SECON 2025
NEW JERSEY

ISC2 CHAPTER

Quantum Computing and AppSec: Preparing for the Post-Quantum Threat

Sheshananda Reddy Kandula

10 June 2025

Agenda

- Introduction
- Quantum Computing Basics
- Quantum Computing Threats
- Traditional Encryption Overview
- Cryptography in Application Security
- Attack Scenarios
- Mitigation Strategies
- Future Directions
- Q&A

Whoami

@Sheshananda Reddy Kandula

15 years in Application Security/Cyber Security

Quantum Mechanics vs Quantum Computing

A fundamental branch of physics that explains how particles (like electrons and photons) behave at the smallest scales

Core Concepts:

- **Superposition:** Particles exist in multiple states simultaneously.
- **Entanglement:** Two particles can be linked, affecting each other instantly, even across distances.
- **Uncertainty Principle:** You can't precisely know both a particle's position and momentum at the same time.

Applications:

- Chemistry and particle physics
- Lasers, transistors, and MRI machines
- Explains atomic behavior

Quantum Computing:
A type of computation that uses **quantum mechanics** principles to perform operations on data using **qubits**.

Core Concepts:

- **Qubits:** Like bits, but can be 0, 1, or both (superposition).
- **Quantum Gates:** Manipulate qubit states using quantum operations.
- **Interference:** Helps amplify correct answers and cancel wrong ones.
- **Entanglement:** Used to link and coordinate multiple qubits.

Classical Bits Vs Quantum Bits

Classical Bits

- Represent either 0 or 1
- Can only be in one state at a time
- Foundation of all modern computing

Classical Computers

Foundation: Operate on "bits" (0 or 1).

Processing: Information processed sequentially.

sequentially.

Limitations: Struggle with some complex issues

issues (e.g., simulating molecules, breaking

advanced encryption).

Quantum Bits (Qubits)

- Can represent 0, 1, or both simultaneously
- Exist in multiple states through superposition
- Enable exponential computational power

Quantum Computers

Foundation: Leverage quantum mechanics

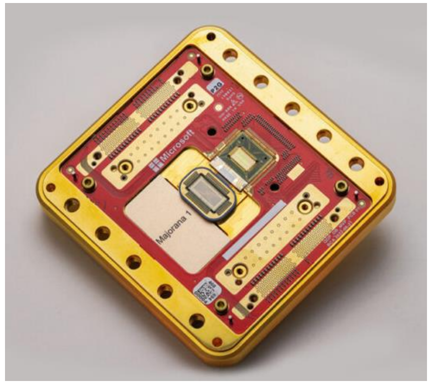
Promise: Solve problems intractable for

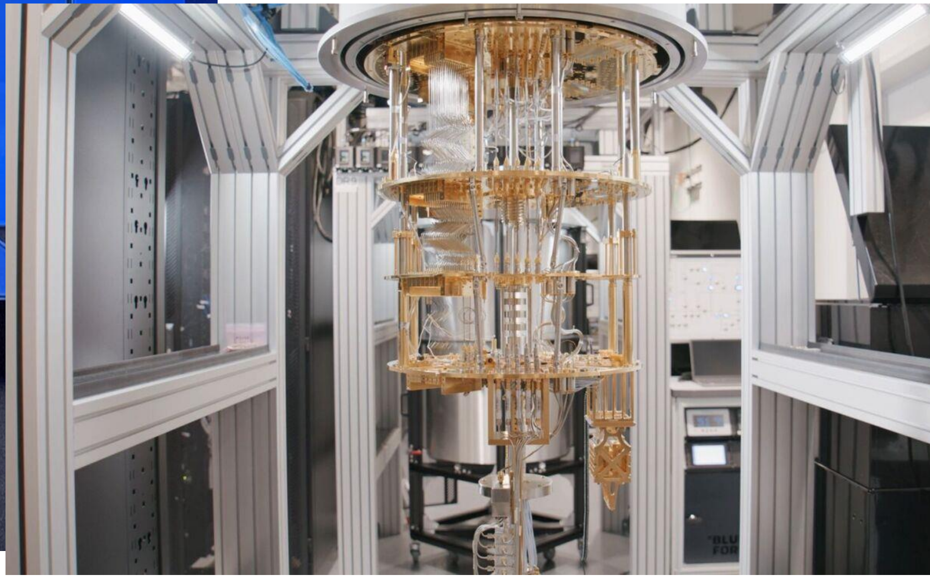
supercomputers.

