Quiz: Lesson 8.2 – Quantum Computing and Post-Quantum Cryptography

Module 8: The Future Problem

Prof. Dr. Joerg Osterrieder

Question 1 (Remember)

What is the key difference between a classical bit and a qubit?

A. A qubit is faster than a classical bit but stores the same information

B. **A classical bit is always 0 or 1; a qubit can exist in a superposition of both 0 and 1 simultaneously until measured**

C. A qubit is a compressed classical bit that uses less energy

D. A qubit can store more data because it uses optical rather than electronic signals

Question 2 (Remember)

What does the term “entanglement” mean in quantum computing?

A. **Two qubits whose states are correlated — measuring one instantly determines the state of the other, regardless of distance**

B. The process of converting classical data into quantum data

C. A technique for compressing quantum data into fewer qubits

D. Two qubits that are physically connected by a wire

Question 3 (Understand)

Shor's algorithm, when run on a sufficiently powerful quantum computer, breaks which of the following?

A. All known cryptographic algorithms
B. SHA-256 hash functions
C. AES-256 symmetric encryption
D. **RSA and ECDSA (public-key cryptography based on factoring and discrete logarithms)**

Question 4 (Understand)

Why is AES-256 considered "weakened" but not "broken" by quantum computers?

A. **Grover's algorithm halves the effective key length (256-bit → 128-bit security), but 128-bit security remains computationally infeasible to brute-force**

B. Because AES-256 was designed specifically to resist quantum attacks

C. Because no quantum algorithm has been discovered that applies to symmetric encryption

D. Because AES-256 uses a different type of qubit that resists quantum attacks

Question 5 (Understand)

What is the "harvest now, decrypt later" (HNDL) threat?

A. A vulnerability in current quantum computers that allows them to be used for password cracking

B. A phishing attack that harvests passwords and uses them to decrypt files immediately

C. **Adversaries collect encrypted data today and store it to decrypt in the future when quantum computers become available**

D. A ransomware technique that encrypts data and demands future payment

Question 6 (Apply)

A bank stores customer mortgage records encrypted with RSA-2048. The records must remain confidential for 30 years. Optimistic estimates suggest a cryptographically relevant quantum computer could arrive by 2035. Is this bank's data at risk?

A. **Yes, because the data must stay secret until 2055, and a quantum computer arriving as early as 2035 could decrypt RSA-2048 — meaning the HNDL window has already opened**

B. No, because quantum computers will not target financial data

C. Yes, but only if the quantum computer has more than 1 million qubits

D. No, because RSA-2048 is considered secure until at least 2040

Question 7 (Remember)

What does “post-quantum cryptography” (PQC) mean?

A. **Cryptographic algorithms that run on classical computers but are designed to resist attacks from both classical and quantum computers**

B. Cryptographic algorithms designed to replace SHA-256

C. Cryptographic algorithms that require quantum computers to run

D. A theoretical framework for encryption that has not yet been implemented

Question 8 (Remember)

Which three families of post-quantum cryptography has NIST selected for standardization?

A. Blockchain-based, AI-based, and quantum-based

B. RSA-extended, ECDSA-extended, and AES-extended

C. **Lattice-based (CRYSTALS-Kyber/Dilithium), hash-based (SPHINCS+), and code-based (Classic McEliece, still in evaluation)**

D. Symmetric-only, asymmetric-only, and hybrid

Question 9 (Understand)

Why did NIST select multiple PQC algorithm families rather than standardizing on a single algorithm?

A. It was a political compromise between competing research groups

B. Each family is optimized for a different hardware platform

C. **Diversification: if one mathematical problem turns out to be easier to solve than expected, the other families provide a fallback — this is cryptographic risk management**

D. Each family is designed for a different programming language

Question 10 (Understand)

What is “crypto agility” and why is it important?

A. The ability to use multiple encryption algorithms on the same data for extra security

B. **The ability of a system to switch between cryptographic algorithms without redesigning the entire system — essential because algorithms may need to be replaced as threats evolve**

C. A measure of how many encryption keys a system can store simultaneously

D. The speed at which a cryptographic algorithm can encrypt data

Question 11 (Apply)

A bank wants to begin PQC migration without disrupting existing systems. What is the recommended first step?

