Assignment 3.1

Quantum Computing Risks for Energy Sector Encryption

Ali Al Said - ama10643, Zixuan Shan - zs2985, Erica Belcena - eb4286, Anmol Vats - av3938

Quantum Computing Risks for Energy Sector Encryption

1. Introduction

The energy sector increasingly depends on encrypted digital systems to operate critical infrastructure, manage grid stability, and protect sensitive operational data. These systems rely on classical cryptographic algorithms that are vulnerable to emerging quantum computing capabilities. As quantum computers become powerful enough to break widely used encryption schemes, long-standing security assumptions in the energy industry may no longer hold.

This shift introduces significant risks: intercepted data may be decrypted in the future, authenticated control signals could be forged, and compromised communication channels may allow attackers to disrupt physical operations. Given the long lifespan of energy infrastructure and the sector's reliance on secure, real-time data exchange, understanding these vulnerabilities is essential. This report outlines key quantum-related threat scenarios and examines their impacts, root causes, and potential mitigations.

2. Threat Identification

Quantum threats in the energy sector stem from the weakening of classical encryption used to secure device communications, operational data flows, and remote access systems. When these protections fail, attackers may intercept, decrypt, modify, or fabricate information that underpins both grid operations and corporate decision-making.

The following threat cases present realistic scenarios that illustrate how quantum-enabled attacks could compromise ICS commands, reveal sensitive data, undermine remote access, disrupt grid synchronization, or manipulate blockchain-based energy platforms. Each case includes the scenario, impact, root cause, and recommended mitigation.

2.1 Threat Case 1: Manipulation of ICS (Industrial Control System) devices and processes.

Scenario:

Industrial Control Systems (ICS), which includes Supervisory Control and Data Acquisition (SCADA), are responsible for monitoring and controlling the physical equipment and processes used by energy companies. This allows the alteration of operational setpoints, overloading of equipment, or disruption of distribution which leads to safety hazards and potential large-scale outages. For example, if an operator initiates a command to lower the pressure of a compressor, an attacker can intercept this command and change it to increase the pressure, which can cause huge consequences.

Impact:

- Financial loss due to large-scale outages.
- Loss of human life from malfunctioning equipment.
- Damage of the ICS equipment.

Root Cause:

The embedded devices used by these systems are outdated, have little to no security attached, and they share real-time generation, transmission, and distribution data. It is an extremely attractive target for malicious attackers. Quantum computers are capable of breaking the encryption which could allow an attacker to intercept and spoof these commands.

Mitigation:

- Update ICS equipment and data channels to adopt post-quantom cryptography.
- Implement local fail-safe logic and physical safety interlocks

2.2 Threat Case 2: Data Breach/Exposure of Operational Data

Scenario:

If sensitive data, such as strategic plans, of an energy company are compromised while they are being transmitted, this may affect the energy sector stabilization. Quantum attacks break the classical encryption which allows malicious actors to decrypt the data and reveal grid topology, power flows, system vulnerabilities among many others. A breach of this information allows for cyber-physical attacks or gives international agencies strategic intelligence about power grid weaknesses. For example, if an energy company plans to reduce production, and this plan is leaked this will affect the energy sector.

Impact:

- The energy price will be affected negatively.
- Lack of integrity in the competition between energy companies.
- Operational visibility gives attackers a roadmap of what to disrupt.

Root Cause:

Breaking the communication channel.

Mitigation:

- Use communication channels that use post-quantum cryptography.
- Network segmentation and zero-trust access controls.

2.3 Threat Case 3: Harvest Now, Decrypt Later (HNDL) Attacks on Strategic Energy Data

Scenario:

Nation-state adversaries are currently intercepting and storing encrypted communications from energy companies, including grid operational data, infrastructure designs, merger/acquisition negotiations, and cybersecurity incident reports. Once quantum computers become available (estimated 2030-2035), attackers will decrypt this archived data. For example, encrypted emails discussing critical infrastructure vulnerabilities, power plant security assessments, or long-term energy policy strategies sent today will be readable in the future, while these systems and strategies may still be in use for 20-30 years.

