© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722795

# Performance Evaluation of Post-Quantum Cryptography in Satellite Security Architecture

NANCY BAKO MADUGU[1], FAUZIYA BAWA IBRAHIM[2], FATIMAH AHMED ALMAKURA[3], PAUL AYAMBE NDIK[4], ZULAIHAT MUKHTAR[5]
[1, 2, 3, 4, 5]*National Space Research and Development Agency (NASRDA)*

***Abstract-*** ***Satellite systems rely on a robust yet light weight cryptographic solution for the security of ground systems, communications links, Telemetry, Tracking and Command (TT&C), payloads, onboard systems and associated subsystems. Cryptography ensures data integrity and overall security especially for satellites whose missions and data transmitted are in general and by global practices included in Critical National Infrastructures (CNIs). But emerging cybersecurity threats might render cryptographic solutions such as Rivest-Shamir-Adleman (RSA), Diffie–Hellman (DH) and Elliptic-Curve Cryptography (ECC) ineffective in securing space assets.***

***Quantum cryptography offers a better solution to the emerging threats of relentless and sophisticated systems and adversaries. This paper evaluates the performance of Post-Quantum Cryptography (PQC) when deployed. The research explored the various standards mapped out by the National Institute of Standards and Technology (NIST) for PQC deployment.***

***Current security architecture of satellite systems was compared to what the PQC solution will offer to these highly classified assets. The paper further explored algorithms in place and how effective they could be in the space industry. In the space sector, deploying PQC requires a beta analysis of its performance; which was explored in the third chapter of this work.***

***Challenges and Deployment Considerations and Computational and Resource Constraints of PQC deployment was evaluated in the fifth and sixth sections of this work. The paper concluded by acknowledging the potential complexities in the eventual wholistic adoption and deployment of Quantum Cryptography.***

***Key words: cryptography; post quantum cryptography; pqc, cybersecurity; cyber threats; critical national infrastructures (cnis); satellite systems.***

## I. INTRODUCTION

Modern satellite architectures increasingly depend on digital communication between spacecraft, ground stations and user terminals, creating a distributed cyber-physical environment in which the confidentiality, integrity and authenticity (core elements of cybersecurity) of information are essential to mission continuity. Consequently, cybersecurity is no longer limited to protecting ground infrastructure; it must encompass the space segment, ground segment and communication links throughout the satellite mission lifecycle. The European Space Agency (ESA) identifies the increasing integration of space systems with terrestrial networks as a significant cybersecurity concern because vulnerabilities in interconnected space and ground infrastructure can expose critical space assets to cyberattacks ; .

Security solutions deployed to enhance the security of these assets continue to evolve so also are the skills and sophistication of techniques employed by malicious adversaries. One prominent solution is cryptography. Cryptography constitutes a fundamental layer of security within this architecture . It supports secure key establishment, data confidentiality, authentication, integrity protection and secure software or firmware updates. In particular, public-key cryptographic mechanisms are important for establishing trust between satellite and ground systems without requiring a pre-shared secret for every communication relationship. Conventional public-key mechanisms, including Rivest–Shamir–Adleman (RSA), Diffie–Hellman (DH) and Elliptic-Curve Cryptography (ECC), have therefore become important components of modern secure communication infrastructures . However, their long-term security is threatened by the development of sufficiently capable quantum computers. Shor's algorithm provides a theoretical basis for efficiently solving the integer-factorization and discrete logarithm problems on which widely deployed RSA and ECC-based cryptographic mechanisms depend. This creates a significant future security concern for

satellite systems whose operational lifetimes and data retention periods are developed to be relevant after many years ; ; .

Quantum threat is particularly relevant to space systems because cryptographic protection may need to remain effective throughout long mission lifecycles. Sensitive satellite telemetry, mission data, command information and other communications intercepted today could potentially be retained and decrypted in the future when sufficiently capable quantum computers become available. This threat, commonly described as "harvest now, decrypt later," strengthens the case for beginning migration toward quantum-resistant cryptographic mechanisms before large-scale quantum computers become operational . The National Institute of Standards and Technology (NIST) has emphasized the need for organizations to begin transitioning toward post-quantum cryptographic standards rather than waiting for the emergence of cryptographically relevant quantum computers as a reactive measure .

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to provide security against adversaries equipped with quantum computers while remaining implementable on conventional computing platforms. In August 2024, NIST finalized three Federal Information Processing Standards (FIPS) for PQC: FIPS 203, which specifies the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM); FIPS 204, which specifies the Module-Lattice-Based Digital Signature Algorithm (ML-DSA); and FIPS 205, which specifies the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). ML-KEM is intended for key establishment, while ML-DSA and SLH-DSA provide quantum-resistant digital signatures for authentication and data integrity.

The emergence of these standards provides an important foundation for securing the future of satellite architectures. , NIST specifies three ML-KEM parameter sets ML-KEM-512, ML-KEM-768 and ML-KEM-1024 each with increasing security strength and corresponding differences in performance than the previous. These differences are particularly important in satellite environments because cryptographic performance cannot be evaluated solely in terms of resistance to quantum attacks but on peculiarity of payloads and overall mission plans .

