Chapter 1
Post-Quantum Cryptography for Integrated Space-Aerial-Terrestrial Networks: Current State, Challenges and Trends

Gürkan Gür and Attila A. Yavuz

Abstract Emerging satellite networks integrated with terrestrial and aerial systems form a key part of next-generation infrastructures supporting the Internet of Everything (IoE). This chapter outlines the current status of PQC-based authentication in integrated Space-Aerial-Terrestrial Networks (SATIN), highlighting the technical challenges in achieving quantum-resilient security within constrained and complex environments. While quantum computing necessitates migration to post-quantum cryptography (PQC), existing standards often demand resources that are unsuited for SATIN's limited hardware and fragile links. We analyze leading NIST PQC signature and key encapsulation schemes in the SATIN context, evaluating trade-offs in computational cost, signature size, and protocol compatibility. Emerging directions, including broader algorithm evaluations, advanced protocol integrations (e.g., EMSS and NIST-PQC with terrestrial backbone, PQ group key management), and some alternative PQ technologies are discussed. Addressing these challenges requires advanced simulation and experimental frameworks to enable scalable, practical, and quantum-resilient secure communications in future integrated networks.

1.1 Introduction

Emerging satellite networks are poised to become a key component of next-generation systems, such as 6G and the Internet of Things (IoT), forming a multi-layered, always-connected infrastructure that supports the Internet of Everything (IoE) vision. These networks will integrate with terrestrial and aerial systems to enable

Gürkan Gür
Zurich University of Applied Sciences ZHAW, Winterthur 8401 Switzerland
e-mail: gueu@zhaw.ch

Attila A. Yavuz
University of South Florida (USF), Tampa, FL 33620 USA
e-mail: attilaayavuz@usf.edu

seamless connectivity. However, ensuring the reliability and security of these integrated systems is crucial. Traditional network security protocols are not well-suited to the unique challenges of satellite systems, which include high latency, error-prone links, and the complexity of space-aerial-terrestrial integrated networks (SATIN) [1]. These systems also face constraints related to energy efficiency, especially in light of global sustainability goals. The rise of quantum computing further complicates security, as post-quantum cryptographic methods are often too resource-intensive for mobile and satellite networks.

This chapter examines NIST Post-Quantum Cryptography (PQC) standards in the context of SATIN, highlighting domain-specific security goals, metrics, and technical challenges. It explores the unique characteristics of satellite networks and presents a toolbox of promising approaches to address these challenges.

1.2 Analysis

Deploying NIST-PQC in SATIN requires evaluation across several critical dimensions: (i) signature generation and encapsulation overhead, which affects computation time and energy use on the sender side; (ii) signature verification and decapsulation overhead, impacting computational demands on receivers; (iii) cryptographic transmission overhead, i.e., the byte size of signatures, ciphertexts, public keys, and certificates, which influences fragmentation and link latency; (iv) storage overhead for keys and certificates; (v) ease of implementation and resilience to side-channel attacks, including algorithmic complexity and leakage resistance; (vi) integration with SATIN-specific communication protocols like DVB-S2X, CCSDS, and CPDCL[1], particularly with respect to MTU constraints and timing behavior; (vii) suitability for advanced security features, including forward secrecy and threshold signatures; and (viii) overall trade-offs between security and performance.

Importance of Signature Size and End-to-End Delays in SATIN: Due to strict Maximum Transmission Unit (MTU) limits (typically around 1500 bytes), oversized signature or certificate payloads trigger fragmentation, which leads to: (i) increased end-to-end latency, where each fragment can add 6–11 ms delay in DVB-S2X systems; and (ii) greater bandwidth usage, especially problematic for uplink and telemetry channels constrained by power and spectrum. Reducing signature and certificate sizes is essential for low-latency, energy-efficient communication. Large signatures also impose higher processing and memory demands, which are particularly challenging for resource-limited onboard systems. These issues compound further during mutual authentication, where certificate chains may be exchanged.

