MSc Cybersecurity, Privacy and Trust – South-East Technological University [SETU]

Evaluating CRYSTALS-Kyber: A Comprehensive Analysis of Post-Quantum Cryptography, Industry Readiness, and "Store Now, Decrypt Later" Threats

Alan McDonnell
Supervisor: Dr James Egan

Introduction

Quantum computing poses an imminent threat to traditional cryptographic methods like (RSA, ECC). Adversaries have begun leveraging 'Store Now, Decrypt Later' (SNDL) attacks which are now threatening long-term data security. This research evaluates CRYSTALS-Kyber, a lattice-based PQC algorithm, to address these quantum threats, industry readiness, and PCI-DSS compliance.

Literature Review

QUANTUM THREATS & THE NEED FOR PQC

Quantum computers are going to break RSA, ECC, DH.
PQC is needed to secure data in the long-term today.
"Store Now, Decrypt Later" attacks are already happening.

CRYSTALS-KYBER

Based on the Module-LWE problem.
Strong security and performance.
Selected by NIST for standardisation.

THE SNDL THREAT

Attackers are already collecting encrypted data.
Hybrid cryptography (classical + PQC) recommended.
Urgent need for proactive cryptographic migration.

NIST STANDARDISATION

Kyber chosen over SABER, NTRU, FrodoKEM.
Selection focused on security, efficiency, and real-world deployment.
Official standardisation is guiding future migrations.

INDUSTRY READINESS

Larger key sizes strain current systems.
PCI-DSS standards are falling behind in terms of PQC needs.
Vulnerability tools not ready for PQC detection.

Research Questions

RQ1:
HOW DOES QUANTUM COMPUTING THREATEN TRADITIONAL ENCRYPTION METHODS?

RQ2:
WHAT ARE THE CHARACTERISTICS OF SNDL ATTACKS, AND HOW DO THEY IMPACT CURRENT CRYPTOGRAPHIC SECURITY CONTROLS?

RQ3:
HOW DOES CRYSTALS-KYBER COMPARE AGAINST EXISTING CRYPTOGRAPHIC METHODS IN A PCI-DSS ENVIRONMENT?

RQ4:
WHAT ARE THE KEY CHALLENGES AND STRATEGIES NEEDED FOR THE TRANSITION TO PQC, AS PERCEIVED BY CYBERSECURITY INDUSTRY PROFESSIONALS?

Methodology

Mixed-methods approach:

Quantitative:

- Mathematical analysis of CRYSTALS-Kyber's cryptographic foundations.
- Comparative evaluation of PQC algorithm performance (CRYSTALS-Kyber, NTRU, SABER).
- Experimental evaluation of PCI-DSS implementation challenges for CRYSTALS-Kyber.

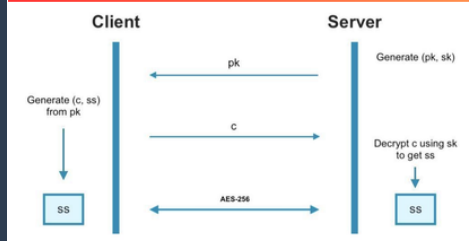
Qualitative:

- Semi-structured interviews with Industry professionals interviews on PQC, adoption readiness, SNDL risks, and compliance concerns.

Why Mixed-Methods?

- Combines technical cryptographic evaluation, practical implementation experimentation, and real-world industry perspectives.
- Provides a complete view from theoretical foundations to operational deployment barriers.

CRYSTALS-Kyber Encryption/Decryption Cycle



Comparative PQC Analysis

ALGORITHM	SECURITY	PERFORMANCE	QUANTUM RESISTANCE
CRYSTALS-KYBER	High	Fast	Strong
NTRU	Medium	Moderate	Strong
SABER	Medium	Fast	Good

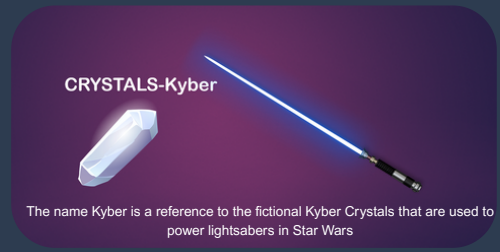
Implementation Challenges

The Integration of CRYSTALS-Kyber in regulated and compliance driven environments comes with additional impacts to Compliance and Operations.

Industry Interviews And Insights

Highlighted that there are many major challenges: practical barriers, limited awareness.

Gap between theoretical research and real-world industry preparedness.

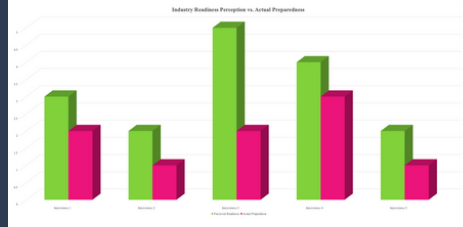


The name Kyber is a reference to the fictional Kyber Crystals that are used to power lightsabers in Star Wars

Results And Findings

CRYSTALS-Kyber demonstrates robust quantum and SNDL resistance.

Identified significant gaps in industry readiness and awareness.



Conclusion

CRYSTALS-Kyber was the strongest candidate for PQC standardisation.

Urgent industry action is needed to bridge existing gaps.

Reference Material

NIST PQC documentation.

The PCI-DSS and Industry Security Frameworks & Guidelines.

CRYSTALS Cryptographic Suite for Algebraic Lattices

The CSA launched a countdown timer for the 14th of April 2030, They predict that this will be the date that quantum computers will be in a position to compromise current cybersecurity systems
This is a point in time capture from the date this poster was created (April 4th 2025) - https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security