Analysis of the Use of Module Lattice Key-Encapsulation Mechanism in Delay Tolerant Networks: A Survey

Fábio Moreira dos Santos, Mark G. Reith and Daniel Koranek
Air Force Institute of Technology, Wright-Patterson AFB, USA

fabio.moreirados_santos.br@au.af.edu
mark.reith.3@au.af.edu
daniel.koranek@us.af.mil

Abstract: Cryptography plays a fundamental role in information security, being directly related to maintaining important properties such as confidentiality and integrity. Many of the algorithms that form the basis of cryptography are based on mathematically difficult computational problems, such as prime number factorization and discrete logarithm. However, the use of quantum computing algorithms poses a threat to some of these cryptographic systems, making communication systems and protocols that use them vulnerable. One example is Delay-Tolerant Networks (DTNs), which have high applicability in space systems and military contexts, but present challenging characteristics for secure implementation. One initiative to combat this threat is the development of algorithms resistant to quantum attacks, collectively known as post-quantum cryptography. These algorithms are based on other mathematical classes that do not have a known optimized solution for quantum or classical computers, but, on the other hand, present greater computational, storage, and data transmission demands. Due to these characteristics, their use must be evaluated according to the context, considering the degree of security required in conjunction with processing, memory, and routing limitations. Thus, this work aimed to conduct a survey of the main characteristics and challenges of cryptographic systems to counter quantum cryptanalysis, paying special attention to the post-quantum algorithm Module-Lattice Key-Encapsulation Mechanism (ML-KEM), as well as its vulnerabilities to hardware-level implementation attacks and spaceborne radiation environments. Furthermore, the main architectural characteristics of DTNs were presented, and security aspects and challenges described in the Bundle Protocol Security (BPSec)—specifically regarding the amplification of message-flooding vulnerabilities under expanded post-quantum payloads—were addressed. Finally, suggestions for future work were presented based on opportunities identified throughout the study.

Keywords: Quantum computing, Delay-tolerant networks, Post-quantum cryptography, Bundle protocol

1. Introduction

The use of cryptography is fundamental for information security, contributing to systems that transmit, store, or manipulate data achieving fundamental characteristics like confidentiality and integrity, in addition to others such as authentication. Such systems vary widely according to criteria such as computational power and data transfer through computer networks. These characteristics can impose additional restrictions on the use of cryptography, such as delay-tolerant or disruption-tolerant networks (DTN), designed for delayed/disrupted connectivity environments.

On the other hand, attacks on encryption systems known as cryptanalysis can lead to the compromise of an algorithm's key, and consequently the data of those who use it. For example, the Data Encryption Standard (DES) was a symmetric encryption standard that, after years of use, became vulnerable due to the increase in computational power available for cryptanalysis. This led to the development of a new, more computationally expensive symmetric cryptographic standard, the Advanced Encryption Standard (AES).

However, new attacks are constantly being developed, making use of new algorithms and increased computing power, such as the latest quantum cryptanalysis algorithms. This new threat has led to the need to develop new cryptographic algorithms, which gave rise to post-quantum cryptography. These algorithms, however, may require greater computational power and a larger volume of stored and transmitted cryptographic data, which poses an additional challenge for DTN networks.

Therefore, researchers must analyze the use of schemes that allow for the secure establishment of keys, while simultaneously meeting the constraints of the systems in which they will be applied. To understand the need for post-quantum cryptography in military and satellite DTN networks, this study first evaluates the imminent threats posed by quantum cryptanalysis.

2. Quantum Cryptanalysis

2.1 Grover's Algorithm and its Impact on Symmetric Cryptography and Hashing

Grover's algorithm is a quantum algorithm for searching unstructured databases, such as an unordered vector of numerical data. The algorithm offers a quadratic speedup compared to classical methods, that is, while a classical computer requires on the order of N evaluations to find an item in a space of N elements in the worst case, Grover's algorithm requires only $N^{0.5}$ operations (Preston, 2023).

This result has direct implications for AES. Because of it, systems need to use at least AES-256 (32 bytes, of 256 bits, key) to remain resistant to Grover's algorithm (Rao et al., 2017). Hash functions are also targeted by the algorithm, making the use of SHA-256 necessary to resist quantum cryptanalysis (Preston, 2023).