Relationship: A specialized, powerful tool, not

replacement for classical computers.

Quantum Computers in Real World





Quantum Superposition

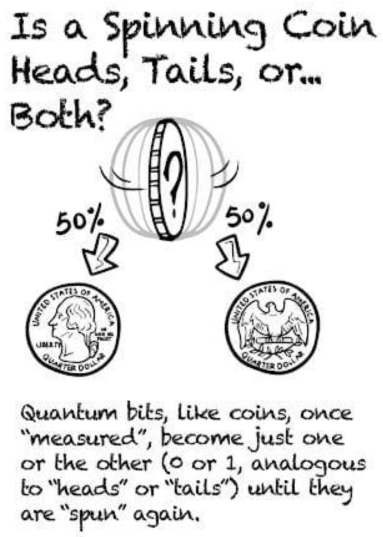
Multiple States

Qubits exist in all possible states simultaneously

Probabilistic Nature

States exist with certain probabilities until measured

A qubit is a combination of 0 and 1 with certain probabilities, until n



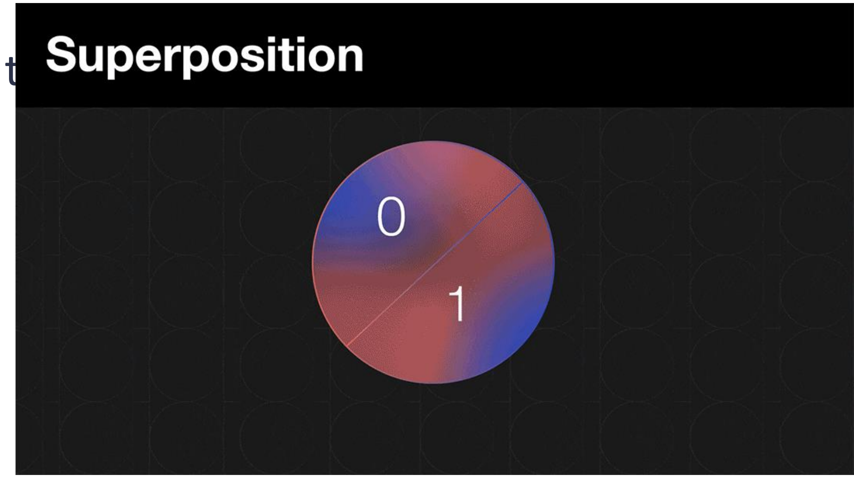
Measurement Impact

Observing a qubit collapses its state to either 0 or 1

A coin spinning in the air is in a superposition of "heads" and "t

Why it Matters:

Allows quantum computers to perform computations on many possibilities concurrently.



