*A Report*

*on*

**Securing Satellite Communication for ISS Using Post-Quantum Cryptography**

*carried out as part of the course CSE CS3203 Submitted by*

***Dhruv Mendiratta (229301807)***

***Kunal Sinha (220301702)***

***VI-CSE***

*in partial fulfilment for the award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

In

**Computer Science & Engineering**



*Under the Guidance of*

*Guide Name: Dr. Anil Kumar*

**1 Abstract**

A symbol of global collaboration, scientific advancement, and human success in space exploration is the International Space Station (ISS). Its ability to transmit data, coordinate systems, and manage remotely is largely dependent on continuous and secure satellite communications. However, the need to secure these channels has become more important as cyber threats get more complex. Traditional encryption techniques like RSA and ECC are vulnerable due to the unique challenge posed by the expanding potential of quantum computing [9]. Post-quantum cryptography (PQC) standards must be adopted in light of the changing threat landscape [10].

This study investigates the use of CRYSTALS-KYBER, a lattice-based PQC algorithm known for its effectiveness and robust security guarantees in environments with constraints, such as space systems [11]. In order to lay the groundwork for KYBER's resilience, the paper starts with a theoretical review of lattice cryptography and the Learning With Errors (LWE) problem [12]. After that, we examine KYBER's architecture, underlying cryptography, and advantages, such as its small key sizes, defence against quantum attacks, and computational viability [13].

We examine the 2007 Chinese cyberattack on American satellites using the Svalbard ground station [14] to put this research in a practical context. This case study serves as a warning about the repercussions of inadequate encryption protocols and draws attention to flaws in satellite-ground communication. This report illustrates how KYBER strikes a balance between security, performance, and deployment ease by comparing it to other PQC algorithms.

In order to ensure future-proof security for space infrastructure and beyond, this report ultimately calls for the quick integration of quantum-resistant cryptographic algorithms in mission-critical systems like the ISS [15].

**Table of Contents**

1 Abstract .................................................................................................................... 3  
2 Introduction .......................................................................................................... 5  
 2.1 Background ................................................................................................. 5  
 2.2 Purpose ..................................................................................................... 5  
 2.3 Overview .................................................................................................. 6  
3 Theoretical Background .................................................................................. 7  
 3.1 Lattice-Based Cryptography and Ring-LWE .......................................... 7  
 3.2 CRYSTALS-KYBER Design and Principles .......................................... 7  
 3.3 Strengths and Weaknesses .................................................................... 8  
4 Analysis and Discussion ................................................................................ 9  
 4.1 Security Analysis ...................................................................................... 9  
 4.2 Performance and Practicality .................................................................. 9  
 4.3 Comparison with PQC Alternatives ..................................................... 10  
5 Case Study .................................................................................................... 11  
 5.1 Introduction to the Case Study ............................................................ 11  
 5.2 Description of the 2007 Svalbard Attack ............................................ 11  
 5.3 Impact and Lessons Learned ................................................................ 12  
 5.4 Future Implications ................................................................................. 12  
6 Conclusion ..................................................................................................... 13  
7 References .................................................................................................... 14

**2 Introduction**

**2.1 Background**

The ISS is an example of a multinational collaboration on important space research and experimentation. A key component of the ISS's everyday operations is the satellite communication system that links it to partner organisations, scientific teams, and ground control. Cyber threats that target these kinds of communication networks have increased over time. Strong encryption techniques are essential, as evidenced by the 2007 Svalbard ground station attack, which revealed weaknesses in satellite-ground interfaces [1].

The fundamental presumptions of conventional cryptography are being called into question as quantum computing advances. Under quantum attack models, encryption protocols that depend on discrete logarithms and integer factorisation, such as RSA and ECC, are becoming outdated [2]. As a result, post-quantum cryptography algorithms are not only novel but also necessary.

**2.2 Purpose**

The purpose of this report is to investigate the application and importance of CRYSTALS-KYBER, a lattice-based post-quantum cryptography algorithm chosen by NIST, in protecting ISS satellite communications. Among the goals are:

* Investigating the theoretical underpinnings of cryptography based on lattices.
* Examining the design, security, and usefulness of CRYSTALS-KYBER.
* Using a real-world case study, illustrate the urgency of the post-quantum transition.

**2.3 Overview**

There are six main sections to the report. After this introduction, Section 3 explores the design rationale of CRYSTALS-KYBER and the theoretical underpinnings of lattice-based cryptography. A thorough examination of the algorithm's security, effectiveness, and relative position to other PQC techniques is provided in Section 4. The 2007 Chinese cyberattack through the Svalbard ground station is examined in Section 5, which also links the necessity of quantum-safe encryption with satellite communications vulnerabilities. Section 6 wraps up the results and suggests some future paths.