Unlike many terrestrial computing environments, space systems operate under strict resource and operational constraints. Onboard computers may have limited processing capability, memory and energy availability, while communication links can impose restrictions on bandwidth and transmission efficiency. Furthermore, space systems may be difficult or impossible to physically access after launch, making cryptographic upgrades considerably more challenging than upgrades to conventional terrestrial systems. These characteristics create an important security-performance problem: a cryptographic mechanism may provide an appropriate level of quantum resistance but still impose excessive computational, memory, energy or communication overhead on a satellite platform ; .

## II. SECURITY ARCHITECTURE OF SATELLITE SYSTEMS

The security of modern satellite systems depends on protecting multiple interconnected components rather than a single communication channel. A satellite architecture generally comprises the space segment, ground segment, and user segment, which interact through communication links and supporting terrestrial infrastructure. The space segment contains spacecraft and their onboard systems, while the ground segment provides mission control, communication, data processing and operational support. The user segment comprises the terminals and entities that access satellite-enabled services. The interdependence of these components create a broad cybersecurity environment in which weaknesses in one segment can potentially affect the security and availability of other components or a potential compromise of the entire system. emphasized that the space cyber ecosystem as a high-cost, often inaccessible environment consisting of distinct but interdependent segments, with particular security concerns surrounding satellite command and control.

Cryptography provides a fundamental mechanism for protecting these interactions. It supports confidentiality, integrity, authentication, secure key establishment and protection of sensitive operational

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722795

information. In satellite systems, these functions may be required across satellite-to-ground communications, inter-satellite links, telemetry, tracking and command (TT&C), mission-data transmission and software-update mechanisms. Consequently, the selection of cryptographic mechanisms must account not only for their security properties but also for the operational characteristics of satellite systems, including constrained processing resources, memory, bandwidth and long mission lifetimes.

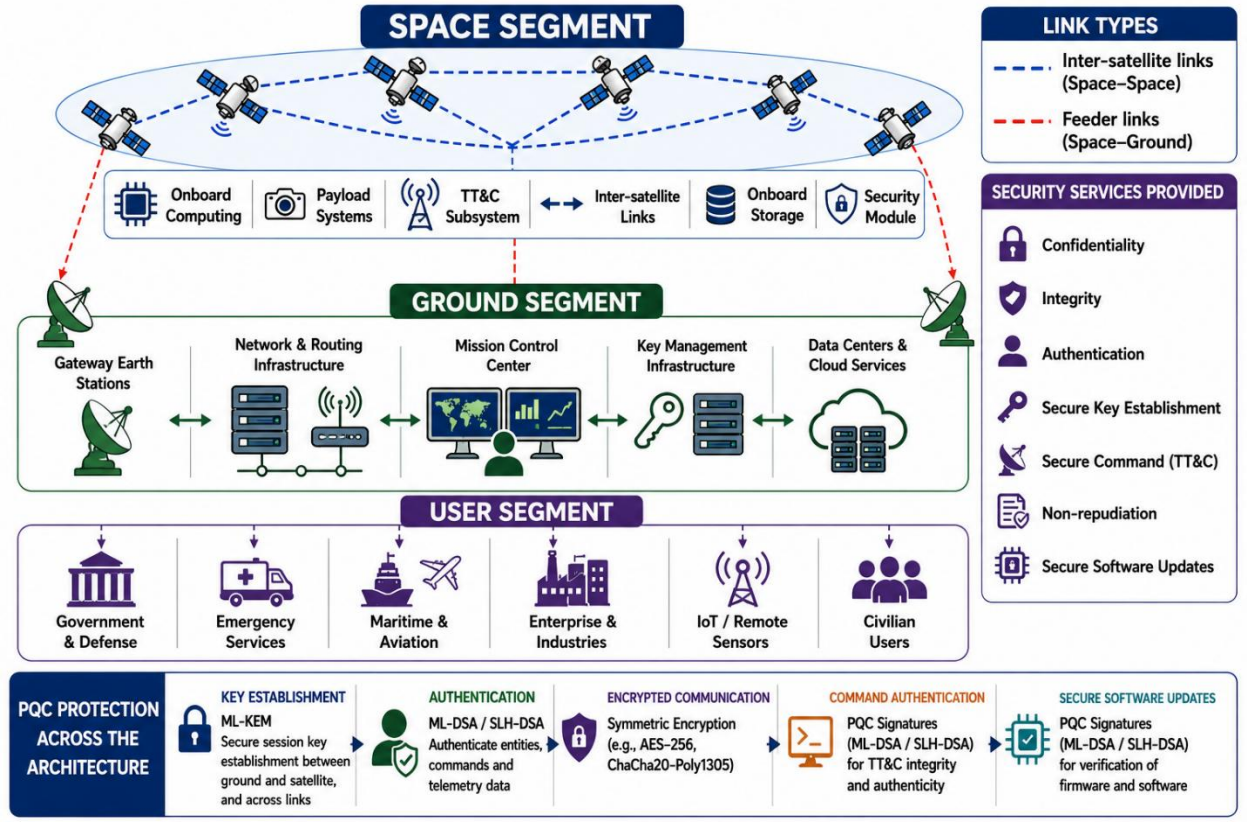


Fig 1: Quantum Threat and PQC Protection Across Satellite Architecture

2.1 Post-Quantum Cryptography and Satellite Architecture Security

Satellite systems have evolved into interconnected cyber-physical infrastructures supporting communications, navigation, Earth observation, scientific missions, defence and other critical services. Their operation depends on the interaction of multiple components, principally the space segment, ground segment, and user segment. These segments are interconnected through communication links and supporting terrestrial networks, creating a distributed architecture in which a compromise of one component may affect the confidentiality, integrity, availability, or operational control of other components. The National Institute of Standards and Technology (NIST) describes the space cyber ecosystem as a high-cost and often inaccessible environment consisting of distinct but interdependent segments, with satellite command and control representing a particularly important security concern .

