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:

a. Classify each system as "quantum-vulnerable" (uses RSA/ECDSA), "quantum-weakened" (uses AES/SHA), or "quantum-safe" (already PQC).

b. Rank the systems by migration priority considering: (i) data sensitivity, (ii) public exposure, (iii) difficulty of migration.

c. The HSM vendor says PQC firmware will be available in 2026. How does this affect your migration timeline?

d. 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 ($\sim$64 bytes) to CRYSTALS-Dilithium ($\sim$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: $<$5ms
- 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:

a. Compare CRYSTALS-Dilithium (signature: $\sim$2.4 KB, public key: $\sim$1.3 KB) with SPHINCS+ (signature: $\sim$17–49 KB, public key: 32–64 bytes). Which meets the performance requirements?

b. The system's current ECDSA signature is 64 bytes. Calculate the bandwidth increase if all 200 million daily transactions use Dilithium instead.

c. Design a hybrid authentication scheme where both ECDSA and Dilithium signatures are included during the transition period. What is the total signature size?

d. 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:

a) Calculate the speedup factor for the current hybrid quantum approach vs. classical.

b) 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).

c) Calculate the net benefit: additional return minus additional cost. Is the quantum approach currently cost-effective?

d) 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 ($\sim$2.4 KB) alongside the existing RSA-2048 signature ($\sim$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?

Answer Key – Exercise 1

(1) HNDL window analysis:

Data Type	Secret Until	Optimistic (2033)	Conservative (2040)
Mortgage (25 yr)	2050	Window OPEN ($25 > 8$)	Window OPEN ($25 > 15$)
Corporate loans (15 yr)	2040	Window OPEN ($15 > 8$)	Borderline ($15 = 15$)
Transaction logs (7 yr)	2032	Borderline ($7 \approx 8$)	SAFE ($7 < 15$)

(2) Priority: (1) Mortgage data — longest shelf life, highest exposure. (2) Corporate loans — significant shelf life. (3) Transaction logs — short shelf life, lowest urgency.

(3) Board response: "If a state-level adversary is recording our encrypted data today, and a quantum computer arrives by 2035, every mortgage record we transmit from now until migration is compromised. This affects [X] million customer records with a potential regulatory fine of up to 4% of annual revenue under GDPR. The cost of migration is €5–15M; the cost of a data breach affecting decades of mortgage records is orders of magnitude higher."

(4) 12-month plan: Q1: Engage vendor to scan all systems for RSA/ECDSA. Q2: Classify all data by confidentiality shelf life. Q3: Map certificate chains and HSM dependencies. Q4: Produce a ranked migration roadmap with cost estimates.

Answer Key – Exercise 2

(a) Classification:

System	Status
Online banking portal (RSA/ECDSA)	Quantum-vulnerable
Mobile banking app (RSA cert pinning)	Quantum-vulnerable
SWIFT gateway (RSA-2048)	Quantum-vulnerable
Internal email (RSA-2048 S/MIME)	Quantum-vulnerable
HSM cluster (RSA-4096)	Quantum-vulnerable
Core banking (AES-256)	Quantum-weakened (but adequate)
Database backups (RSA-2048 encrypted)	Quantum-vulnerable

(b) Priority ranking: (1) Database backups — stored data, HNDL exposure. (2) SWIFT gateway — high-value interbank. (3) Online banking — public-facing. (4) HSM cluster — key infrastructure. (5) Mobile app — requires app store update. (6) Email — lower sensitivity. (7) Core banking AES-256 — adequate as-is.

(c) HSM is the bottleneck. If PQC firmware arrives in 2026, full migration of key management cannot start before then. Plan: use software-based PQC for other systems in 2025; migrate HSM in 2026–2027.

(d) Hybrid: Issue certificates with both RSA-2048 and ML-KEM key pairs. TLS 1.3 clients that support PQC negotiate the PQC cipher suite; legacy clients fall back to RSA. Both keys must validate for the connection to succeed.