Optimal PQC scheme selection should therefore balance computational efficiency, transmission size, and compatibility with existing protocols: (i) minimizing signature and certificate sizes to prevent fragmentation and latency overhead; (ii) enabling threshold signatures to reduce bandwidth and verification cost in multi-node

[1] https://rosap.ntl.bts.gov/view/dot/48805

scenarios; and (iii) ensuring seamless integration with SATIN's existing communication stack to avoid extensive redesign.

Key Encapsulation Mechanisms (KEMs): While signatures are a primary feature of SATIN handshakes, Key Encapsulation Mechanism (KEM) is crucial for standard protocols like PQ-TLS. For point-to-point communication, KEM with signatures allows for authenticated symmetric encryption, facilitating fast and secure communication. The NIST-standardized ML-KEM (previously CRYSTALS-Kyber[2]), with public keys and ciphertexts typically ranging from 800 to 1600 bytes, fits well within SATIN's MTU limits. Its encapsulation and decapsulation processes are swift, taking only milliseconds on common hardware, which ensures efficient and low-latency key exchange.

Overview of NIST-PQC Standards and Relevant RFCs: PQC encompasses a range of schemes built upon diverse intractable problems, including multivariate, code-based, and isogeny-based cryptography. Here, we overview the performance characteristics of the NIST PQC standards, with an emphasis on lattice-based and hash-based digital signatures.

Lattice-based Signature Schemes: ML-DSA (NIST FIPS 204) [3] is based on the Module Learning With Errors (MLWE) problem employing the Fiat-Shamir with Abort framework. Parameters vary to balance size and security; for instance, ML-DSA-44 offers a public key of $\sim$1,312 bytes and signatures of $\sim$2,420 bytes, while ML-DSA-65 and ML-DSA-87 have larger sizes and security margins. ML-DSA allows offline pre-computation of randomness, reducing online signing latency and energy consumption, suitable for constrained SATIN nodes. It can support thresholding, but signature aggregation is currently unsupported.

FN-DSA (draft FIPS 206, Falcon) [4], is a hash-and-sign scheme based on NTRU lattices and the Gentry, Peikert and Vaikuntanathan (GPV) framework. It produces relatively compact keys and signatures; for example, the 512-bit parameter set yields public keys of approximately 897 bytes and signatures of around 666 bytes. However, FN-DSA requires careful floating-point arithmetic that is implemented securely against side-channel leaks. Its offline-online signing mode necessitates transmitting a fresh one-time public key with every signature, increasing transmission overhead in bursty communications typical in SATIN.

Hash-based Signature Schemes: SLH-DSA (FIPS 205, SPHINCS+) uses nested Merkle trees and one-time hash-based signatures to achieve quantum safety without state management, but incurs very large signatures ranging from $\sim$7.8 KB to nearly 50 KB, often prohibitive due to fragmentation and latency concerns. XMSS (RFC 8391), a stateful hash-based scheme with smaller signatures ($\sim$2.5 to 9 KB), requires strict state synchronization, complicating distributed satellite operations.

Quantum-Safe Approaches Beyond NIST-PQC Standards: China's Micius satellite proposed space-based quantum key distribution by demonstrating entangled photon transmission over 1,000 kilometers [5], while the European Space Agency is developing post-quantum cryptographic solutions through projects like PQC AS-TrAL, which integrate NIST-standardized algorithms into satellite onboard comput-

ers [6]. These complementary approaches represent distinct strategies for achieving quantum-safe satellite communications[2].

PQ-secure group key management for satellites presents unique challenges due to bandwidth constraints and broadcast communication requirements. Logical Key Hierarchy (LKH) [7], a symmetric and broadcast-efficient protocol, organizes group members as leaves of a balanced binary tree where the root contains the group key. This organization enables logarithmic rekeying overhead during member join/leave operations. Meanwhile, the Iolus partitions large multicast groups into subgroups managed by distributed Group Security Agents for scalability [8]. Recent dynamic PQ-secure group key establishment protocols leverage lattice-based cryptography to achieve quantum resistance [9]. Satellite-specific implementations of these protocols are focusing on hybrid key exchange protocols, which combine PQC with classical schemes for authenticated key establishment [10].