Satellite security can be considered across three principal architectural domains: the space segment, ground segment and user segment. The space segment contains the spacecraft and its onboard subsystems, including the onboard computer, payload, communication systems, data storage and TT&C functions. The ground segment includes ground stations, mission-control Centres, communication networks, data-processing infrastructure and other systems responsible for controlling and monitoring spacecraft. The user segment consists of terminals and

organizations that consume satellite services. This segmentation is consistent with the cybersecurity architecture described by the National Institute of Standards and Technology (NIST), which identifies the space, ground and user components as interconnected elements of the space cyber ecosystem ; ; .

Each segment presents distinct security requirements. The space segment requires protection against unauthorized commands, manipulation of onboard systems and compromise of mission data. The ground segment must protect mission-control infrastructure and the interfaces through which commands are transmitted to spacecraft. Similarly, user systems require mechanisms for authentication and secure access to satellite services. NIST's satellite cybersecurity guidance places particular emphasis on protecting satellite command and control because compromise of these functions could affect the operation of spacecraft and their payloads .

Cryptographic mechanisms contribute to these security requirements in several ways. Key establishment enables communicating entities to derive shared secret keys for subsequent secure communication. Digital signatures can authenticate commands, software and other digitally signed information. Encryption can protect mission and user data from unauthorized disclosure, while integrity mechanisms can detect unauthorized modification.

The characteristics of spacecraft make cryptographic selection particularly important. Space systems may have limited computing and memory resources and are generally difficult to physically access after launch. As a result, cryptographic mechanisms incorporated into a spacecraft may need to remain effective throughout a substantial portion of its operational lifetime. This creates a requirement for security mechanisms that are not only resistant to emerging threats but also practical within the constraints of the intended satellite architecture .

Cryptography constitutes an important layer of protection within this architecture. It enables secure key establishment, authentication, confidentiality and integrity of information exchanged between spacecraft, ground stations and users. Cryptographic protection may therefore be required for satellite-to-ground communication, inter-satellite links, telemetry, tracking and command (TT&C), mission-data transmission, and software or firmware updates. However, the cryptographic requirements of satellite systems differ from those of conventional terrestrial networks because spacecraft typically operate with constrained computing resources and may remain inaccessible for extended periods after deployment. These characteristics make the selection and long-term suitability of cryptographic mechanisms an important architectural consideration; .

For satellite architectures, this transition presents a complex systems problem. Conventional cryptographic mechanisms may be distributed across spacecraft software, ground systems, communication protocols and key-management infrastructure. Replacing them therefore requires coordination across multiple architectural components. Furthermore, the long operational lifetime and limited physical accessibility of space systems can make post-launch cryptographic migration difficult to deploy.

2.2 Post-Quantum Cryptographic Algorithms for Satellite Security

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to resist attacks from both conventional computers and sufficiently capable quantum computers. Unlike quantum key distribution, PQC does not require quantum communication channels or specialized quantum hardware. It can therefore be implemented using conventional computing platforms and integrated into existing communication architectures .

The standardization of PQC by NIST has provided concrete algorithms for organizations preparing for the quantum era. In August 2024, NIST finalized Federal Information Processing Standard (FIPS) 203, specifying the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM); FIPS 204, specifying the Module-Lattice-Based Digital Signature Algorithm (ML-DSA); and FIPS 205, specifying the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) .

ML-KEM is particularly relevant to satellite communication because a Key-Encapsulation

Mechanism (KEM) enables two parties to establish a shared secret over a public communication channel. The resulting shared secret can subsequently be used with symmetric cryptography to protect communication sessions. NIST specifies three ML-KEM parameter sets: ML-KEM-512, ML-KEM-768 and ML-KEM-1024. They provide increasing security strength but decreasing performance in that order, making the choice of parameter set an important security-performance consideration for constrained systems ; .

ML-DSA provides a post-quantum mechanism for digital signatures. Digital signatures can be used to authenticate the source of information and detect unauthorized modification. In satellite systems, this makes ML-DSA relevant to satellite identity authentication, ground-station authentication, command authentication and software or firmware verification. NIST specifies ML-DSA as a digital-signature algorithm designed to remain secure against adversaries possessing large-scale quantum computing capabilities .

SLH-DSA provides an alternative signature mechanism based on hash-based cryptography. NIST specifies SLH-DSA as a stateless hash-based digital-signature algorithm derived from the SPHINCS+ construction. It can provide authentication and integrity protection while offering a cryptographic construction different from the lattice-based approach used by ML-DSA .

