward cybersecurity systems beyond cryptographic protection. Quantum computing may affect intrusion detection, optimization of security configurations, secure communication, random-number generation, blockchain systems, identity management, privacy-preserving computation, and security analytics. Hybrid quantum-classical models are being studied for intrusion detection because quantum circuits can potentially serve as feature transformations or classification components. However, many such applications remain experimental, and current hardware limitations prevent broad conclusions about production-scale quantum cybersecurity systems. [13]

A 2025 systematic review of quantum computing and cybersecurity found that the literature is dominated by work on post-quantum solutions, while emerging threats and implementation barriers remain important research categories. More recent work in 2026 has emphasized practical quantum-key-distribution networks and hybrid quantum-classical security architectures. These studies highlight a common conclusion: quantum cybersecurity requires coordinated development across cryptography, hardware engineering, communication networks, software architecture, and security operations rather than dependence on a single technology. [13–15]

Methodology

This article adopts a structured review methodology to examine applications of quantum computing in cybersecurity and cryptographic systems. The literature was organized into four major categories: quantum-enabled attacks, quantum-enabled defensive technologies, post-quantum cryptographic systems, and quantum-enhanced cybersecurity applications. Foundational quantum algorithms, international cryptographic standards, recent systematic reviews, quantum communication research, and current migration guidance were considered to establish a broad technical framework.

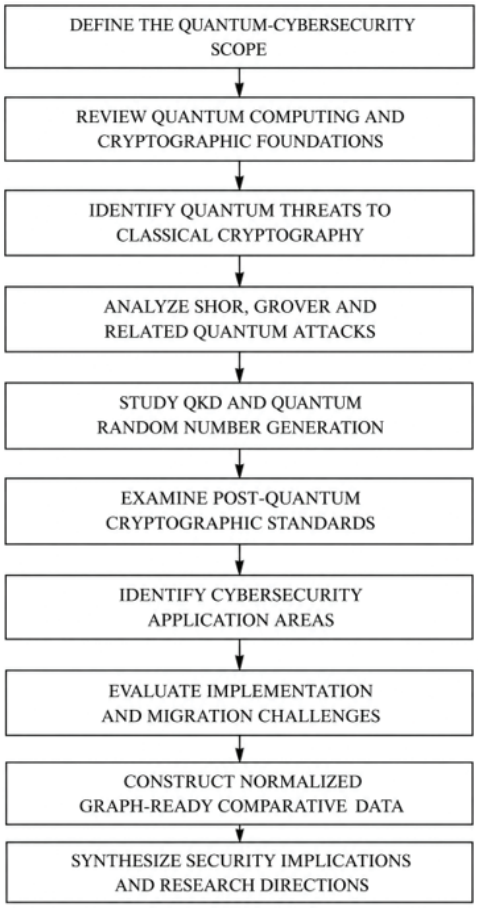
The first stage of the methodology identifies the cryptographic primitives affected by quantum algorithms. Public-key mechanisms are analyzed primarily with respect to Shor-type attacks, while symmetric cryptography and hash functions are analyzed with respect to quantum search and related generic attacks. The second stage examines technologies that can strengthen cybersecurity, including QKD and QRNG. The third stage investigates PQC mechanisms and migration strategies. The fourth stage considers emerging cybersecurity applications such as quantum-assisted intrusion detection, secure communication, blockchain protection, and quantum-aware security monitoring.

For basic comparative evaluation, the following security-performance measure is used:

Security Retention (%) = (Effective Quantum-Resistant Security / Reference Security) × 100

The numerical values presented later in the article are normalized or illustrative comparative values intended for graph generation. They do not represent the result of a single laboratory experiment or one universal benchmark. They are constructed to translate qualitative differences identified in the literature into consistent numerical visualizations.

The final analysis compares the security impact, application potential, implementation maturity, and major obstacles associated with quantum computing and quantum-resistant cybersecurity. Particular attention is given to the distinction between technologies that use quantum physics for security and technologies that remain classical but are designed to resist quantum attacks..



Methodology flow chart

Implementation and Results

The implementation framework compares current cryptographic mechanisms, quantum attacks, defensive quantum technologies, and post-quantum protection approaches. The objective is to show how the security landscape changes when quantum computing is included in the threat model. The comparison uses numerical indices that can be directly plotted as graphs while preserving the distinction between established facts and illustrative evaluation values.