1.3 SATIN-Centric Comparative Analysis

Evaluating the NIST PQC for SATIN requires a holistic view of computational, communication, and protocol suitability.

ML-DSA benefits greatly from offline pre-computation, transforming signing into a lightweight online process (e.g., μs delay on ARM Cortex-A72 processors), reducing energy and latency for constrained nodes but with more memory usage. FN-DSA yields smaller signature and public key sizes but requires floating-point arithmetic with secure side-channel protections. Its offline-online mode inflates bandwidth as each signature includes a fresh one-time public key ($\sim$897 bytes), increasing transmission overhead during bursty telemetry uplinks.

Hash-based schemes, such as SLH-DSA and XMSS, are generally impractical due to their large signatures (several KB to tens of KB) and, for XMSS, the complex state management required across distributed satellite terminals. In satellite communications, signature and certificate sizes affect packet fragmentation over typical MTUs (1500 bytes), increasing retransmissions and latency due to per-fragment processing delays ($\sim$6–11 ms on DVB-S2X links). The handshake protocols must minimize these overheads to enable real-time communications.

Table 1.1 summarizes key PQC signature schemes relevant to SATIN, covering signature/key sizes, processing times, certificate chain impact, advanced features support, side-channel resistance, and implementation complexity.

ML-DSA variants provide a balanced solution for SATIN, offering moderate signature sizes, efficient computation, and support for offline precomputation to reduce both latency and energy consumption. They also enable threshold signatures (though not aggregation), facilitating secure multi-node operations while reducing communication overhead. FN-DSA is well-suited for scenarios requiring minimal signature and public key sizes, assuming the presence of floating-point hardware and tolerance

[2] https://connectivity.esa.int/projects/e2eqss

Table 1.1 Comparison of PQC Signature Schemes and ML-KEM [2, 3, 4] for SATIN/PQ-TLS

Feature	ML-DSA-44	FN-DSA-512	SLH-DSA	XMSS	ML-KEM
Sig. Size (bytes)	2,420	666	Avg. 28,000	Avg. 5,750	N/A
Pub. Key Size (bytes)	1,312	897	32	1,000	800–1,568
Sec. Key Size (bytes)	2,560	1,280	Large	Large	2,400
Sig. Gen. Time (ms)*	1.8	3.1	> 50	> 10	N/A
Sig. Verif. Time (ms)*	1.2	1.8	> 100	> 15	N/A
Cert. Chain Impact	Moderate	Lower	Extreme	High	As in sigs.
Offl. Pre-comp.	Yes	Limited	No	No	N/A
Thresholding Support	Strong	Limited	Weak	Weak	No
Side-Channel Res.	Good	Medium	Excellent	Variable	Good
Impl. Complexity	Medium (Integer)	High (FP)	Low	Medium	Medium

*Benchmarks on ARM Cortex-A72, typical values

for transmission overhead introduced by one-time keys. Due to its higher computational and energy demands, it is better suited to less constrained environments such as uplinks or ground stations. Finally, hash-based signature schemes (e.g., SLH-DSA, XMSS) are generally ill-suited for SATIN's low-latency, bandwidth-constrained environments, due to their large signature sizes and state management requirements.

SATIN protocols (e.g., DVB-S2X, CCSDS, and MAVLink) must be adapted to account for fragmentation and retransmission issues caused by large PQ signatures and certificates. Careful tuning of latency and error recovery mechanisms is required to maintain system responsiveness under cryptographic overhead. To reduce certificate chain overhead in SATIN, it is essential to limit chain length, exploit caching at verifiers, and explore hybrid classical–PQC certificate hierarchies to ease the transitional deployment burden.

In conclusion, ML-DSA combined with ML-KEM offers a practical and scalable quantum-safe foundation for SATIN. FN-DSA may be selectively deployed on bandwidth-sensitive links, while hash-based signatures remain niche options under current system constraints.