Consequently, the adoption of PQC in satellite systems should not be assessed solely on the basis of its resistance to quantum attacks. Its computational requirements, memory and storage requirements, communication overhead, cryptographic object sizes and security strength must also be considered in relation to the constraints of satellite platforms. A mechanism offering stronger security but substantially greater resource requirements may not necessarily represent the most appropriate solution for every satellite application .

## III. PERFORMANCE CONSIDERATIONS OF POST-QUANTUM CRYPTOGRAPHY IN SATELLITE SYSTEMS

The adoption of Post-Quantum Cryptography (PQC) in satellite systems requires consideration of more than its resistance to quantum attacks. Satellite platforms operate under constraints that can influence the practicality of cryptographic implementations, including limited processing capability, memory, storage, power availability and communication bandwidth. Consequently, the performance characteristics of PQC mechanisms are important determinants of their suitability for different satellite security functions. This section of this paper will examine four principal considerations: computational performance, memory and storage requirements, communication overhead, and security performance trade-off.

### 3.1 Computational Performance

Computational performance refers to the processing resources and execution time required to perform cryptographic operations. In a satellite environment, this consideration is particularly important because cryptographic operations compete with other onboard functions for processing resources. Excessive computational requirements could increase processing latency or interfere with other mission-critical operations.

For Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), the principal operations are key generation, encapsulation and decapsulation. These operations support the establishment of shared secrets between communicating entities and are therefore relevant to satellite-to-ground and inter-satellite communications. NIST specifies three ML-KEM parameter sets—ML-KEM-512, ML-KEM-768 and ML-KEM-1024—which provide increasing security strength but involve different performance characteristics .

The computational indications become more significant as the selected security parameter expands. Higher security configurations generally require larger mathematical operations and additional processing resources. This creates a trade-off between selecting a stronger security parameter and maintaining

acceptable processing performance on constrained space systems.

Digital-signature operates in a similar fashion and technical considerations. Module-Lattice-Based Digital Signature Algorithm (ML-DSA) and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) can be used for authentication and integrity protection, but their computational requirements differ. ML-DSA is based on lattice cryptography, whereas SLH-DSA uses a hash-based construction. NIST standardized both mechanisms as quantum-resistant digital-signature algorithms but with different parameter sets and implementation characteristics ; .

For satellite applications, computational performance is particularly relevant to functions that occur frequently. For example, if authentication is performed repeatedly for telemetry, tracking and command (TT&C) messages or communication sessions, even relatively small increases in processing requirements can accumulate over time. Conversely, operations such as software-update verification may occur less frequently and may therefore tolerate greater computational overhead .

3.2 Memory and Storage Requirements

Memory consumption represents a second important consideration. Satellite computers may have substantially fewer memory resources than modern terrestrial servers and personal computers, while onboard memory must simultaneously support flight software, payload processing, telemetry, data storage and other mission functions.

PQC can introduce additional memory requirements because its cryptographic keys, intermediate values and signatures or ciphertexts can be considerably larger than those associated with some conventional public-key algorithms. The NIST specifications demonstrate this difference through the parameter sizes defined for ML-KEM and ML-DSA ; .

Memory requirements can be considered at two levels. First, there is static storage, which includes cryptographic keys and the software required to implement the algorithms. Second, there is dynamic memory, which includes temporary buffers and intermediate values required while cryptographic operations are being executed.

This distinction is particularly relevant to spacecraft. A cryptographic implementation that fits within the available permanent storage may nevertheless require more temporary memory than the onboard processor can efficiently provide. Consequently, algorithm selection should consider both the size of cryptographic objects and the memory required during execution.

Research into PQC on constrained embedded platforms has demonstrated that memory requirements can become a significant limitation when implementing lattice-based and hash-based cryptographic algorithms. observed substantial resource requirements when implementing ML-KEM and ML-DSA on a highly constrained microcontroller, reinforcing the importance of evaluating PQC in relation to the actual limitations of the target platform. For satellite architecture, this means that the selection of a PQC mechanism should not be based exclusively on its security classification. The availability of sufficient memory for cryptographic operations, key storage and secure software execution must also be considered.

3.3 Communication Overhead

Communication overhead is particularly important for satellite systems because communication resources are often more constrained than those available in terrestrial networks. PQC algorithms generally involve larger public keys, ciphertexts or digital signatures than many traditional public-key mechanisms. Consequently, migrating from conventional cryptography to PQC can increase the amount of data transmitted over satellite communication links.

For ML-KEM, the relevant communication objects include the public key and ciphertext generated during the key-establishment process. For ML-DSA and SLH-DSA, the principal consideration is the size of the digital signature and associated public key. The NIST standards specify different sizes across the available parameter sets, creating different communication requirements .

This is important because satellite communication links may operate with limited bandwidth and may experience propagation delays. Larger cryptographic objects can increase transmission time and consume additional communication capacity. The effect becomes more significant where authentication or key establishment occurs frequently. The communication overhead of PQC can therefore influence architectural decisions.

3.4 Security Performance Trade-off

PQC adoption involves a fundamental security-performance trade-off. Increasing cryptographic security can involve additional computational, memory and communication costs. Conversely, selecting a lower-cost configuration may reduce the resources required by the satellite but provide a lower security margin.