A. Immediately replace all RSA certificates with PQC certificates

B. **Conduct a cryptographic inventory: catalog all systems, protocols, and certificates using RSA, ECDSA, or Diffie-Hellman, and identify data with long confidentiality requirements**

C. Switch all systems to AES-256, which is quantum-resistant

D. Wait for quantum computers to arrive before taking action

Question 12 (Apply)

What is a "hybrid certificate" in the context of PQC migration?

A. A certificate issued jointly by two different certificate authorities

B. A certificate that combines encryption and digital signature functionality

C. **A single digital certificate containing both a classical (RSA/ECDSA) key pair and a PQC key pair, allowing systems to use PQC if supported and fall back to classical otherwise**

D. A certificate that works on both mobile and desktop devices

Question 13 (Understand)

Why is blockchain especially vulnerable to quantum computing compared to traditional banking systems?

A. Because blockchain transactions are processed more slowly, giving quantum computers more time

B. Because blockchain uses weaker encryption algorithms than banks

C. Because blockchain does not use any form of encryption

D. **Because blockchain is immutable — historical transactions with exposed ECDSA public keys cannot be retroactively re-signed with PQC algorithms, and "lost wallet" funds become stealable**

Question 14 (Understand)

Bitcoin mining uses SHA-256, and Bitcoin transactions use ECDSA. Which component is threatened by quantum computers?

A. **Transactions (ECDSA), because Shor's algorithm breaks elliptic curve signatures. SHA-256 mining is weakened (Grover) but not broken**
B. Mining (SHA-256), because quantum computers can compute hashes instantly
C. Neither — Bitcoin was designed to be quantum-resistant
D. Both mining and transactions are equally threatened

Question 15 (Apply)

The NSA's CNSA 2.0 mandate requires U.S. national security systems to migrate to PQC by 2030–2035. What does this signal to the financial industry?

A. That PQC algorithms are only suitable for government use

B. **That post-quantum migration is becoming a compliance requirement for critical infrastructure, and financial regulators are likely to follow with similar mandates**

C. That financial institutions should wait for a separate financial mandate

D. Nothing — military requirements do not apply to finance

Question 16 (Apply)

Which quantum computing application in finance has the most immediate practical urgency?

A. Quantum machine learning for credit scoring

B. Quantum optimization of trading algorithms

C. Quantum simulation of financial markets

D. **Migration to post-quantum cryptography to protect financial data and transactions from future quantum attacks**

Question 17 (Understand)

A quantum computer with enough qubits could forge ECDSA signatures on a blockchain. What would this allow an attacker to do?

A. Shut down the entire blockchain network

B. Reverse confirmed transactions on the blockchain

C. Mine blocks faster than any other miner

D. **Spend cryptocurrency from any wallet whose public key has been exposed on-chain, by forging the owner's signature**

Question 18 (Evaluate)

Some organizations argue that PQC migration can wait until a "cryptographically relevant" quantum computer is demonstrated. What is the strongest counterargument?

A. PQC algorithms might be deprecated before quantum computers arrive

B. There is no valid counterargument; waiting is the rational strategy

C. Early migration is always cheaper in absolute terms

D. **The "harvest now, decrypt later" attack means data is already being collected for future decryption — and cryptographic infrastructure takes years to migrate, so starting later guarantees a period of vulnerability**

Question 19 (Evaluate)

A CTO argues: "Quantum computers are overhyped. We should focus our budget on AI security threats instead." How would you respond?

A. AI and quantum threats are identical and should be addressed with the same tools

B. **Both AI and quantum threats are real, but quantum migration requires longer lead times (years of infrastructure changes) and cannot be done reactively — the cryptographic inventory should begin now even if other threats receive more operational budget**

C. The CTO is correct; AI threats are more immediate and quantum threats are speculative

D. Quantum threats are more dangerous than AI threats and should receive the entire security budget

Question 20 (Evaluate)

If an estimated 3–4 million BTC sit in "lost wallets" (owners lost their private keys), what happens when a quantum computer capable of breaking ECDSA becomes available?

A. The Bitcoin network would fork to prevent quantum access

B. Nothing — lost wallets cannot be accessed by anyone, including quantum computers

C. **Anyone with a quantum computer could derive the private keys from the exposed public keys and steal the funds — creating a massive, sudden redistribution of wealth on the Bitcoin network**

D. The Bitcoin protocol will automatically protect these wallets