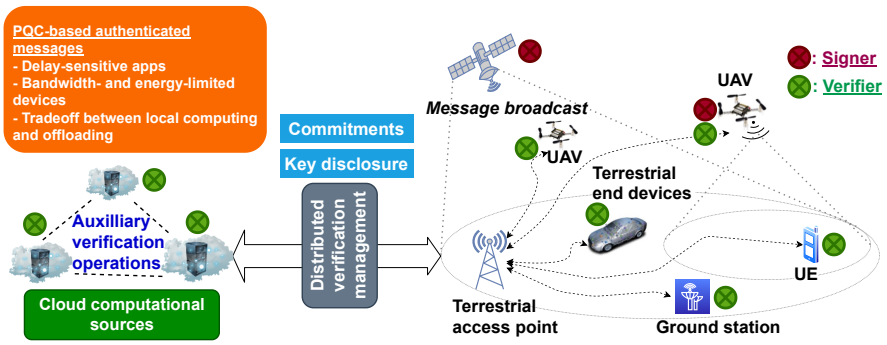

Fig. 1.1 An example SATIN system with PQC and potential optimizations.

Simulation and Performance Analysis Gaps: Despite the importance of practical evaluation, a significant research gap remains in comprehensive protocol-level PQC performance assessment in complex SATIN environments (Fig. 1.1). Current studies insufficiently address multi-hop satellite-to-drone-to-ground chains involving heterogeneous protocols, such as DVB-X and MAVLink [11, 12, 13], and lack insights into PQC-induced delays, fragmentation, and packet loss effects on system efficiency.

Similarly, simulation-based analysis of multi-tier satellite systems with dynamic terrestrial links and large-scale IoT/IoE deployments remains sparse, limiting understanding of trade-offs involving PQC overhead, communication delays, and distributed computing or offloading benefits. Existing general-purpose simulators, such as NS-3[3] and OMNeT++[4], support flexible network simulations but lack dedicated capabilities for advanced cryptographic primitive integration and performance evaluation. Satellite-centric tools like STK and SatNetSim excel at link dynamics modeling but do not support large-scale multi-layer network simulations that incorporate sophisticated cryptography and distributed applications. Bridging this gap requires enhancing simulators or developing new tools that support scalable, protocol-accurate PQC performance evaluation in SATIN, which is critical for designing and deploying next-generation quantum-safe satellite and integrated communication systems. PQC schemes should be implemented more on both COTS and specialized SATIN architectures to quantify device-centric performance in PQC regimes. Any simulation or testbed infrastructure should enable the evaluation of their behavior when integrated into communication protocols by measuring operational flow, delay, and communication efficiency while investigating packet fragmentation and loss, and comparing conventional, NIST-PQC; this protocol-level work should consider IP networking and transport options (TCP, UDP, QUIC) as well as application-layer protocols (HTTP/3, CoAP, MAVLink 2) and different protocol configurations such as buffer sizes and QUIC ACK settings. Such capabilities should also support the investigation of distributed key management, studying delay, synchronization impairments, and packet-loss sensitivity of any proposed lightweight PQC schemes via analytical queueing-theory models with buffer behavior, packet-loss models for heterogeneous links (SAT–UAV, SAT–UE, SAT–GroundStation), and comparisons across satellite constellations (LEO vs MEO).

1.4 Trends

On top of the existing NIST PQC standards, a new set of fourteen additional digital signature algorithms (e.g., CROSS, FAEST, HAWK, and UOV) has advanced to Round 2 of NIST's ongoing standardization process [14]. For key encapsulation, ML-KEM remains the leading standardized option [2], while alternative candidates

[3] https://www.nsnam.org/

[4] https://omnetpp.org/

such as HQC and NTRUEncrypt continue to be evaluated, despite generally involving larger key and ciphertext sizes [15, 16]. This broader evaluation is essential for enhancing cryptographic agility and future-proofing SATIN deployments.