Impact:

- Exposure of infrastructure weaknesses that remain exploitable decades later
- Loss of competitive advantage in energy markets and technology development
- National security compromise of critical energy infrastructure details
- Retroactive espionage revealing decision-making processes and strategic priorities

Root Cause:

Long shelf-life of energy sector data (infrastructure operates for 20-50 years) combined with current use of quantum-vulnerable encryption (RSA-2048, ECC) and the reality that adversaries are harvesting encrypted traffic today.

Mitigation:

Immediately deploy hybrid post-quantum/classical encryption for all sensitive communications, prioritize

PQC migration for data with sensitivity exceeding 10 years, and re-encrypt existing archives of high-value strategic data using quantum-resistant algorithms.

2.4 Threat Case 4: Remote Access and VPN Infrastructure Compromise

Scenario:

Energy companies rely heavily on encrypted VPN connections for remote access to SCADA systems, substations, and corporate networks by field engineers, contractors, and remote operations centers. Current VPN protocols use RSA or Diffie-Hellman for key exchange and authentication. If quantum computers break these protocols, attackers could decrypt captured VPN handshakes to steal credentials, session keys, and authentication tokens, enabling unauthorized access to critical operational networks. For instance, a captured VPN session from a field engineer accessing a wind farm control system could be broken to extract access credentials.

Impact:

- Unauthorized remote access to operational technology (OT) networks
- Credential theft enabling persistent access to critical systems
- Bypass of perimeter security and network segmentation
- Potential for remote sabotage of generation and distribution systems

Root Cause:

VPN protocols (IKEv2, OpenVPN, IPSec) rely on RSA and Diffie-Hellman key exchange mechanisms that are vulnerable to Shor's algorithm on quantum computers.

Mitigation:

Transition VPN infrastructure to quantum-resistant key exchange mechanisms (e.g., post-quantum IKE), implement certificate-based authentication with PQC signatures, deploy quantum-safe VPN solutions, and enforce hardware-based multi-factor authentication that doesn't rely solely on cryptographic key exchange.

2.5 Threat Case 5: Grid Desynchronization via Quantum Key Spoofing

Scenario:

Modern electrical grids rely on Phasor Measurement Units (PMUs) and cryptographically protected time synchronization signals to maintain grid-wide frequency and phase alignment. If quantum computers are able to break the digital signatures used to authenticate PMU timestamps and phasor data, attackers could forge synchronization signals. This may cause phase angle divergence, frequency instability, incorrect relay operations, or region-wide grid separation.

Impact:

- Misoperation of transmission line protection systems due to inaccurate phasor data
- Large-scale cascading outages caused by frequency and phase instability
- Grid balancing failures that may result in regional or cross-regional blackouts

Root Cause:

Dependence on traditional cryptographic signatures (ECC/RSA) for PMU time and phasor authentication, which are vulnerable to quantum decryption and signature forgery.

Mitigation:

- Adopt PQC-based (e.g., Dilithium, Falcon) digital signatures for PMU time synchronization and phasor authentication.

- Implement multi-source time synchronization such as GPS + GLONASS + local atomic clocks to avoid single points of failure.
- Deploy physics-based anomaly detection models to automatically flag unphysical phase-angle deviations.

2.6 Threat Case 6: Quantum Attack on Distributed Energy Blockchains

Scenario:

Distributed energy systems—including microgrids, residential solar, energy storage, and charging infrastructure—rely on blockchains for peer-to-peer energy trading, carbon credit accounting, and billing transparency. Most current blockchains use ECDSA signatures based on elliptic curve cryptography. Quantum computers can rapidly derive private keys from public keys, enabling attackers to forge transactions, alter carbon accounting records, or maliciously trigger smart contract executions, undermining market trust.