2.2 Shor's Algorithm: History and Implementation Challenges

Another quantum algorithm applicable to cryptanalysis was proposed by Peter Shor in 1994. This algorithm solves integer factorization and discrete logarithm problems in polynomial time, offering an exponential speedup over the best-known classical algorithms, such as the Number Field Sieve (Shor, 1997). Also, theoretical improvements have been proposed, such as Regev's algorithm, which reduces the number of quantum gates required to $O(n^{3/2})$ (Regev, 2025). Such results directly compromise widely used public-key cryptosystems, including RSA and Elliptic Curve Cryptography (ECC) (Rao et al., 2017).

The practical implementation of Shor's algorithm, however, faces significant physical challenges, mainly related to quantum decoherence—the loss of coherence due to the interaction of the system with the environment (Chuang et al., 1995). Historically, experimental demonstrations have been limited to small numbers due to the requirement for precise control over the qubits.

One of the first notable implementations occurred in 2001, using Nuclear Magnetic Resonance (NMR) to factor the number 15 using 7 qubits. Although successful, the experiment highlighted the difficulty of scalability due to decoherence and the complexity of spin coupling networks (Vandersypen et al., 2001).

To overcome resource limitations, later approaches focused on circuit optimization. In 2012, a photonic implementation factored the number 21 using a "qubit recycling" technique. This iterative version of the algorithm replaces the n-qubit control register with a single qubit reused n times, reducing the total resource demand to about one-third of the standard protocol, demonstrating a viable path to scalability (Martín-López et al., 2012).

More recently, hybrid approaches such as Variational Quantum Factoring (VQF) have been tested on superconducting processors. Experiments factoring larger numbers have revealed that, in addition to traditional decoherence, coherent errors represent dominant barriers to the successful execution of quantum optimization algorithms (Karamlou et al., 2021).

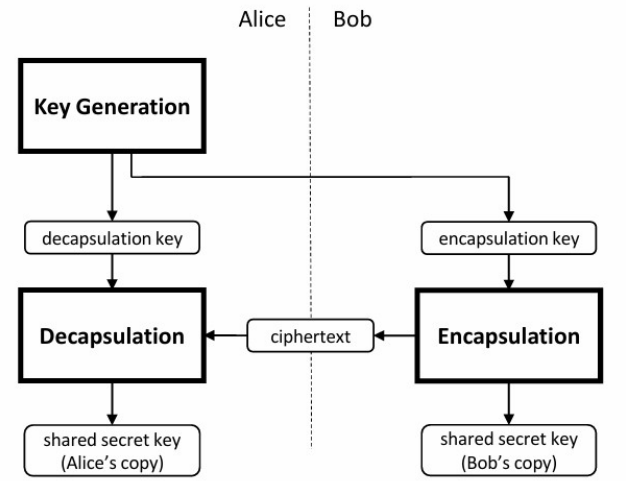
Although implementing the Shor's algorithm is still a challenge, continuous progress has been made, leading to the need to seek new cryptographic solutions to prevent the compromise of information security.

3. Module-lattice Key-encapsulation Mechanism

To counter the previously mentioned quantum cryptanalysis algorithms, one approach involved developing a new class of classical cryptographic algorithms, collectively known as post-quantum cryptography (Bavdekar et al., 2023). Although other methods have been studied (Bavdekar et al., 2023), lattice-based cryptography has been standardized by NIST for use in key establishment and also in digital signatures (NIST, 2024a, 2024b). Lattices are algebraic structures where certain computational problems, such as the Module Learning With Errors (MLWE) problem, are believed to be intractable for both classical and quantum computers.

For key establishment, the first chosen algorithm was the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM). ML-KEM consists of three fundamental operations (Alagic et al., 2025), which are also represented in the scheme in Figure 1:

- Key Generation: a pair of encapsulation/decapsulation keys is generated by one party (Alice), and the encapsulation key is sent to the other party (Bob);
- Encapsulation: after receiving the encapsulation key, Bob performs an operation that generates the shared secret in both plaintext and ciphertext form, which is then sent to Alice; and
- Decapsulation: Alice receives the ciphertext and uses her key to decrypt the shared secret.



Note. Source: Alagic et al. (2025)

Figure 1: ML-KEM overview

The process described above can occur in two distinct ways, ephemeral or static. In the first, for each generation of a shared secret, the entire process must be performed, and the generated keys must be discarded after use. In the second, the key generation is done once, and the encapsulation key is distributed to all parties who wish to generate a shared secret. It should be noted that the generated secrets are distinct from each other (Alagic et al., 2025).

The proponents of the algorithm specified three sets of parameters: ML-KEM-512, ML-KEM-768, and ML-KEM-1024, targeting security categories 1, 3, and 5, respectively. Table 1 shows the size values for the three configurations.