To reduce transmission overhead from large certificate chains, SATIN leverages the terrestrial backbone (Fig. 1.1) to ferry certificates among ground-based authorities, allowing verifiers to retrieve them locally and minimizing over-the-air transmissions. Integrating broadcast-based schemes, such as TESLA (used in Galileo) and EMSS [17], with SATIN's signature framework can further enhance efficiency and resilience by conveying disclosed symmetric keys via the terrestrial backbone, thereby reducing bandwidth consumption while maintaining strong security guarantees.

Given satellite lifecycles of 15–20 years, cryptographic upgrades must align with projected quantum computing deadlines to protect against threats that may emerge well before satellites reach end-of-life[5],[6]. PQ transitions for satellite systems also face practical challenges, including economic costs and interoperability with existing ground infrastructure, which can increase deployment complexity[7]. Additionally, satellites face elevated side-channel attack risks compared to terrestrial systems due to limited physical shielding, harsh space environments, and hardware reuse, making tailored countermeasures essential for securing onboard cryptographic modules [18, 19].

Bringing together expanded PQC evaluations, terrestrial backbone optimizations, and TESLA/EMSS via integration within a unified performance and security framework is vital for the maturation of SATIN. In this direction, the NSF–SNSF-funded SATUQ project [20] is developing novel methods that (1) reduce over-the-air certificate transmission via terrestrial infrastructure, (2) incorporate emerging PQC signature standards and alternative KEMs, and (3) integrate lightweight authenticated broadcast protocols. SATUQ aims to build a comprehensive simulation and experimental analysis platform tailored for quantum-safe communications across space–air–terrestrial networks, addressing critical evaluation gaps and guiding the deployment of scalable, robust SATIN systems resilient to quantum-era threats.

1.5 Conclusion

In this chapter, we outlined key aspects of PQC and authentication as critical enablers of future-proof security in integrated SATIN. Our analysis highlights the importance of balancing signature and key sizes, computational efficiency, and protocol integration to address SATIN's stringent latency, bandwidth, and operational constraints. Among current PQC candidates, ML-DSA stands out for its favorable trade-offs and support for advanced cryptographic features, while FN-DSA offers

[5] https://blog.cloudflare.com/state-of-the-post-quantum-internet-2025/

[6] https://www.satellitetoday.com/

[7] https://blog.cloudflare.com/state-of-the-post-quantum-internet-2025/

situational alternatives. Real-world deployments must also mitigate certificate chain overheads through terrestrial backbone optimizations. Furthermore, the complexity of benchmarking and performance evaluation in realistic network testbeds and simulation environments remains a significant challenge that initiatives like the NSF SNSF-funded SATUQ project are actively addressing by developing comprehensive analysis frameworks. Ultimately, securing SATIN against emerging quantum threats requires an integrated approach that combines cryptographic innovation, network protocol engineering, and rigorous, scalable performance assessment to achieve robust, efficient, and resilient quantum-safe communications.

Acknowledgements This work has received co-funding from the NSF and SNSF, in the framework of the SATUQ project under **SNSF (Grant No 10000409)** and **NSF (ECCS 2444615)**.

About the Author(s)

Gürkan Gür is a senior lecturer at Zurich University of Applied Sciences (ZHAW) InIT Information Security Group in Winterthur, Switzerland. He received his B.S. degree in electrical engineering in 2001 and Ph.D. degree in computer engineering in 2013 from Bogazici University in Istanbul, Turkey. His research interests include Future Internet, 5G and Beyond networks, information security, and critical infrastructure protection. Currently, he is involved in Horizon Europe NATWORK and SNSF-NSF co-funded SATUQ projects. He is a member of IEEE 3394 S2CY - Space System Cybersecurity and IEEE 1920.2 Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems standardization work groups. He is a senior member of IEEE and a member of ACM.