Quantum Impact On Cryptographic Systems

The first comparison evaluates major cryptographic primitives according to their relative quantum exposure. RSA, Diffie–Hellman, and elliptic-curve cryptography are strongly affected by Shor's algorithm because their security is based on mathematical problems for which efficient quantum algorithms are known in principle. AES and hash functions experience a different form of quantum pressure because generic search or collision-related quantum techniques do not produce the same complete cryptographic collapse. Thus, security planning must distinguish between public-key and symmetric cryptographic technologies rather than treating all algorithms as equally vulnerable. [4,5].

Table 1 shows the strong difference between asymmetric and symmetric cryptography under the quantum threat model. RSA, Diffie–Hellman, and ECC receive very high quantum-exposure values because Shor's algorithm directly targets their underlying mathematical assumptions. AES-128 receives a substantially lower exposure value because Grover's algorithm provides a

Table 1: Normalized quantum impact on major cryptographic systems

Crypto-graphic System	Classical Security Index	Quantum Exposure Index	Migration Priority	Quantum-Resistant Potential
RSA	92	97	98	18
Diffie–Hellman	91	96	97	20
ECC	94	98	99	17
AES-128	88	48	45	76
AES-256	96	27	25	94

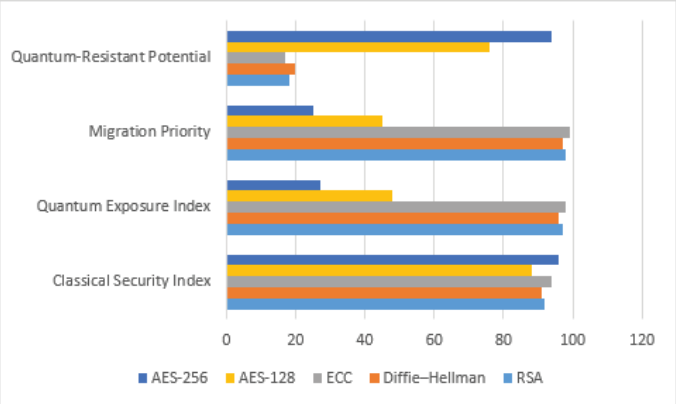


Fig 1: *Grouped bar graph comparing quantum cryptographic exposure*

quadratic rather than an exponential attack advantage under the idealized model. AES-256 receives an even lower exposure value because its larger key space provides a greater margin against generic quantum search. The migration-priority values reflect the strategic emphasis generally placed on replacing quantum-vulnerable public-key mechanisms.

Fig 1 should be created as a grouped bar graph with the five cryptographic systems on the horizontal axis and the four numerical indicators on the vertical axis. The graph can directly use the values 92, 97, 98, 18 for RSA; 91, 96, 97, 20 for Diffie–Hellman; 94, 98, 99, 17 for ECC; 88, 48, 45, 76 for AES-128; and 96, 27, 25, 94 for AES-256. This makes the contrast between quantum-vulnerable public-key systems and comparatively resilient symmetric systems immediately visible.

The analysis does not imply that AES is immune to quantum attacks. Grover's algorithm changes the theoretical complexity of exhaustive search, and other quantum cryptanalytic techniques may influence future security assessments. However, NIST currently recognizes that practical limitations reduce the expected usefulness of Grover-based attacks, particularly because fully achieving the quadratic speedup requires highly sequential quantum computation. This is why public-key migration remains a particularly urgent component of quantum-readiness planning. [5]

Applications of Quantum Computing in Cybersecurity

Quantum computing can influence cybersecurity beyond direct cryptanalysis. Quantum communication provides new mechanisms for secret-key distribution, quantum random-number generation can contribute high-quality entropy, and quantum optimization may eventually assist selected security-management problems. Hybrid quantum-classical approaches

Table 2: *Normalized cybersecurity applications of quantum computing*

Application	Security Impact	Technical Maturity	Scalability Index	Research Potential
Quantum Key Distribution	92	72	58	91
Quantum Random Number Generation	88	79	70	86
Quantum-Assisted Intrusion Detection	74	48	42	88
Quantum-Secure Communications	90	69	55	93
Quantum Optimization for Security	68	41	38	82

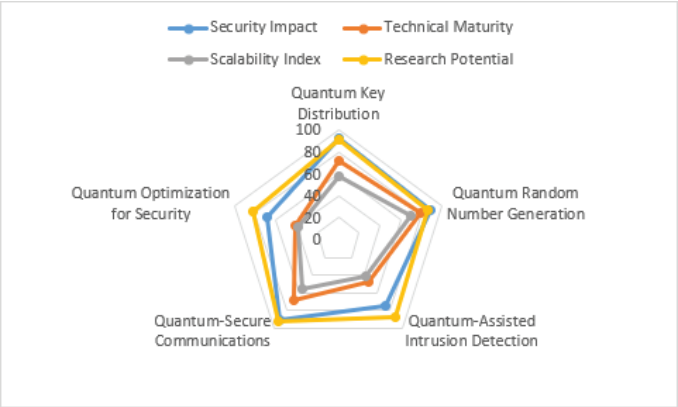


Fig 2: *Radar chart comparing quantum cybersecurity applications*

can also be investigated for anomaly detection and intrusion detection. Quantum computing may therefore affect multiple layers of cybersecurity, including cryptographic protection, identity, communications, monitoring, and security analytics.