Table 1: ML-KEM settings (values in bytes)

Algorithm	Encapsulation key	Decapsulation key	Ciphertext	Secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

Note. Source: NIST (2024)

Regarding practical deployment, ML-KEM demonstrates high versatility and can be implemented across diverse software and hardware architectures, including central processing units (CPUs), graphics processing units (GPUs), application-specific integrated circuits (ASICs), and field-programmable gate arrays (FPGAs) (Nguyen et al., 2025). This adaptability extends to extreme operational environments such as space systems, where the algorithm has proven viable on radiation-hardened FPGAs and embedded space-grade processors (Kim, 2026).

However, deployment in these specialized environments is bounded by severe physical and hardware constraints that mandate careful resource optimization (Kim, 2026; Nguyen et al., 2025). Most critically, spaceborne implementations are generally prohibited from utilizing standard external DDR memory due to its susceptibility to radiation-induced single-event upsets (SEUs), forcing the cryptographic subsystem to rely entirely on severely limited on-chip static memory (Kim, 2026). Furthermore, these systems must operate within strict power budgets while handling the transmission of larger post-quantum keys over highly constrained telemetry bandwidths (Kim, 2026).

The security of ML-KEM against both classical and quantum computing adversaries is fundamentally derived from the hardness of the MLWE problem, which establishes a baseline security of indistinguishability under chosen-plaintext attack (IND-CPA) (Avanzi et al., 2021). According to the NIST evaluation criteria, this passive IND-CPA security framework is considered sufficient for purely ephemeral key exchange protocols, (NIST, 2016). For the static deployments, the scheme applies a Fujisaki-Okamoto (FO) transform to the underlying IND-CPA-secure encryption to achieve the required indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) (Avanzi et al., 2021).

Despite its robust mathematical foundations, practical deployments of ML-KEM remain susceptible to physical hardware exploits, which is a critical consideration for exposed nodes in Delay Tolerant Networks (Nguyen et al., 2025; Renita et al., 2025). These physical vulnerabilities bypass theoretical protections and are predominantly divided into passive Side-Channel Attacks (SCA) and active Fault Injection Attacks (FIA) (Ravi et al., 2024).

Passive SCAs exploit unintentional physical leakages, such as power consumption and electromagnetic (EM) emanations (Renita et al., 2025). The decapsulation phase is particularly vulnerable; attackers can utilize Deep Learning-enhanced Side-Channel Analysis (DL-SCA) to extract secret polynomial coefficients during Number Theoretic Transform (NTT) or point-wise multiplication operations (Hoang et al., 2024; Renita et al., 2025). This technique is highly efficient, requiring as few as 50 traces, and can successfully compromise even hardware implementations that use parallel architectures (Hoang et al., 2024). By exploiting these leakages, adversaries can construct practical plaintext-checking or decryption-failure oracles to systematically recover the secret key (Ravi et al., 2024).

In addition to power and EM leakages, ML-KEM is threatened by timing-based vulnerabilities, notably the KyberSlash exploits (Bernstein et al., 2024; Ji et al., 2025). These vulnerabilities occur when compilers optimizing for code size inadvertently introduce variable-time division operations during ciphertext compression or message decoding (Bernstein et al., 2024). Because the execution time of these operations depends on the secret inputs, they reliably leak key information, allowing systems to be compromised remotely or without advanced physical measurement probes (Bernstein et al., 2024).