**3 Theoretical Background**

**3.1 Lattice-Based Cryptography and Ring-LWE**

A subfield of post-quantum cryptography known as "lattice-based cryptography" is based on the difficulty of lattice problems, like Learning With Errors (LWE) and the Shortest Vector Problem (SVP) [3]. These cryptographic structures are strong because they can withstand both classical and quantum attacks. Practical lattice-based schemes frequently employ Ring-LWE, a structured form of LWE that improves efficiency [4]. By operating inside polynomial rings, it streamlines processes and drastically cuts down on computation time and key sizes.

**3.2 CRYSTALS-KYBER Design and Principles**

NIST selected CRYSTALS-KYBER, a module lattice-based key encapsulation mechanism (KEM), for post-quantum standardisation. It generates, encapsulates, and decapsulates keys using Module-LWE [5]. Included in the design are:

* Key Generation: Uses noise and uniformly sampled polynomials to generate a public-private key pair.
* Encapsulation: Creates a ciphertext and shared secret by combining the public key with a random seed.
* Decapsulation: Retrieves the shared secret using the private key.

These procedures maintain speed and compactness appropriate for embedded and restricted environments, while guaranteeing indistinguishability under chosen-ciphertext attacks (IND-CCA2 security).

**3.3 Strengths and Weaknesses**

**Strengths:**

* Provable security based on hard lattice problems.
* Efficient computation and small key sizes.
* Strong quantum resistance [6].

**Weaknesses:**

* Vulnerable to side-channel attacks if not implemented securely.
* Polynomial arithmetic can be complex to implement correctly.
* No widespread legacy support compared to RSA/ECC.

**4 Analysis and Discussion**

**4.1 Security Analysis: Quantum Resistance at Its Core**

CRYSTALS-KYBER's strong defence against quantum-based attacks is its main advantage. Even in the face of adaptive attacks, KYBER provides semantic security by taking advantage of the Module-LWE problem's difficulty [5]. Because of this, it is appropriate for critical infrastructure, like satellite systems, where low-latency, secure key exchange is crucial. Its suitability for secure ISS communication is further reinforced by its resistance to chosen-ciphertext attacks.

**4.2 Performance and Practicality: Real-World Efficiency**

With a small memory footprint, KYBER has been tuned for fast encryption and decryption [6]. Because of this, it is perfect for settings with limited resources, such as embedded systems on satellites. KYBER provides a better trade-off between key size and computational speed than RSA and ECC. For example, Kyber512 outperforms RSA's multi-kilobyte keys in terms of quantum security, requiring only 800 bytes for the public key [7].

**4.3 Comparison with PQC Alternatives**

In contrast to other post-quantum cryptography contenders such as NTRU, SABRE, and BIKE, KYBER achieves a balance between security, ease of use, and efficiency. In certain situations, NTRU is quicker, but KYBER offers a better key size to security ratio. Similar resistance is offered by SABRE, but KYBER's incorporation into the CRYSTALS suite gives it a standardised and structured advantage that fits with deployment requirements in the real world, particularly for space communication systems [8].

**5 Case Study**

**5.1 Introduction to the Case Study**

This section examines the 2007 cyberattacks on U.S. satellites via the Svalbard ground station in Norway, a significant real-world incident that highlights the risks associated with unprotected satellite communications. When evaluating how antiquated cryptographic infrastructures and inadequate security protocols can leave even valuable government assets vulnerable to foreign meddling, these incidents provide an essential case study [14].

**5.2 Description of the 2007 Svalbard Attack**

Attackers believed to be connected to Chinese state-sponsored organisations illegally accessed American Earth observation satellites, including Terra and Landsat-7, between 2007 and 2008. Exploiting unencrypted data links between the satellites and the Svalbard ground station allowed for the intrusions. The attackers disrupted the satellite systems at least four times, twice gaining complete command-and-control authority for a few minutes [14]. The breach represented a significant breakdown in satellite-ground authentication and encryption systems, despite the fact that no reports of permanent damage or data manipulation were made.

The use of antiquated or inadequate communication protocols that did not facilitate encrypted payload delivery or mutual authentication constituted the main cryptographic flaw. Because of these flaws, adversaries were able to covertly intercept, replay, and possibly spoof ground-station signals.