Attila A. Yavuz is an Associate Professor at the USF Bellini College of Artificial Intelligence, Cybersecurity, and Computing at the University of South Florida (USF). He served as an Assistant Professor at Oregon State University (2014–2018) and was a member of the security and privacy group at the Robert Bosch Research and Technology Center North America (2011–2014). He earned his Ph.D. in Computer Science from North Carolina State University (2011) and his M.S. from Bogazici University (2006) in Istanbul, Turkey. His research focuses on the design, analysis, and application of cryptographic tools to enhance system security. Dr. Yavuz is a recipient of the NSF CAREER Award, Cisco Research Award (four times), and research gifts from Robert Bosch. He has authored over 115 scholarly products, including patents, and his work has led to real-world deployments impacting tens of millions globally. He is a senior member of IEEE and a member of ACM.

References

1. JC Pavur, M Strohmeier, V Lenders, and I Martinovic. QPEP: An actionable approach to secure and performant broadband from geostationary orbit. Internet Society, 2021.
2. NIST Post-Quantum Cryptography Standardization. NIST submission: CRYSTALS-KYBER. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions, 2023. Accessed July 2025.
3. NIST. FIPS 204: Crystals-dilithium (ml-dsa) digital signature algorithm. https://csrc.nist.gov/publications/detail/fips/204/draft, 2024. Draft Standard, Accessed July 2025.
4. NIST. Draft FIPS 206: Falcon digital signature algorithm. https://csrc.nist.gov/publications/detail/fips/206/draft, 2024. Draft Standard, Accessed July 2025.
5. Jian-Wei Pan et al. Micius quantum experiments in space. *Reviews of Modern Physics*, 94:025002, 2022.
6. AROBS Group. Arobs polska to develop post-quantum satellite communication system for esa. The Quantum Insider, March 2025. PQC ASTrAL project.
7. Debby Wallner, Eric Harder, and Ryan Agee. Key management for multicast: Issues and architectures. *RFC 2627*, 1999.
8. Suvo Mittra. Iolus: A framework for scalable secure multicasting. *ACM SIGCOMM Computer Communication Review*, 27(4):277–288, 1997.
9. Sara Ricci, Lukáš Malina, Dirmanto Jap, Shivam Bhasin, Jan Hajny, and Lejla Batina. Secure post-quantum group key exchange: Implementing a solution based on kyber. *IET Information Security*, 17(1):126–142, 2023.
10. Erik Lewerenz. Deploying post quantum cryptography on newspace satellites. In *Small Satellite Conference*, August 2025.
11. ArduPilot Development Team. Mavlink basics. https://ardupilot.org/dev/docs/mavlink-basics.html, 2025. Accessed July 2025.
12. Branislav S. and Milos P. A secure communication protocol for unmanned aerial vehicles. In *Communications in Computer and Information Science (CCIS), Vol. 70*, pages 71–87. Tech Science Press, 2021.
13. MAVLink Developer Community. Protocol overview – mavlink guide. https://mavlink.io/en/about/overview.html, 2025. Accessed July 2025.
14. NIST Post-Quantum Cryptography Standardization. Nist announces 14 candidates to advance to the second round of additional digital signatures. https://csrc.nist.gov/news/2024/pqc-digital-signature-second-round-announcement, 2024. Accessed July 2025.
15. NIST Post-Quantum Cryptography Standardization. NIST submission: HQC. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions, 2023. Accessed July 2025.
16. NIST Post-Quantum Cryptography Standardization. NIST submission: Ntruencrypt. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions, 2023. Accessed July 2025.
17. A. Perrig, R. Canetti, J. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. In *Proc. IEEE Symposium on Security and Privacy*, pages 56–73. IEEE, 2000.
18. Vijay Varadharajan and Neeraj Suri. Security challenges when space merges with cyberspace. *Space Policy*, 67:101600, 2024.
19. Secure-IC. Mitigating side-channel attacks in post quantum cryptography for space systems. https://www.secure-ic.com/mitigating-side-channel-attacks-in-pqc/, 2023.
20. Attila A. Yavuz and Gurkan Gur. NSF-SNSF: A Resilient and Efficient Cyber-security Fabric and Evaluation Framework for Future Integrated Satellite-Terrestrial Networks (SATUQ). National Science Foundation Award Abstract #2444615, University of South Florida, Oct 2024. Accessed July 2025; project homepage not publicly available.