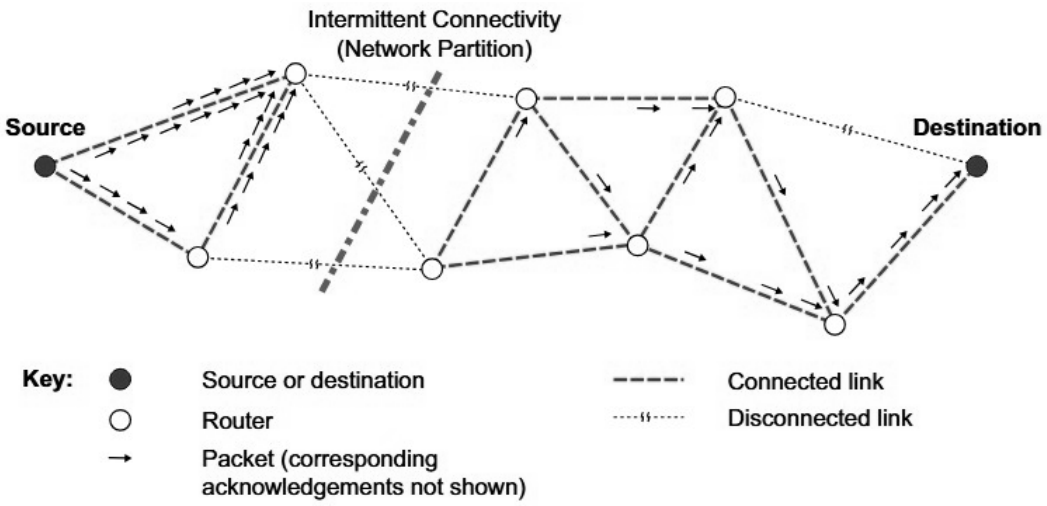
Finally, ML-KEM is also threatened by active manipulation through Fault Injection Attacks (FIA), which deliberately induce transient hardware errors (Renita et al., 2025). Advanced FIA techniques include loop-abort faults induced via electromagnetic pulses, which target the standardized KECCAK hash function across all operational phases (Wang et al., 2025). These faults allow adversaries to bypass permutations or zeroize crucial arrays to effortlessly recover secret random seeds (Wang et al., 2025). Other critical fault vectors include corrupting NTT twiddle factors, forcing nonce reuse during the sampling of ephemeral secrets, or using clock glitching to completely skip the final ciphertext equality check—effectively downgrading the protocol to weaker indistinguishability under chosen-plaintext attack (IND-CPA) security (Ravi et al., 2024; Ji et al., 2025).

4. Delay/Disruption Tolerant Networks

Delay-Tolerant and Disruption-Tolerant Networks (DTNs) are designed to operate in contexts where the use of the traditional TCP/IP protocol stack presents limitations, such as high error rates, delays that can reach the order of days, and lack of end-to-end connectivity (Cerf et al., 2007; Gao et al., 2015). DTNs can be applied in scenarios such as underwater networks, satellite networks, sensor networks, or battlefield networks (Cerf et al., 2007; Gao et al., 2015). Bravo et al. (2025) analyzed the use of LunaNet, which uses the DTN architecture, on the International Space Station for a period of eighteen days, conducting a series of experiments to verify its behavior and performance (Bravo et al., 2025). The characteristics of DTNs are also being integrated into vehicular network projects, Vehicular-DTN (Pereira, 2011). Some studies have also been conducted on the application of DTNs in rural areas (Abdeljabar et al., 2025; Hanifah et al., 2025).

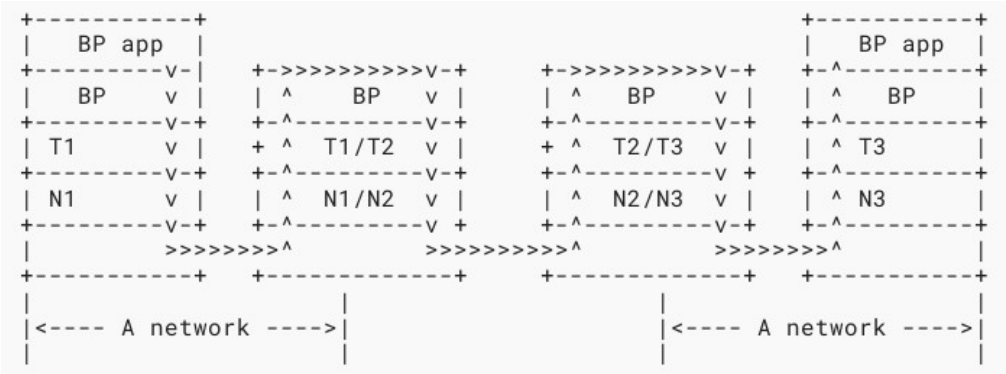
A disruption scenario is represented in Figure 2, where the network becomes partitioned, preventing the routing of packets between the source and destination. To address the problem of lack of connectivity and high error rates, the nodes belonging to DTNs use a store-and-forward approach in which packets are stored so that they can be transmitted when the link is re-established (Cerf et al., 2007).

DTNs utilize the Bundle Protocol (BP), where the term "bundle" refers to the packet used. BP acts as an overlay layer over other network and transport protocol stacks, called Convergence Layers, allowing different networks to be interconnected (Burleigh et al., 2022). Figure 3 shows a DTN formed by two different networks connected so that BP applications (BP app) can exchange messages. The variety of Convergence Layers is represented by the pairs Tx/Nx, with x varying from 1 to 3.