**5.3 Impact and Lessons Learned**

The defence and aerospace industries were rocked by the attacks. It became clear that sophisticated cyber threats could not be handled by satellite control systems, which frequently used outdated architectures. A number of lessons became apparent:

* All uplink and downlink transmissions must now be encrypted from beginning to end.
* Upgrades and security audits had to be performed on the ground station infrastructure.
* In order to transition from shared-key models to asymmetric public-key systems with more robust mathematical underpinnings, authentication protocols [14] [15].

The incident acted as a catalyst for the U.S. Air Force, NASA, and NOAA to review their cryptographic policies, enact mandatory hardware security modules (HSMs), and investigate new encryption paradigms, such as post-quantum cryptography (PQC) [16].

**5.4 Measures Taken Post-Attack**

Several quick actions were taken after the breach:

* Check for vulnerabilities in the signal pathways and satellite access points.
* Implementation of more robust access controls, such as two-factor authentication for ground command systems.
* Growing interest in transitional cryptographic models known as Hybrid Key Encapsulation Mechanisms (Hybrid KEMs), which combine quantum-safe and classical algorithms [16].
* Red-teaming exercises and internal simulations are used to test actual exploit scenarios.

The attacks also demonstrated the need for secure key exchange protocols that are impervious to man-in-the-middle attacks, which is a crucial benefit provided by PQC schemes such as CRYSTALS-KYBER [11].

**5.5 Future Implications and Relevance to PQC**

The Svalbard incident is particularly pertinent today, as classical encryption faces an existential threat from quantum computing. Confidential command streams could be cracked instantly if a similar breach happened today and the attacker had access to quantum decryption techniques.

This emphasises how crucial it is to switch to lattice-based post-quantum cryptography algorithms like CRYSTALS-KYBER, which provide:

* Compact keys that work well in space systems with limited bandwidth.
* Robust semantic security despite models of adaptive attacks.
* Hybrid encryption framework compatibility for a phased implementation [11][13][16].

Integrating PQC is not only a best practice, but also a requirement for upcoming space missions, including those involving the ISS.

**6 Conclusion**

Securing satellite infrastructure's communication systems is crucial as it becomes more and more essential to scientific research and national security. This study showed how the lattice-based post-quantum algorithm CRYSTALS-KYBER offers a dependable and cutting-edge way to encrypt satellite communications, especially for valuable targets like the ISS.

It is clear from assessing KYBER's cryptographic underpinnings, implementation efficiency, and practicality that its adoption is both possible and required. The Svalbard attack case study emphasises the risks associated with antiquated encryption and the significance of incorporating quantum-resistant solutions. In order to incorporate PQC into space communication protocols before quantum threats materialise, cooperation between cryptographers, aerospace engineers, and legislators is essential going forward.

**7 References**

[1] U.S.-China Economic and Security Review Commission. *2011 Report to Congress*. November 2011.

[2] Shor, Peter W. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” *35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994.

[3] Peikert, Chris. “A Decade of Lattice Cryptography.” *Foundations and Trends® in Theoretical Computer Science*, vol. 10, no. 4, 2016, pp. 283–424.

[4] Regev, Oded. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.” *Journal of the ACM*, vol. 56, no. 6, 2009, pp. 1–40.

[5] Bos, Joppe W., et al. “CRYSTALS–Kyber: A CCA-Secure Module-Lattice-Based KEM.” *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018.

[6] NIST. “Post-Quantum Cryptography Standardization.” *National Institute of Standards and Technology*, 2022.

[7] Albrecht, Martin R., et al. “The Cost of Post-Quantum Security.” *Lecture Notes in Computer Science*, vol. 10401, Springer, 2017, pp. 169–190.

[8] Hülsing, Andreas, et al. “Post-Quantum Cryptography: State of the Art.” *Communications of the ACM*, vol. 64, no. 4, 2021, pp. 72–81.

[9] Chen, Lily, et al. “Report on Post-Quantum Cryptography.” National Institute of Standards and Technology, 2016.

[10] Aggarwal, Divesh, et al. “Quantum Attacks on Public-Key Cryptosystems.” *Nature Reviews Physics*, vol. 1, 2019, pp. 367–380.

[11] Bos, Joppe W., et al. “CRYSTALS–Kyber: A CCA-Secure Module-Lattice-Based KEM.” *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018.

[12] Regev, Oded. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.” *Journal of the ACM*, vol. 56, no. 6, 2009, pp. 1–40.

[13] Howe, John. “A Practical Guide to Post-Quantum Cryptography.” *Cybersecurity Journal*, vol. 12, no. 2, 2021, pp. 110–124.

[14] U.S.-China Economic and Security Review Commission. “2011 Report to Congress.” November 2011.

[15] Bindel, Nina, et al. “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange.” *Post-Quantum Cryptography*, Springer, 2020, pp. 206–226.