Computational Power

Enables parallel computation of multiple possibilities

Quantum Entanglement

Connection

Qubits become linked linked regardless of distance

Correlation

Changes to one qubit qubit instantly affect its its partner

Speed

Information appears transfer instantly

Applications

Enables secure communications and quantum teleportation teleportation

Quantum Computing Timeline

1980s

Theoretical foundations established by Feynman and Deutsch

1990s

Shor's algorithm proves quantum computers can factor large numbers

2010s

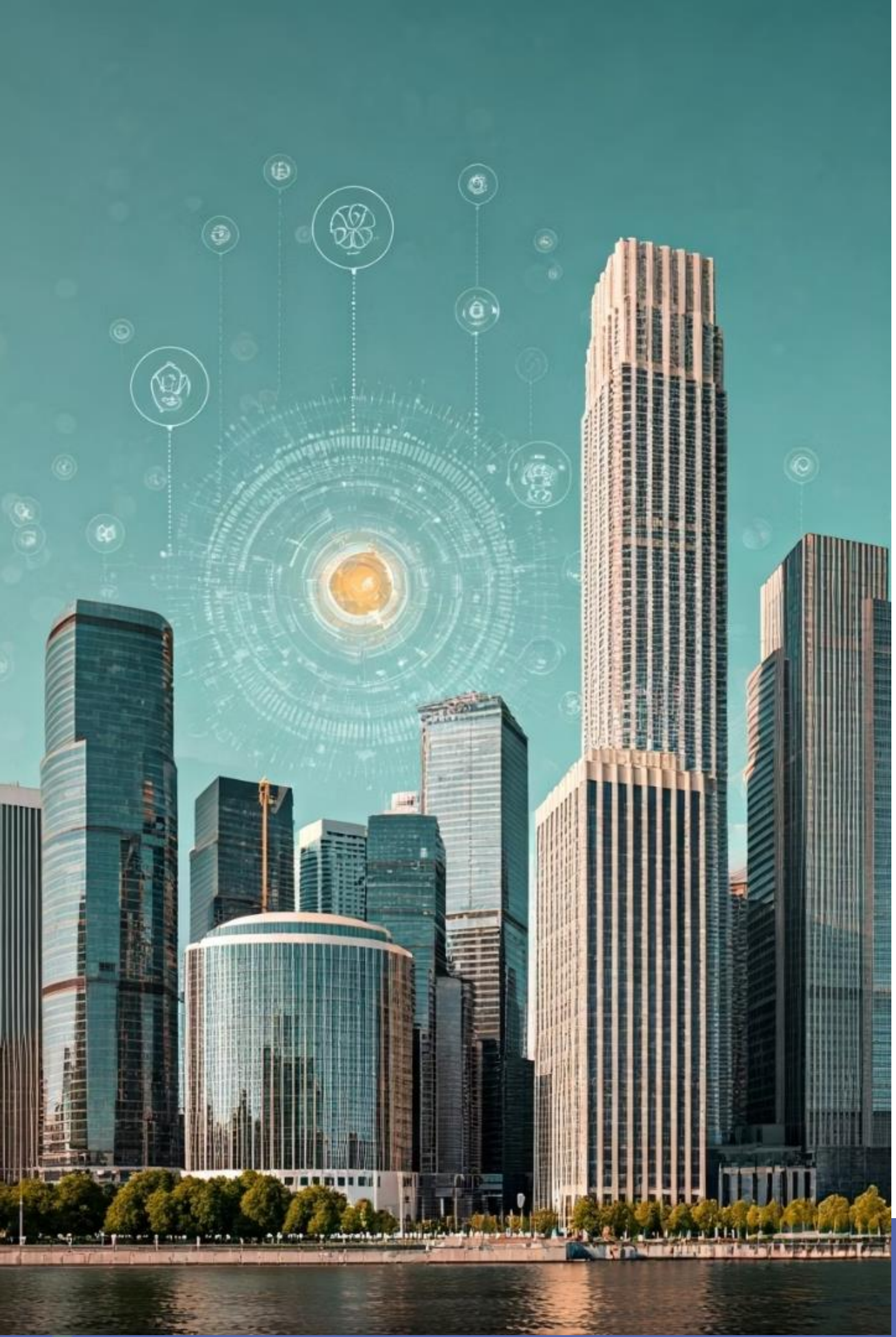
First quantum computers with 50+ qubits developed

2020s

Quantum advantage demonstrated for specific problems

Future

Commercial applications expected as technology matures



Quantum Computing Applications

Cryptography

- Breaking current encryption
- Creating unbreakable codes
- Secure communications