Note. Adapted from NASA

Figure 2: Disrupted DTN where the source and destination nodes are unreachable



Note. Source: Burleigh et al. (2022)

Figure 3: Overlay BP with different stack convergence layers

Security in DTN networks is provided by the Bundle Protocol Security (BPSec) protocol, defined in RFC 9172. BPSec was designed to operate independently of the network topology, applying security services directly to the data, rather than protecting the communication channel, since end-to-end connectivity is not guaranteed (Birrane & McKeever, 2022). The protocol does not impose fixed cryptographic algorithms; instead, it uses context identifiers to abstract the cipher suite and parameters used (Birrane et al., 2023).

The introduction of post-quantum algorithms imposes additional challenges on key management, mainly due to the larger size of keys and signatures. BPSec facilitates this transition by allowing additional security parameters (such as encapsulated keys or salts) to be transported within the security blocks themselves (Birrane et al., 2023). Key management must consider that, in a DTN, a key valid at the time of sending may have expired by the time of reception, requiring security policies that take network latency into account. Not only that, but one must also consider the challenge of distributing keys in an environment where there may not be end-to-end connectivity for the execution of the protocols (Birrane et al., 2023).

Building on these connectivity challenges, the store-carry-and-forward paradigm uniquely exposes Delay Tolerant Networks (DTNs) to a range of operational threats. Because DTNs strictly require cooperation between intermittent nodes to deliver messages, they are highly susceptible to routing misbehavior (Nabais et al., 2021). The most critical threats include Black-hole attacks, where compromised nodes silently drop received messages instead of forwarding them, and Wormhole attacks, where adversaries tunnel packets through hidden, low-latency links to manipulate the perceived network topology (Altaweel et al., 2023; Nabais et al., 2021). Additionally, attackers may launch Sybil attacks by forging or stealing multiple identities to aggressively influence routing decisions and intercept traffic, exploiting the fundamental nature of opportunistic contacts to disrupt the network (Altaweel et al., 2023).

Furthermore, the resource constraints of DTN nodes make them prime targets for Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks (Khalid et al., 2023; Zekkori et al., 2021). Adversaries may deploy flooding attacks, overwhelming the network with genuine, replicated, or entirely forged bundles to rapidly deplete node buffers and congest available wireless bandwidth (Khalid et al., 2023; Zekkori et al., 2021). In environments like space information networks, where components are physically inaccessible and structurally constrained, these resource-exhaustion attacks can be catastrophic. By forcing legitimate nodes to drop crucial packets due to buffer overflow, flooding halts communication and critically degrades the network's packet delivery ratio (Sharmin et al., 2025; Zekkori et al., 2021).

5. SWOT Analysis

5.1 Strengths

- Robust Quantum Resistance: ML-KEM utilizes the Fujisaki-Okamoto (FO) transform to provide strong indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2), ensuring that data remains secure against both classical and future quantum adversaries.
- Computational Efficiency: Compared to other post-quantum algorithms, ML-KEM is efficient for memory and processing-constrained environments because it leverages the Number Theoretic Transform to optimize polynomial multiplications with minimal resource overhead.
- Protocol Adaptability: The Bundle Protocol Security standard utilized in DTNs allows the integration of post-quantum cryptography without requiring fundamental architectural changes.

5.2 Weaknesses

- Resource Overhead: ML-KEM demands significantly larger key and ciphertext sizes compared to classical cryptography; for instance, ML-KEM-768 requires an 1184-byte encapsulation key and a 1088-byte ciphertext. This heavy data footprint might conflict with the buffer constraints of DTN nodes.
- Synchronous Assumptions in Asynchronous Networks: ML-KEM key exchange assumes prompt communication, which is not always possible in DTNs. A post-quantum key valid at the time of transmission may expire before reaching its destination, complicating key management.

5.3 Opportunities

- Environmental Immunity to Implementation Attacks: Assuming the nodes are physically inaccessible (e.g., satellites), it’s practically impossible for adversaries to attach measurement probes or use electromagnetic equipment to launch passive Side-Channel Attacks or active Fault Injection Attacks. Furthermore, the extreme latency and frequent disruptions inherent to the DTN architecture completely mask the minute clock-cycle variations required to execute remote timing attacks, rendering vulnerabilities like the KyberSlash exploits ineffective.
- Specialized Hardware Integration: Advances in space-grade Field-Programmable Gate Arrays (FPGAs) allow ML-KEM to be implemented efficiently using entirely on-chip static memory, avoiding the need for external DDR memory.