This trade-off is explicitly reflected in the NIST ML-KEM standard. ML-KEM-512, ML-KEM-768 and ML-KEM-1024 provide progressively greater security strength, while their computational and cryptographic resource requirements also change across the parameter sets .

The appropriate choice therefore depends on the security requirements and operational characteristics of the satellite application. A high-security government or military satellite handling highly sensitive information may justify greater computational and communication overhead than a low-data-rate scientific satellite with highly constrained onboard resources. Similarly, security mechanisms protecting critical TT&C channels may require different performance considerations from mechanisms used for occasional software updates .

However, this relationship should not be interpreted as meaning that the strongest cryptographic configuration is always the most appropriate. Rather, the objective should be to identify a configuration that provides an adequate security margin while remaining compatible with the operational constraints of the satellite.

This is the principal basis for the comparative assessment presented in the next section. The analysis will examine the reported characteristics of selected PQC algorithms and compare them with conventional cryptographic mechanisms to determine their relative suitability for satellite security applications .

## IV. COMPARATIVE ASSESSMENT OF PQC APPROACHES

The transition from conventional public-key encryption to PQC requires more than evaluating resistance to quantum attacks. For satellite systems, cryptographic algorithms must also operate within constraints imposed by limited processing capability, memory, power availability, communication bandwidth and intermittent connectivity. Consequently, the selection of a suitable PQC mechanism requires a balance between security strength and operational performance. Recent studies have shown that these considerations are particularly important for resource-constrained satellite platforms, where cryptographic overhead can affect both communication efficiency and onboard processing requirements .

4.1 Comparison of Major PQC Approaches

PQC algorithms are based on different mathematical problems, with lattice-based, code-based and hash-based approaches receiving significant attention. NIST's first finalized PQC standards comprise ML-KEM for key establishment, ML-DSA for digital signatures and SLH-DSA as a hash-based digital-signature alternative .

Lattice-based cryptography currently provides the most prominent option for general-purpose PQC deployment. ML-KEM, derived from CRYSTALS-Kyber, is designed for establishing shared secret keys over public communication channels, while ML-DSA, derived from CRYSTALS-Dilithium, this algorithm provides quantum-resistant digital signatures (NIST, 2024). ML-KEM offers three security parameter sets ML-KEM-512, ML-KEM-768 and ML-KEM-1024 with increasing security strength accompanied by decreasing performance .

For satellite systems, the principal advantage of lattice-based schemes is their relatively balanced combination of security and performance. Their computational requirements and communication overhead remain important considerations, but recent

satellite-focused research indicates that lattice-based mechanisms can provide a practical path toward quantum-resistant satellite communications when implemented with appropriate consideration of hardware and protocol constraints .

Hash based cryptography provides another important option, particularly for digital signatures. SLH-DSA, standardized in NIST FIPS 205 and derived from SPHINCS+, relies on hash function security rather than lattice assumptions (NIST, 2024). This makes it valuable as a cryptographic alternative with a different underlying security assumption. However, it is most suitability for satellite applications which must be evaluated against the additional communication and processing requirements associated with hash signatures.

Code-based cryptography represents another PQC approach, with the Classic McEliece historically receiving substantial attention, its security is based on the difficulty of decoding certain error-correcting codes. Although code-based mechanisms remain relevant to the broader PQC landscape, their large public-key requirements can make them less attractive where satellite memory and communication resources are constrained. Code-based alternatives have seen continued interest in the development by NIST as part of its ongoing standardization activities, including Classic McEliece and Hamming Quasi-Cyclic (HQC) ;.

Thus, the comparison suggests that security alone cannot determine the most appropriate PQC algorithm for satellite architecture. The cryptographic mechanism must also be evaluated according to the particular resource and communication requirements of the subsystem in which it will operate.

4.2 Suitability for Different Satellite Subsystems

Satellite architecture consists of several interconnected components, including onboard processors, payload systems, telemetry and telecommand links, inter-satellite links, ground stations and mission-control infrastructure. These components do not have identical computational or communication requirements. Consequently, a PQC algorithm that performs adequately on a ground-based mission-control server may impose unacceptable overhead when implemented directly on a resource-constrained spacecraft processor.

For key establishment, ML-KEM is a particularly relevant candidate because it provides a standardized quantum-resistant mechanism for establishing shared secrets, after which symmetric cryptography can be used for bulk data protection . This makes it potentially suitable for securing communication sessions between spacecraft and ground infrastructure.

For authentication and digital signatures, ML-DSA provides a standardized lattice-based solution capable of generating and verifying quantum-resistant signatures . Such functionality is important for protecting satellite telemetry, telecommands, software updates and other mission-critical messages from forgery or unauthorized modification .

SLH-DSA can provide an alternative signature mechanism based on a fundamentally different cryptographic construction. Its availability as a standardized alternative is important from a cryptographic-agility perspective because dependence on a single mathematical family could introduce systemic risk if weaknesses are subsequently discovered in that family .

4.3 Comparative Performance Considerations

The performance implications of PQC in satellite architecture can be evaluated through several parameters: computational latency, memory consumption, key and ciphertext/signature size, communication overhead and energy consumption. These parameters are interconnected. For example, larger cryptographic objects require more transmission capacity and storage, while computationally intensive operations may increase processor utilization and energy consumption.