Impact:

- Forged or manipulated energy transactions leading to financial loss and market instability
- Compromised carbon credit ledgers affecting regulatory and auditing credibility
- Unauthorized smart contract executions that can result in billing errors or denial-of-service conditions

Root Cause:

Blockchains rely on ECDSA and other cryptographic signatures that are vulnerable to quantum attacks, allowing adversaries to forge transactions and manipulate blockchain states.

Mitigation:

- Migrate blockchain networks to PQC-based signature schemes through hard forks or version upgrades.
- Use off-chain Trusted Execution Environments (TEEs) to validate smart contract operations and isolate critical logic.
- Implement multisignature (multisig) schemes combined with quantum-safe key management to increase resistance to key forgery.

3. Focus area

Future research will focus on privacy-preserving communication and long-term security in a quantum-enabled environment, with particular emphasis on how post-quantum cryptography (PQC) can support a secure communication infrastructure for the energy sector. Because energy systems have long operational lifespans, geographically distributed networks, and frequent cross-regional coordination, their data streams and control signals must remain confidential, verifiable, and tamper-resistant even in a future where quantum computers can break current cryptographic schemes.

The study will examine the suitability of PQC for scenarios such as smart grid communication, SCADA control links, VPN-based remote access, and blockchain-supported energy platforms. This includes analyzing the computational cost of PQC signature algorithms (e.g., Dilithium and Falcon), evaluating the impact of PQC-based key exchange on latency and bandwidth, and assessing the feasibility of hybrid encryption approaches during the transition phase. In addition, we will explore how PQC can work alongside physical-layer redundancy, distributed trust models, multi-source time synchronization, and privacy-enhancing techniques such as differential privacy and trusted execution environments. The objective is to build an end-to-end privacy protection framework that remains effective across the entire lifecycle of critical infrastructure.

4. Additional resources

Giani, A., & Eldredge, Z. (2021). Quantum computing opportunities in renewable energy. SN Computer Science, 2(5), 393. https://link.springer.com/article/10.1007/s42979-021-00786-3
https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html
https://apricorn.com/data-encryption-in-energy/
CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography:
https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
CISA: Post-Quantum Considerations for Operational Technology(2.5、2.6)
https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf
Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure (Baseri et al., 2024)(2.5、2.6)
https://arxiv.org/abs/2404.10659
Migration to post-quantum cryptography – Mastercard White Paper(2.5、2.6)
https://www.mastercard.com/content/dam/mccom/shared/news-and-trends/stories/2025/quantum-explainer-and-white-paper/Migration-to-post-quantum-cryptography-WhitePaper_2025.pdf Mastercard
White paper series: Understanding the quantum threat, post-quantum cryptography and the upcoming NIST standards (PQShield)(2.5、2.6)
https://pqshield.com/white-paper-series-understanding-the-quantum-threat-post-quantum-cryptography-and-the-upcoming-nist-standards/
Cloudflare: Simple PQC Explanation
https://blog.cloudflare.com/post-quantum-for-all/
ENISA Report on PQC for Energy Sector
https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
Google's PQC Migration Experience
https://security.googleblog.com/2022/07/protecting-chrome-traffic-with-hybrid.html
HNDL Attacks:
https://medium.com/spherity/q-day-countdown-the-hdnl-cybersecurity-crisis-europe-cant-ignore-0694ce4a5802
Microsoft: Quantum Threat Timeline(2.3):
https://www.microsoft.com/en-us/security/blog/2023/06/01/quantum-computing-harvest-now-decrypt-later/
RAND Corporation Analysis(2.3):
https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html
NIST on Quantum-Safe VPNs(2.4):
https://www.nccoe.nist.gov/crypto-agility-considerations-migrate-post-quantum-cryptographic-algorithms
Energy Sector VPN Security Guide(2.4):
https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
Quantum-Safe VPN Deployment Guide(2.4):
https://www.etsi.org/technologies/quantum-safe-cryptography