5.4 Threats

- Amplification of Flooding Attacks: Because DTNs are highly susceptible to DoS and flooding attacks, the substantially larger payload of ML-KEM keys and ciphertexts makes it much easier for remote adversaries to rapidly exhaust node buffers and wireless bandwidth.
- Environmental Faults: Even without physical access by a human attacker, space-based DTN nodes are constantly bombarded by galactic cosmic rays and radiation. This environment induces Single-Event Upsets —random bit flips in memory that can corrupt keys or intermediate computations, effectively mirroring the disruption of a malicious Fault Injection Attack. This threat is particularly acute for ML-KEM, because its expansive public key and ciphertext sizes present a vastly larger operational memory profile than classical cryptography, reducing the mathematical probability of error-free state retention across the system.

6. Future Work

Based on the topic discussed and the SWOT analysis, three recommendations for future work involving the use of post-quantum cryptography in systems connected to DTNs are presented.

- Investigate decentralized, latency-aware key management policies for ML-KEM in DTNs. Future studies must specifically address the 'Synchronous Assumptions' weakness by exploring how to handle key expiration, asynchronous certificate revocation, and delayed authentication in an environment where a post-quantum key may expire before reaching its destination;
- Evaluate the performance impact of ML-KEM's large cryptographic payloads on various DTN routing protocols. Because the substantial size of post-quantum keys exacerbates the network's susceptibility to resource-exhaustion and flooding attacks, future research should investigate lightweight, randomized routing algorithms (such as k-RAND) or anomaly detection mechanisms to dynamically protect node buffers from being overwhelmed by cryptographic traffic; and
- Explore the hardware-software co-design of Hardware Security Modules (HSMs) optimized for post-quantum cryptography in space systems. Future work should focus on implementing ML-KEM within the strict confines of on-chip static memory (avoiding DDR), while developing fault-tolerant architectures to mitigate Single-Event Upsets (SEUs) from cosmic radiation, which can fatally corrupt keys and mirror malicious Fault Injection Attacks.

7. Conclusion

The imminent threat of quantum computing requires a shift towards post-quantum cryptography to ensure long-term security. This work explored this transition, focusing on the Modular Lattice-Based Key Encapsulation Mechanism (ML-KEM) and the dynamics of deploying it within Delay-Tolerant Networks (DTNs) for space systems.

While ML-KEM is theoretically robust, practical deployments are susceptible to physical hardware exploits, such as passive Side-Channel Attacks (SCA), active Fault Injection Attacks (FIA), and remote timing vulnerabilities like KyberSlash. However, the unique environmental characteristics of DTNs actually provide a natural defense against these threats. For physically inaccessible DTN nodes like satellites, it is practically impossible for adversaries to attach measurement probes required to launch local SCAs or FIAs. Furthermore, the extreme latency and frequent disruptions inherent to the DTN architecture completely mask the minute clock-cycle variations necessary to execute remote timing attacks, rendering vulnerabilities like KyberSlash ineffective.

Despite this environmental immunity to certain implementation attacks, significant challenges remain. The substantial resource overhead of ML-KEM, specifically its larger key and ciphertext sizes, amplifies existing network-level vulnerabilities in DTNs. This heavy data footprint makes constrained nodes much more susceptible to resource-exhaustion and flooding attacks. Additionally, space-based DTNs must contend with radiation-induced single-event upsets (SEUs) which corrupt keys and intermediate computations, effectively mirroring the disruption of malicious fault injections without requiring a human attacker.

Addressing these challenges will require investigating decentralized, latency-aware key management policies, developing lightweight routing algorithms to protect against payload-amplified flooding, and exploring fault-tolerant co-designs to mitigate radiation hazards in space systems.

Ethics Declaration: Ethical clearance was not required for this research, as the study involves a survey of existing literature and does not involve human participants, animal subjects, or the collection of sensitive personal data.

AI Declaration: Google NotebookLM was utilized during the development of this paper as a tool for self-study and to enhance the comprehension of the technical concepts.

Disclaimer Statement: "The views expressed are those of the author and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government."

References

Abbas, A., & Hasan, R. (2024). A multi-attribute-based data forwarding scheme for delay tolerant networks. *Journal of Supercomputing*, *80*(5).