Recent research specifically examining lattice-based PQC in satellite communications identifies computational efficiency, bandwidth overhead, memory footprint and energy consumption as important dimensions for evaluating PQC deployment on resource-constrained spacecraft . Therefore, an algorithm should not be considered superior simply because it provides stronger security or faster computation in isolation.

A particularly important consideration is the difference between ground and space segments. Ground infrastructure generally has greater processing and storage capacity and can therefore accommodate larger cryptographic workloads. Spaceborne systems, in contrast, may operate with more constrained processors and power budgets. This suggests that PQC deployment should be architecture-aware, with computationally demanding operations preferentially allocated to components capable of supporting them while minimizing unnecessary cryptographic processing onboard .

## V. CHALLENGES AND DEPLOYMENT CONSIDERATIONS

Despite the security benefits offered by post-quantum cryptography (PQC), its deployment in satellite architecture presents several technical and operational challenges. Unlike conventional terrestrial networks, satellite systems often operate with constrained processing resources, limited bandwidth, strict energy budgets, long operational lifetimes and communication links characterized by latency and intermittent connectivity. These conditions can amplify the overhead introduced by PQC algorithms. Recent work on non-terrestrial networks identifies high latency, constrained onboard processing, long satellite lifecycles, limited link budgets and complex multi-stakeholder environments as important considerations for PQC migration ;.

## VI. COMPUTATIONAL AND RESOURCE CONSTRAINTS

One of the principal challenges is the additional computational and memory requirements associated with PQC. Compared with conventional public-key algorithms, PQC mechanisms generally involve larger keys, ciphertexts or signatures and may require additional processing and memory resources. These requirements can be particularly significant for spacecraft equipped with radiation-hardened processors whose computational capabilities may be considerably more limited than those of contemporary terrestrial systems.

For satellite applications, this creates a direct relationship between cryptographic security and spacecraft resource consumption. Increased computational activity can raise processor utilization and energy consumption, while larger cryptographic objects increase memory requirements and communication overhead. Recent research on PQC for satellite communications similarly identifies computational efficiency, bandwidth, memory footprint and energy consumption as important deployment considerations .

### 6.1 Bandwidth and Communication Overhead

The larger public keys, ciphertexts and digital signatures associated with many PQC schemes can create significant overhead over satellite links. This is particularly important where bandwidth is limited or links experience packet loss and retransmission. Recent experimental work on PQ-secured LEO satellite networks found that larger PQC messages can interact negatively with path-MTU limitations, potentially resulting in fragmentation or retransmissions and consequently increasing handshake latency and reducing reliability. This suggests that PQC implementation cannot be evaluated solely according to cryptographic computation time; message size and its effect on the communication protocol must also be considered ;.

This issue is particularly relevant during authentication and key-establishment procedures, where several relatively large cryptographic messages may need to be exchanged before a secure session is established.

### 6.2 Long Satellite Lifecycles

Satellite systems typically have long development and operational lifecycles. Consequently, a spacecraft launched with cryptographic mechanisms that are considered secure today may remain operational when those mechanisms are no longer considered adequate. This creates a strong argument for incorporating PQC during the design stage rather than waiting until quantum computers become capable of breaking existing cryptographic systems. NIST currently recommends that organizations begin migration to its finalized PQC standards, while its transition planning anticipates the eventual removal of quantum-vulnerable algorithms from relevant standards .

For space systems, this issue is particularly important because cryptographic hardware and firmware may be

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722795

difficult or impossible to modify after launch. Cryptographic agility should therefore be incorporated into the architecture so that cryptographic algorithms, parameters and keys can be updated throughout the mission lifecycle ;.

6.3 Interoperability and Standardization

Satellite networks frequently involve multiple vendors, ground stations, spacecraft platforms and communication protocols. Introducing PQC without adequate interoperability mechanisms could therefore result in incompatible security implementations across different components.

NIST has finalized ML-KEM, ML-DSA and SLH-DSA as its initial PQC standards, while additional algorithms continue to be evaluated for future standardization. For satellite systems, implementation should therefore remain aligned with recognized standards and emerging specifications rather than relying on proprietary or experimental cryptographic mechanisms.

Interoperability is also important because satellite communications increasingly interact with terrestrial 5G/6G infrastructure and other non-terrestrial networks. The GSMA's recent guidance specifically addresses PQC deployment across satellite-to-ground, satellite-to-user and inter-satellite communications, highlighting the need for coordinated migration across the broader ecosystem ; .

6.4 Cryptographic Agility and Hybrid Migration

A further challenge is the possibility that a currently standardized PQC algorithm could eventually be weakened by advances in cryptanalysis. PQC does not eliminate cryptographic risk; it replaces dependence on quantum-vulnerable mathematical problems with alternative computational assumptions. NIST therefore continues to develop additional algorithms as potential alternatives or backups to its initial standards.

For long-lived satellite systems, this makes cryptographic agility essential. A spacecraft should ideally be capable of supporting algorithm replacement or parameter updates without requiring complete hardware replacement .

A phased or hybrid migration can also reduce transition risks. Classical and PQC mechanisms can initially operate together while compatibility and performance are evaluated. Such an approach has already been demonstrated in satellite-oriented research, including hybrid key-exchange implementations combining PQC and elliptic-curve cryptography on satellite onboard computers.