QKD receives a high security-impact value because it uses quantum properties for key establishment and can provide detection mechanisms for particular classes of interception. QRNG receives a strong maturity value because practical quantum random-number generation has progressed beyond purely theoretical proposals. Quantum-assisted intrusion detection and security optimization receive lower maturity and scalability values because current quantum hardware and hybrid execution overhead limit broad deployment. Their research-potential values are nevertheless high because quantum feature processing, optimization, and hybrid learning continue to be active research areas.

Fig 2 should be constructed as a radar chart using the four indicators in Table 2. Each application is represented using Security Impact, Technical Maturity, Scalability Index, and Research Potential as the four axes. This graph will show that some applications have strong security potential but comparatively lower scalability, while others have progressed further toward practical implementation. The radar presentation is particularly useful because cybersecurity applications are multidimensional and cannot be meaningfully characterized using a single performance value.

QKD should be distinguished clearly from PQC. QKD changes how keys are distributed by using quantum communication,

whereas PQC changes the underlying cryptographic algorithms while remaining compatible with conventional computing and network infrastructure. NIST identifies PQC as a principal route for protecting conventional systems against future quantum computers, while the NSA has stated that QKD involves significant operational and implementation limitations and currently does not recommend it for protecting National Security Systems unless those limitations are overcome. [6,8]

QRNG represents a complementary technology because cryptographic protocols depend fundamentally on unpredictable values. Quantum sources can generate physical randomness, but the output still needs appropriate entropy validation, conditioning, health monitoring, and protection against implementation faults. Consequently, the security value of quantum randomness depends on the full system architecture rather than on the quantum source alone. This principle also applies to QKD: security claims based on ideal quantum protocols do not eliminate practical vulnerabilities in detectors, transmitters, control systems, authentication, or network operations. [7,10]

Implementation Challenges

Quantum cybersecurity technologies face several implementation challenges. Quantum hardware remains sensitive to noise, device imperfections, limited coherence, and connectivity constraints. QKD requires specialized optical or quantum communication infrastructure and can experience losses over distance. PQC introduces larger keys, signatures, ciphertexts, or computational requirements in some configurations, which may affect bandwidth, storage, embedded systems, and constrained devices. Legacy systems may also contain cryptographic dependencies that are difficult to discover. Therefore, quantum-readiness involves both technological migration and organizational cryptographic inventory management. [6,12]

Table 3: *Normalized implementation challenges for quantum cybersecurity*

Challenge	Security Risk	Implementation Cost	Scalability Difficulty	Urgency Index
Legacy Cryptographic Dependencies	89	86	91	96
Quantum Hardware Limitations	84	94	92	81
PQC Integration Overhead	72	78	76	91
QKD Infrastructure Requirements	80	96	88	73
Cryptographic Inventory Gaps	87	74	85	94

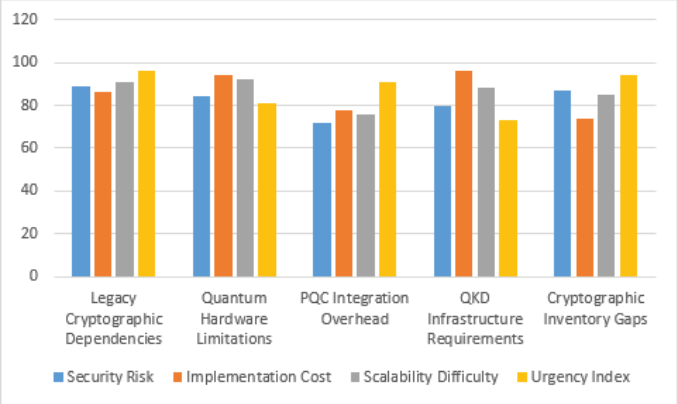


Fig 3: *Grouped vertical bar graph comparing implementation challenges*

Table 3 is designed for a grouped vertical bar graph in which each challenge is represented by Security Risk, Implementation Cost, Scalability Difficulty, and Urgency Index. Legacy Cryptographic Dependencies have a high urgency value because systems that continue to depend on RSA, ECC, or related vulnerable public-key mechanisms may require substantial migration planning. QKD Infrastructure Requirements receive the highest implementation-cost value because deployment can require specialized quantum communication equipment, dedicated links, and carefully controlled environments.