Abdeljabar, S., Zennaro, M., & Alouini, M.-S. (2025). Delay Tolerant Networking to Extend Connectivity in Rural Areas Using Public Transport Systems: Design And Analysis. IEEE Internet of Things Journal, 1–1. doi:10.1109/JIOT.2025.3640016

Ahmad, A., & Jagatheswari, S. (2024). Lattice-Based Three Party Authenticated Key Agreement Scheme in Medical IoT for Post-Quantum Environment. *IEEE Access*, *12*, 157247–157259. doi:10.1109/ACCESS.2024.3483971

Alagic, G., Barker, E., Chen, L., Moody, D., Robinson, A., Silberg, H., & Waller, N. (2025). Recommendations for key-encapsulation mechanisms. *NIST Special Publication (SP)*, 800-227.

Altaweel, A., Aslam, S., & Kamel, I. (2023). Security attacks in opportunistic mobile networks: A systematic literature review. Journal of Network and Computer Applications, 220, Article 103730. https://doi.org/10.1016/j.jnca.2023.103730

Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2021). CRYSTALS-Kyber algorithm specifications and supporting documentation (Round 3 submission). pq-crystals.org. https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf

Bagchi, P., Roy, A., Wazid, M., Das, A. K., Bhargava, B. K., & Park, Y. (2026). Big Data Analytics-Envisioned Quantum-Safe Lattice-Based Three-Party Authenticated Key Agreement Protocol for Cloud IoT-Enabled Healthcare Applications. *IEEE Transactions on Dependable and Secure Computing*, *23*(1), 368–385. doi:10.1109/TDSC.2025.3605524

Bavdekar, R., Jayant Chopde, E., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations. *2023 International Conference on Information Networking (ICOIN)*, 146–151. doi:10.1109/ICOIN56518.2023.10048976

Bernstein, D. J., Bhargavan, K., Bhasin, S., Chattopadhyay, A., Chia, T. K., Kannwischer, M. J., Kiefer, F., Paiva, T., Ravi, P., & Tamvada, G. (2024). KyberSlash: Exploiting secret-dependent division timings in Kyber implementations (Cryptology ePrint Archive, Report 2024/1049). International Association for Cryptologic Research. https://eprint.iacr.org/2024/1049

Birrane III, E. J., Heiner, S., & McKeever, K. (2023). Securing Delay-Tolerant Networks with BPSec. John Wiley & Sons.

Birrane, III, E. & McKeever, K. (2022). RFC 9171: Bundle Protocol Security

Blake, I. F., & Garefalakis, T. (2004). On the complexity of the discrete logarithm and Diffie–Hellman problems. *Journal of Complexity*, *20*(2-3), 148-170.

Bravo, A. M., Ochoa, A. M., Hill, E., Acosta, V., & Ahmed, S. (2025). Operationalizing LunaNet Service Provider Delay Tolerant Networks on the International Space Station. 2025 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), 1–6. doi:10.1109/WiSEE57913.2025.11229867

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In *2018 IEEE European symposium on security and privacy (EuroS&P)* (pp. 353-367). IEEE.

Burleigh, S., Fall, K., & Birrane, III, E. (2022). RFC 9171: Bundle protocol version 7.

Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K. & Weiss, H. (2007). RFC 4838: Delay-tolerant networking architecture.

Chuang, I. L., Laflamme, R., Shor, P. W., & Zurek, W. H. (1995). Quantum computers, factoring, and decoherence. Science, 270(5242), 1633–1635.

Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman (pp. 365-390)

Gao, L., Yu, S., Luan, T. H., & Zhou, W. (2015). *Delay tolerant networks* (pp. 9-16). Springer International Publishing.

Hanifah, S., Kurnianingrum, I. P., Jamil, A. R. A., Yovita, L. V., & Wibowo, T. A. (2025). Performance Evaluation of Real Delay Tolerant Network in Rural Environments. 2025 IEEE International Symposium on Future Telecommunication Technologies (SOFTT), 256–261. doi:10.1109/SOFTT67007.2025.11212896

Hoang, A. T., Kennaway, M., Pham, D. T., Mai, T. S., Khalid, A., Rafferty, C., & O'Neill, M. (2024). Deep learning enhanced side channel analysis on CRYSTALS-Kyber. 2024 25th International Symposium on Quality Electronic Design (ISQED), 1–8. https://doi.org/10.1109/ISQED60706.2024.10528674

Ji, R., Eswari Devi, N., & Annadurai, S. (2025). Side-channel and fault attacks on ML-KEM: A survey of vulnerabilities and countermeasures. In 2025 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET) (pp. 1-6). IEEE. https://doi.org/10.1109/WiSPNET64060.2025.11004937.