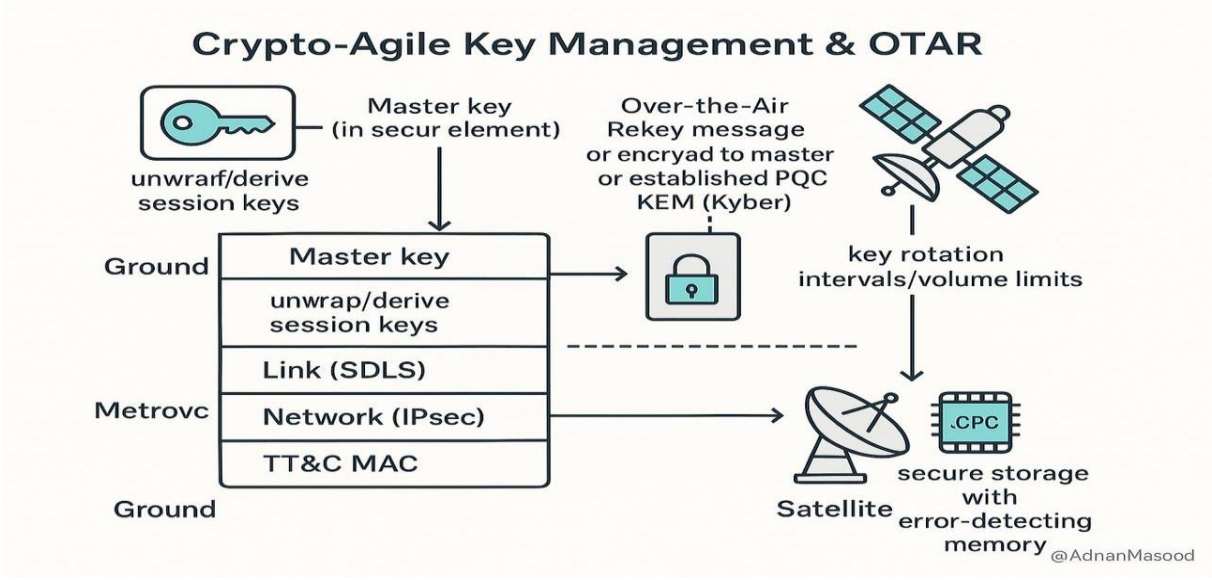


Figure 2: Cryptographic Agile Key Management

## VII. CONCLUSION

The increasing prospect of large-scale quantum computing presents a significant long-term challenge to the cryptographic mechanisms currently used to protect satellite communication and space-based infrastructure. Because satellite systems often have long operational lifetimes and may be difficult to upgrade after deployment, preparing for the post-quantum threat requires consideration during the design and modernization of satellite security architectures. NIST has responded to this challenge by standardizing ML-KEM, ML-DSA and SLH-DSA as its first post-quantum cryptographic standards for key establishment and digital signatures.

This paper evaluated post-quantum cryptography from the perspective of satellite architecture security and performance. The assessment demonstrates that PQC provides an important pathway toward protecting satellite systems against quantum-enabled attacks, but its adoption introduces additional computational, memory, communication and energy requirements. These costs are particularly significant in spacecraft environments where processing capability, power and communication bandwidth are constrained. Recent satellite-focused studies similarly identify computational efficiency, bandwidth overhead, memory footprint and energy consumption as important factors in PQC deployment.

The comparative assessment indicates that lattice-based mechanisms currently provide a particularly practical balance between security and performance for satellite applications. ML-KEM provides a standardized mechanism for quantum-resistant key establishment, while ML-DSA provides a corresponding mechanism for digital signatures.

## REFERENCES

[1] Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martin, P. (2025). A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography*.

[2] Badawy, W. (2025). Protocols, Technologies, and Global Deployment Challenges for Quantum Key Distribution. *International Journal of Information & Digital Security* , 18-36.

[3] Bakyt, M., Spada, L. L., Zeeshan, N., Moldamurat, K., Atanov, S., Konyrkhanova, A., . . . Tilenbayev, A. (2025). Advanced Cybersecurity Framework for LEO Aerospace: Integrating Quantum Cryptography, Artificial Intelligence Anomaly Detection, and Blockchain Technology. *J Robot Control (JRC)*, 695-714.

[4] Bernstein, D. J., Chou, T., Lange, T., Maurich, I., Misoczki, R., Niederhagen, R., . . . Wang, W. (2017). Classic McEliece.

[5] Brule, J., Suloway, T., & Lightman, S. (2022). Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control. *NIST*.

[6] Chen, S.-J., & Tsai, Y.-H. (2025). Quantum-Safe Networks for 6G: An Integrated Survey on PQC, QKD, and Satellite QKD with Future Perspectives. *Computing&AI Connect*.

[7] Dalal, Y. M., Supreeth, S., Amuthabala, K., Satheesha, T. Y., Asha, P. N., & Somanath, S. (2024). Optimizing Security: A Comparative Analysis of RSA, ECC, and DH Algorithms. *IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 1-6.

[8] Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. (2023). A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography*.

[9] Dash, J., & Ogutu, B. O. (2016). Recent advances in space-borne optical remote sensing systems for monitoring global terrestrial ecosystems. *Progress in Physical Geography: Earth and Environment*, 322-351.

