

Exercises: Lesson 8.2 – Quantum Computing and Post-Quantum Cryptography
Module 8: The Future Problem

Prof. Dr. Joerg Osterrieder

Exercise 1: Harvest Now, Decrypt Later — Risk Assessment

Scenario: You are the Chief Information Security Officer (CISO) of a European bank. Your bank processes 5 million transactions per day, stores customer data encrypted with RSA-2048, and communicates with SWIFT using RSA-signed messages. You need to present a quantum risk assessment to the board.

Given data:

- Customer mortgage data: must remain confidential for 25 years
- Corporate loan records: must remain confidential for 15 years
- Daily transaction logs: must remain confidential for 7 years
- Estimated earliest quantum computer capable of breaking RSA-2048: 2033 (optimistic), 2040 (conservative)

Tasks:

- 1 For each data category, calculate whether the HNDL window has already opened (i.e., whether years-until-quantum < years-data-must-stay-secret). Use both the optimistic and conservative estimates.
- 2 Rank the three data categories by urgency of migration. Which should be re-encrypted first?
- 3 The board asks: “What is the cost of doing nothing?” Draft a 3-sentence response that quantifies the risk in terms the board can understand.
- 4 Propose a 12-month action plan for Phase 1 (cryptographic inventory) with specific deliverables.

Exercise 2: Cryptographic Inventory for a Mid-Size Bank

Scenario: A mid-size bank with 2,000 employees has the following systems:

System	Crypto Used	Purpose
Online banking portal	TLS 1.3 (RSA/ECDSA)	Customer access
Mobile banking app	Certificate pinning (RSA)	Customer access
SWIFT gateway	RSA-2048 signatures	Interbank messaging
Internal email	S/MIME (RSA-2048)	Staff communication
HSM cluster	RSA-4096 key storage	Key management
Core banking system	AES-256 encryption	Data at rest
Database backups	RSA-2048 encrypted	Archive storage

Tasks:

- Classify each system as “quantum-vulnerable” (uses RSA/ECDSA), “quantum-weakened” (uses AES/SHA), or “quantum-safe” (already PQC).
- Rank the systems by migration priority considering: (i) data sensitivity, (ii) public exposure, (iii) difficulty of migration.
- The HSM vendor says PQC firmware will be available in 2026. How does this affect your migration timeline?
- Design a hybrid deployment strategy for the online banking portal using hybrid certificates.

Exercise 3: Quantum-Proofing a Blockchain

Scenario: You are advising a blockchain consortium that operates a permissioned blockchain for trade finance. The blockchain uses ECDSA (secp256k1) for transaction signatures and SHA-256 for block hashing. The consortium has 50 member banks and processes 100,000 transactions per day.

Tasks:

- 1 Explain which component (ECDSA signatures or SHA-256 hashing) is threatened by quantum computers and why.
- 2 The blockchain has 3 years of historical transactions with exposed public keys. What is the quantum risk to these historical transactions? Can they be retroactively protected?
- 3 Design a migration plan: How should the consortium transition from ECDSA to a PQC signature scheme (e.g., CRYSTALS-Dilithium)? Consider: backward compatibility, hard fork vs. soft fork, and the transition period.
- 4 A member bank asks: “Can we just increase the ECDSA key size to 512 bits instead of migrating to PQC?” Explain why this does not solve the problem.
- 5 Estimate the impact on block size if signatures change from ECDSA (~64 bytes) to CRYSTALS-Dilithium (~2,420 bytes). What are the implications for throughput?

Exercise 4: Selecting a PQC Algorithm for a Payment System

Scenario: A national payment system processes 200 million transactions per day. The system currently uses ECDSA for transaction authentication and RSA-2048 for TLS. The central bank has mandated migration to PQC by 2030.

Performance requirements:

- Transaction authentication latency: $<5\text{ms}$
- Maximum signature size increase tolerable: 10x current ECDSA (640 bytes max)
- Key storage budget: 2 KB per participant maximum
- Must support hybrid mode during transition

Tasks:

- Compare CRYSTALS-Dilithium (signature: ~ 2.4 KB, public key: ~ 1.3 KB) with SPHINCS+ (signature: ~ 17 – 49 KB, public key: 32–64 bytes). Which meets the performance requirements?
- The system's current ECDSA signature is 64 bytes. Calculate the bandwidth increase if all 200 million daily transactions use Dilithium instead.
- Design a hybrid authentication scheme where both ECDSA and Dilithium signatures are included during the transition period. What is the total signature size?
- Recommend which PQC algorithm the payment system should adopt. Justify your choice considering latency, bandwidth, and storage constraints.