Karamlou, A. H., Simon, W. A., Katabarwa, A., Scholten, T. L., Peropadre, B., & Cao, Y. (2021). Analyzing the performance of variational quantum factoring on a superconducting quantum processor. npj Quantum Information, 7(156).

Khalid, W., Ahmed, N., Khan, S., Ullah, Z., & Javed, Y. (2023). Simulative survey of flooding attacks in intermittently connected vehicular delay tolerant networks. IEEE Access, 11, 75628–75656. https://doi.org/10.1109/ACCESS.2023.3297439

Kim, H. (2026). Post-quantum cryptography for space systems: Algorithms, implementation, and design constraints—A systematic survey. Acta Astronautica, 246, 863–886. https://doi.org/10.1016/j.actaastro.2026.002730

Liu, G., Li, W., Yuan, C., Wang, N., Ma, C., Mu, N., Liu, Z., Liu, Y., Xiang, T. (2025). LBRAKA: Lattice-Based Robust Authenticated Key Agreement for VANETs. *IEEE Transactions on Vehicular Technology*, *74*(4), 6533–6547. doi:10.1109/TVT.2024.3515072

Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., & O'Brien, J. L. (2012). Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature Photonics, 6, 773–776.

Nabais, C., Pereira, P. R., & Magaia, N. (2021). BiRep: A reputation scheme to mitigate the effects of black-hole nodes in delay-tolerant Internet of Vehicles. Sensors, 21(3), Article 835. https://doi.org/10.3390/s21030835

National Institute of Standards and Technology. (2016). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process [Call for Proposals]. U.S. Department of Commerce. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

National Institute of Standards and Technology. (2024). Module-Lattice-Based Digital Signature Standard (FIPS 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. IEEE Access, 13, 89003–89024. https://doi.org/10.1109/ACCESS.2025.3571307

Pereira, P. R., Casaca, A., Rodrigues, J. J., Soares, V. N., Triay, J., & Cervelló-Pastor, C. (2011). From delay-tolerant networks to vehicular delay-tolerant networks. *IEEE Communications Surveys & Tutorials*, *14*(4), 1166-1182.

Preston, R. H. (2023). Applying Grover's Algorithm to Hash Functions: A Software Perspective. IEEE Transactions on Quantum Engineering, 4, 1-10.

Rao, S. K., Mahto, D., Yadav, D. K., & Khan, D. A. (2017). The AES-256 Cryptosystem Resists Quantum Attacks. International Journal of Advanced Research in Computer Science, 8(3), 404-408.

Ravi, P., Chattopadhyay, A., D'Anvers, J. P., & Baksi, A. (2024). Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results. ACM Transactions on Embedded Computing Systems, 23(2), 1–54. https://doi.org/10.1145/3603170

Regev, O. (2025). An Efficient Quantum Factoring Algorithm. Journal of the ACM, 72(1), Article 10.

Rezaei, P., & Derakhshanfard, N. (2025). Reinforcement learning based routing in delay tolerant networks. *Wireless Networks*, 1-15.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 800-207.

Sharmin, A., Mahmud, B. U., Nabi, N., Shaima, M., & Faruk, M. J. H. (2025). Cyber attacks on space information networks: Vulnerabilities, threats, and countermeasures for satellite security. Journal of Cybersecurity and Privacy, 5(3), 76–103. https://doi.org/10.3390/jcp5030076

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5), 1484–1509.

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414, 883–887.

Wang, Y., Yu, J., Qu, S., Zhang, X., Li, X., Zhang, C., & Gu, D. (2025). Mind the faulty KECCAK: A practical fault injection attack scheme applied to all phases of ML-KEM and ML-DSA. IEEE Transactions on Information Forensics and Security, 20, 10035–10048. https://doi.org/10.1109/TIFS.2025.3607242

Wei, G., Fan, K., Zhang, K., Wang, H., Li, H., & Yang, Y. (2024). Quantum-Safe Lattice-Based Certificateless Anonymous Authenticated Key Agreement for Internet of Things. *IEEE Internet of Things Journal*, *11*(5), 9213–9225. doi:10.1109/JIOT.2023.3323275

Yan-Tao, Z. (2018). Lattice Based Authenticated Key Exchange with Universally Composable Security. *2018 International Conference on Networking and Network Applications (NaNA)*, 86–90. doi:10.1109/NANA.2018.8648765

Zekkori, H., Agoujil, S., & Qaraai, Y. (2021). Effective controlling scheme to mitigate flood attack in delay tolerant network. International Journal of Computer Networks and Applications, 8(5), 585–596. https://doi.org/10.22247/ijcna/2021/209989