[10] Faruk, J. H., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022). A Review of Quantum Cybersecurity: Threats, Risks and Opportunities. *1st International Conference on AI in Cybersecurity (ICAIC)*.

[11] Forouzan, B. A. (2007). Cryptography & Network Security. *McGraw-Hill, Inc.*

[12] Fournaris, A. P., Tasopoulos, G., Brohet, M., & Regazzoni, F. (2023). Running Longer To Slim

Down: Post-Quantum Cryptography on Memory-Constrained Devices. *IEEE International Conference on Omni-layer Intelligent Systems (COINS)*.

[13] Ghosh, T., & Nath, I. (2026). Secure Satellite Communication in the Post-Quantum Era: A Lattice-Based Cryptographic Approach. *International Journal of Satellite Communications and Networking*, 524-543.

[14] Hanna, Y., Veksler, M., & Akkaya, K. (2026). PQ-CKEM: Efficient Quantum-Resistant Group Key Creation for Large-Scale LEO Satellite Networks. *IEEE 32nd International Symposium on Local and Metropolitan Area Networks (LANMAN)*.

[15] Howe, J., Pöppelmann, T., O'neill, M., O'sullivan, E., & Güneysu, T. (2015). Practical Lattice-Based Digital Signature Schemes. *ACM Transactions on Embedded Computing Systems*, 1-24.

[16] Hughes, R. J., Buttler, W. T., Kwait, P. G., Lamoreuax, S. K., Morgan, G. L., Nordholt, J. E., & Peterson, C. G. (2000). Quantum cryptography for secure satellite communications. *IEEE Aerospace Conference Proceedings*.

[17] Korgi, M. A., & Alsammed, S. M. (2026). A Systematic Review of Satellite Communication Security: Challenges, Motivation, and Future Directions. *Engineering and Technology Journal*, 1-51.

[18] Kumar, M., & Pattnaik, P. (2020). Post Quantum Cryptography(PQC) - An overview. *IEEE High Performance Extreme Computing Conference (HPEC)*, 1-9.

[19] Lee, J. (2024). Assessing Quantum Integer Factorization Performance with Shor's Algorithm. In *Quantum Computing* (p. 10). CRC Press.

[20] Lomonaco, S. J., & Kauffman, L. (2007). Quantum Hidden Subgroup Algorithms: An Algorithmic Toolkit. In *Mathematics of Quantum Computation and Quantum Technology* (p. 44). Chapman and Hall/CRC.

[21] Meraz, R., & Vahala, L. (2020). Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications. *OUR Journal: ODU Undergraduate Research Journal*.

[22] Mohammed, A. (2023). Protecting Space Assets: Cybersecurity Challenges and Solutions for the Final Frontier . *Baltic Journal of Engineering and Technology*, 55-61.

[23] Nguyen, T.-H., Dang, T.-K., Dam, D.-T., Nguyen, K.-D., Duong, P.-P., & Pham, C.-K. (2025). An Area-Time Efficient Hardware Architecture for ML-KEM Post-Quantum Cryptography Standard. *IEEE Acess*, 2169-3536.

[24] Niro, F., Goryl, P., Dransfeld, S., Boccia, V., Gascon, F., Adams, J., . . . Doxani, G. (2021). European Space Agency (ESA) Calibration/Validation Strategy for Optical Land-Imaging Satellites and Pathway towards Interoperability. *Remote Sensing*.

[25] NIST. (2024, August 30). *Post-Quantum Cryptography PQC*. Retrieved from Computer Security Resource Centre (CSRC): https://csrc.nist.gov/projects/post-quantum-cryptography

[26] Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). Rethinking Satellite Cybersecurity: A System-Level Taxonomy and Longitudinal Analysis. *Computer Science > Cryptography and Security*.

[27] Raavi, M., Whuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X., & Chang, S.-Y. (2021). Security Comparisons and Performance Analyses of Post-quantum Signature Algorithms. *Applied Cryptography and Network Security*, 424-447.

[28] Rey, D. G. (2026). Quantum-Risk Posture and Space Infrastructure: Post-Quantum Cryptography, Homeland Security, and Critical Infrastructure Resilience. *Applied Counterterrorism and Homeland Security Analysis Portfolio*.

[29] Salim, S., Moustafa, N., & Reisslein, M. (2024). Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *IEEE Communications Surveys & Tutorials*, 372 - 425.

[30] Shaheed, N. A., Mubasheer, F., & Sunad, Y. S. (2020). QUANTUM CRYPTOGRAPHY - BREAKING RSA ENCRYPTION USING

QUANTUM COMPUTING WITH SHOR'S ALGORITHM . *International Journal For Technological Research In Engineering* .

[31] Sivaraman, S., Aswatha, P. N., Chattopadhyay, S., Prabhu, P., & Kumar, S. (2026). FPGA Implementation of Quantum Key Distribution Post-processing for a Post-Quantum Era. *IEEE 6th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA)*.

[32] Truong, Q. D., Duong, P. N., & Lee, H. (2024). Efficient Low-Latency Hardware Architecture for Module-Lattice-Based Digital Signature Standard. *IEEE Access*, 32395-32407.