Fig 3 should place the five challenges on the horizontal axis and the normalized index from 0 to 100 on the vertical axis. The graph will show that quantum cybersecurity challenges are distributed across technical, economic, and organizational dimensions. Hardware limitations have high cost and scalability values, whereas cryptographic inventory gaps have very high urgency. This distinction is important because organizations cannot solve quantum risk simply by purchasing new cryptographic software; they must understand where vulnerable algorithms exist and determine which assets require migration first.

Cryptographic inventory is one of the most important migration activities. Modern systems frequently use cryptography indirectly through certificates, network protocols, operating systems, device firmware, cloud services, authentication frameworks, vendor libraries, and third-party components. An organization may therefore depend on vulnerable algorithms without explicitly knowing where they are used. NIST migration guidance emphasizes the need to identify and prioritize vulnerable systems before implementing a transition.

Cryptographic asset discovery also supports algorithm agility by establishing where algorithms and key lengths can be updated without redesigning complete applications. [6,12] PQC integration creates a different type of challenge. The new algorithms must operate within existing protocols while maintaining acceptable latency, bandwidth, memory, and computational requirements. Larger public keys or signatures can influence constrained Internet of Things systems, certificates, VPNs, TLS implementations, and embedded applications. Hybrid approaches may be used during transition, but they can increase computational and communication overhead. Consequently, post-quantum migration should evaluate the total system rather than only the cryptographic primitive. QKD has its own infrastructure burden.

Practical networks require optical channels, quantum

transmitters and receivers, key-management systems, classical communication channels, authentication, and network control. Distance and photon loss can reduce operational performance, while trusted relay models can introduce additional assumptions. Research into device-independent QKD aims to reduce dependence on detailed device models, but practical device-independent implementations remain technologically difficult because they require demanding conditions for entanglement distribution and measurement. [7,10]

Post-Quantum Cryptographic Protection

The implementation of post-quantum cryptography represents one of the most direct responses to the threat posed by future quantum computers. NIST's finalized standards from 2024 define ML-KEM as a key-encapsulation mechanism, while ML-DSA and SLH-DSA provide digital-signature mechanisms. NIST subsequently selected HQC in March 2025 as an additional KEM for standardization, providing a backup approach to ML-KEM based on different mathematical foundations. The transition is therefore moving from algorithm selection toward system-wide deployment, interoperability, testing, and cryptographic agility. [6,9,11]

Table 4 provides four numerical dimensions suitable for a bubble chart. Security Index and Deployment Readiness represent the relative practical assessment of each mechanism. Classical Compatibility reflects the extent to which the technology can be incorporated into existing computing and communication infrastructures. Quantum Resilience represents the normalized resistance to the threat model considered in this article. The numerical values are illustrative and are not security certification scores.

Table 4: *Normalized comparison of quantum-resistant protection mechanisms*

Protection Mechanism	Security Index	Deployment Readiness	Classical Compatibility	Quantum Resilience
ML-KEM	94	88	91	95
ML-DSA	93	86	89	94
SLH-DSA	91	82	87	96
HQC	90	61	84	93
QKD	96	58	49	98

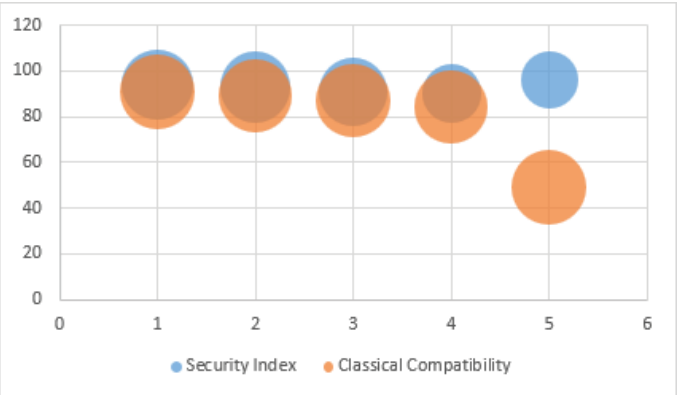


Fig 4: *Bubble chart comparing quantum-resistant protection mechanisms*

Fig 4 should use Security Index as the horizontal axis and Deployment Readiness as the vertical axis, with bubble size proportional to Classical Compatibility. Quantum Resilience can be represented using labels or a secondary annotation. This arrangement allows the graph to show the difference between highly quantum-resistant technologies and the practicality of integrating them into current infrastructure. ML-KEM and ML-DSA occupy high-readiness regions, while QKD demonstrates high quantum-resilience and security values but comparatively lower compatibility and deployment-readiness values.