Answer Key – Exercise 3

(1) ECDSA is threatened (Shor's algorithm solves the discrete logarithm problem). SHA-256 is weakened but not broken (Grover provides a sqrt speedup, but SHA-256 remains computationally hard).
(2) Historical transactions with exposed public keys are permanently at risk. They cannot be retroactively re-signed because the blockchain is immutable. The only mitigation is for users to move funds to new PQC-secured addresses before quantum arrives.
(3) Migration plan: Phase 1 (6 months): Deploy Dilithium alongside ECDSA in a soft fork — new transactions carry both signatures; old nodes validate only ECDSA. Phase 2 (12 months): All members upgrade to validate Dilithium. Phase 3 (6 months): Hard fork to require Dilithium-only signatures; ECDSA deprecated.
(4) Increasing ECDSA key size does not help because Shor's algorithm scales polynomially — doubling the key size does not meaningfully increase the time a quantum computer needs. The fundamental mathematical problem (discrete logarithm) remains solvable regardless of key size.
(5) Signature size increases by $\sim$38x (64 bytes $\rightarrow$ 2,420 bytes). For 100K transactions/day: additional storage per day = 100,000 $\times$ 2,356 bytes $\approx$ 236 MB/day. Throughput impact: blocks become larger; either increase block size limit or accept fewer transactions per block.

Answer Key – Exercises 4–6

Exercise 4:
(a) Dilithium: signature 2.4 KB (<640 bytes limit? No, 2.4 KB = 2,420 bytes > 640 bytes). SPHINCS+: 17–49 KB (far exceeds limit). **Neither meets the 640-byte constraint.** The system must either relax the constraint or use Dilithium at the smallest parameter set (∼1.3 KB for Dilithium2, which is closer but still >640 bytes).
(b) Bandwidth: 200M × (2,420 − 64) bytes = 200M × 2,356 bytes ≈ **471 GB/day** additional bandwidth.
(c) Hybrid signature size: ECDSA (64 bytes) + Dilithium (2,420 bytes) = **2,484 bytes total**.
(d) Recommendation: Dilithium (ML-DSA). Despite exceeding the original size constraint, it is the only viable option given SPHINCS+ is 10–20x larger.

Exercise 6:
(a) Speedup: 8 hours / 15 minutes = **32x**.
(b) 100x more combinations = 10x × 10x, yielding 0.15% + 0.15% = 0.30% improvement. On €10B: €30M/year additional return.
(c) Net benefit: €30M − (€500K − €200K) = €30M − €300K = **€29.7M/year**. Highly cost-effective *if* the return estimate holds. Caveat: the 0.15% per 10x is a simplifying assumption.
(d) Risks: Quantum hardware reliability, vendor lock-in, model risk from over-optimization, regulatory scrutiny of opaque optimization methods.

Answer Key – Exercises 7–8

Exercise 7:
(a) A forged SWIFT message could authorize fraudulent interbank transfers (as in the 2016 Bangladesh Bank heist, which used credential theft rather than crypto-breaking). With quantum-forged signatures, an attacker could create authentication tokens that are indistinguishable from legitimate messages.
(b) Phase 1: SWIFT adds Dilithium signature as optional alongside RSA. Phase 2: Dilithium becomes mandatory; RSA retained for legacy verification. Phase 3: RSA deprecated.
(c) Additional per message: 2,420 bytes. Daily: 45M $\times$ 2,420 bytes $\approx$ **109 GB/day** additional bandwidth. Significant but manageable with modern infrastructure.
(d) SWIFT could: (i) provide cloud-hosted PQC signing as a service (smaller banks sign via SWIFT's HSM), (ii) subsidize HSM upgrades for developing-country members, (iii) extend the hybrid period to give more migration time.

Exercise 8 (key points):
(a) 72-hour actions: (1) Activate PQC migration team. (2) Re-encrypt highest-priority data (HNDL backlog). (3) Enable hybrid TLS on public-facing systems. (4) Brief the board and regulators. (5) Contact HSM/vendor vendors to accelerate firmware delivery.
(b) Criteria: (i) Already compromised = data transmitted in the past over RSA-protected channels that was intercepted. (ii) Imminent risk = data with long shelf life still protected by RSA. (iii) Safe = data encrypted with AES-256 or already migrated to PQC.
(e) Competitive advantage: Market the bank as "quantum-ready," offer PQC-protected data storage as a premium service for corporate clients, and use early compliance as a differentiator in RFP responses.