Exercise 5: Communicating Quantum Risk to Non-Technical Stakeholders

Scenario: You must present the quantum computing threat to your bank's board of directors. Board members include: a CEO with an MBA, a CFO who focuses on cost, a Chief Risk Officer who manages regulatory risk, and two non-executive directors with no technical background.

Tasks:

- 1 Write a 5-sentence executive summary of the quantum threat to the bank. Use zero technical jargon (no “qubits,” “Shor’s algorithm,” or “ECDSA”). Use only analogies and business language.
- 2 The CFO asks: “How much will migration cost?” Provide a rough order-of-magnitude estimate for a bank with 500 systems using RSA/ECDSA. Consider: (i) cryptographic inventory (€200K–500K), (ii) hybrid deployment (€1M–3M), (iii) full migration (€5M–15M), (iv) staff training and vendor coordination.
- 3 The CEO asks: “What happens if we do nothing for 3 years?” Draft a risk statement that quantifies the exposure in terms the CEO can understand.
- 4 The CRO asks: “Are regulators requiring this?” Summarize the regulatory landscape in 4 bullet points (NIST, NSA CNSA 2.0, EU/BSI, BIS).

Exercise 6: Quantum Computing for Portfolio Optimization

Scenario: An asset management firm manages €10 billion across 500 individual securities. The current portfolio optimization runs overnight (8 hours) on a classical supercomputer, testing 10,000 portfolio combinations.

Given:

- Classical optimization: 8 hours for 10,000 combinations
- Quantum annealing (D-Wave): estimated 15 minutes for 10,000 combinations (current hybrid quantum-classical)
- Full quantum advantage: estimated 1 minute for 1,000,000 combinations (5–10 years away)
- D-Wave cloud access cost: €500K/year
- Current supercomputer cost: €200K/year

Tasks:

- Calculate the speedup factor for the current hybrid quantum approach vs. classical.
- If the firm can test 100x more combinations, estimate the potential improvement in portfolio returns (assume each additional 10x in combinations tested yields a 0.15% improvement in annual return on a €10B portfolio).
- Calculate the net benefit: additional return minus additional cost. Is the quantum approach currently cost-effective?
- What non-financial risks should the firm consider before adopting quantum computing for portfolio optimization?

Exercise 7: SWIFT Post-Quantum Migration

Scenario: SWIFT connects 11,000+ financial institutions across 200 countries. All SWIFT messages are authenticated using RSA-2048 digital signatures. SWIFT has announced it is testing PQC integration.

Tasks:

- a Explain why SWIFT message authentication is a critical target for quantum attacks. What could an attacker do with a forged SWIFT message?
- b SWIFT must maintain backward compatibility during migration (not all 11,000 members will migrate simultaneously). Design a three-phase migration strategy that uses hybrid signatures.
- c Calculate the message size increase if SWIFT adds a Dilithium signature (~ 2.4 KB) alongside the existing RSA-2048 signature (~ 256 bytes) during hybrid mode. If SWIFT processes 45 million messages per day, what is the additional daily bandwidth?
- d A bank in a developing country says it cannot afford to upgrade its HSMs for PQC. How should SWIFT handle this? Propose a solution that maintains security without excluding smaller institutions.

Exercise 8: Full Quantum Readiness Assessment

Scenario: It is 2030. A large-scale quantum computer has just been demonstrated to factor a 1024-bit RSA key in 24 hours. While RSA-2048 is not yet broken, experts estimate it will be breakable within 3–5 years. You are the CISO of a global bank.

Tasks:

- a. **Immediate actions (24–72 hours):** List 5 actions you would take in the first 72 hours after this announcement.
- b. **Data triage:** Categorize your bank's data into (i) already compromised (HNDL exposure), (ii) at imminent risk, and (iii) safe for now. What criteria do you use?
- c. **Stakeholder communication:** Draft a 3-paragraph internal memo to all staff explaining the situation and immediate steps.
- d. **Regulatory response:** You receive a letter from the ECB requiring a PQC migration plan within 90 days. Outline the plan structure.
- e. **Competitive advantage:** Your competitor has not started PQC migration. How can your early preparation be turned into a competitive advantage for winning corporate clients who care about data security?