ML-KEM is intended primarily for general encryption and key establishment. It is especially relevant to protocols where two parties must establish a shared secret over a public channel. ML-DSA is designed for digital signatures and therefore supports authentication, integrity, and non-repudiation functions. SLH-DSA provides a hash-based signature alternative and is important as a diversity mechanism because it relies on a substantially different mathematical construction from lattice-based signatures. HQC adds further diversity to key establishment and is expected to serve as a backup rather than replacing ML-KEM as the primary general-purpose KEM. [6,9]

The migration process also involves algorithm agility. Systems should support the ability to replace algorithms, certificates, parameters, and cryptographic libraries with minimal disruption. This is especially important because cryptographic standards can evolve in response to new cryptanalysis or performance findings. Algorithm agility therefore acts as a form of operational resilience. Organizations can prepare for future cryptographic changes by separating cryptographic functions from application logic and by maintaining clear inventories of cryptographic dependencies.

NIST currently advises organizations to begin migrating to the finalized PQC standards. Its transition planning identifies the need to move away from quantum-vulnerable algorithms and anticipates that such algorithms will be deprecated and eventually removed from relevant standards, with high-risk systems transitioning earlier. This policy direction illustrates that quantum readiness is no longer solely a long-term research issue; it has become an active engineering and governance requirement for systems with long confidentiality lifetimes. [6]

Conclusion

Quantum computing is becoming an important factor in the strategic development of cybersecurity and cryptographic systems because it simultaneously introduces new attack capabilities and enables new security technologies. Shor's algorithm represents the most serious long-term threat to widely deployed public-key systems based on factoring and discrete logarithms, including RSA, Diffie–Hellman, and elliptic-curve cryptography. Grover's algorithm creates a different and more limited threat to symmetric cryptography by reducing generic search complexity, making larger security margins particularly relevant. In response, Post-Quantum Cryptography has progressed from research into practical standardization, with NIST finalizing ML-KEM, ML-DSA, and SLH-DSA in 2024 and selecting HQC for further standardization in 2025. Quantum Key Distribution and quantum random-number generation provide additional opportunities for specialized security applications, while quantum-assisted intrusion detection and optimization remain emerging research areas. The comparative analysis shows that quantum cybersecurity must be approached as a complete architecture involving cryptographic

migration, hardware, communications, software, authentication, monitoring, and organizational planning. The future security landscape is therefore likely to involve a combination of post-quantum classical cryptography and selected quantum technologies rather than reliance on a single solution. Early cryptographic inventory, algorithm agility, interoperability testing, and phased migration are essential for protecting long-lived information before cryptographically relevant quantum computing becomes practical.

References

1. P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
2. Y.-K. Liu and D. Moody, "Post-Quantum Cryptography and the Quantum Future of Cybersecurity," Physical Review Applied, vol. 21, 040501, 2024.
3. W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson.
4. P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, pp. 1484–1509, 1997.
5. L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.
6. National Institute of Standards and Technology, Post-Quantum Cryptography, NIST Computer Security Resource Center.
7. S. Pirandola et al., "Advances in Quantum Cryptography," Advances in Optics and Photonics, vol. 12, pp. 1012–1236, 2020.
8. National Security Agency, Post-Quantum Cybersecurity Resources: Quantum Key Distribution and Quantum Cryptography Guidance, 2025.
9. National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," 2024.
10. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Walther, "Advances in Quantum Cryptography," Advances in Optics and Photonics, vol. 12, pp. 1012–1236, 2020.
11. National Institute of Standards and Technology, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," 2025.
12. National Institute of Standards and Technology, Transition to Post-Quantum Cryptography Standards, NIST IR 8547, 2024.
13. F. Barrett-danes and F. Ahmad, "Quantum Computing and Cybersecurity: A Rigorous Systematic Review of Emerging Threats, Post-Quantum Solutions, and Research Directions," Discover Applied Sciences, vol. 7, article 1083, 2025.
14. M. Goyal, V. Kumar, and S. M. N. Islam, eds., Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies, Springer, 2025.
15. "Practical Quantum Key Distribution Networks: A Mini-Review," European Physical Journal Special Topics, vol. 235, pp. 2947–2965, 2026.
16. "Comprehensive Survey of Global Research Trends, Challenges, and Comparative Advances in Quantum Cryptography and Post-Quantum Cryptographic Algorithms," Discover Artificial Intelligence, 2026.