Scientific Research

- Molecular modeling
- Materials science
- Climate simulation

Optimization

- Supply chain logistics
- Financial modeling
- Traffic flow optimization

Quantum Computing Challenges

Quantum Supremacy

Demonstrating quantum advantage over classical computers

Error Correction

Maintaining quantum states against decoherence

Temperature

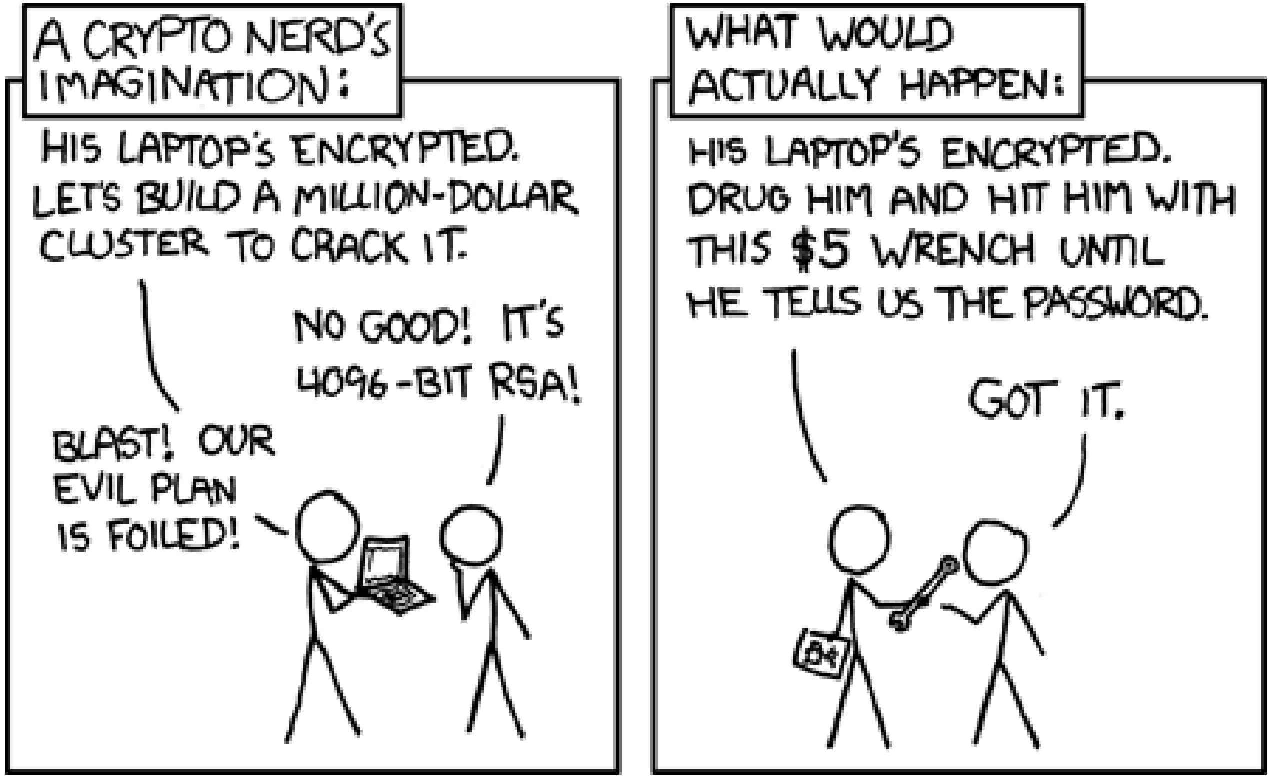
Operating at near absolute zero temperatures

Programming

Developing quantum algorithms and software

How Quantum Computing Breaks Encryption?

NOT Like THIS



https://xkcd.com/538/

How Quantum Computers Solve Problems (High Level)

Not brute force, but clever manipulation of probabilities:

1. **Initialization:** Qubits start in a known state (e.g., $|0\rangle$).
2. **Encoding the Problem:** The Problem is translated into quantum states, often using superposition and entanglement to represent all possible solutions.
3. **Applying Quantum Gates (Computation):**
   - A sequence of quantum gates (the algorithm) manipulates the probability amplitudes.
   - Interference amplifies correct solutions and cancels incorrect ones.
4. **Measurement:**
   - Qubits are measured, collapsing the superposition to a classical 0 or 1.
   - The measured outcome is overwhelmingly likely to be the desired solution.
   - Algorithms often run multiple times for confirmation due to their probabilistic nature.

Key Quantum Algorithms (Examples of Potential)

Demonstrating quantum superiority:

- **Shor's Algorithm (1994):**
  - **Purpose:** Efficiently factorizes large numbers.
  - **Impact:** Threatens current RSA encryption; requires quantum-safe cryptography.
  - Breaks TLS encryption, digital signatures, SSH, VPNs, and even cryptocurrencies.

Problem	Classical Time	Quantum (Shor's) Time
Factor 2048-bit RSA	>10^20 years	Hours or minutes
ECC Discrete Logarithm	Infeasible	Feasible

- **Grover's Algorithm (1996):**
  - **Purpose:** Speeds up unstructured database search.
  - **Speedup:** Quadratic speedup (N vs. N).
  - **Impact:** Optimizing search and data analysis.

Key Quantum Algorithms (Examples of Potential)

Demonstrating quantum superiority:

- **Quantum Simulation:**
  - **Purpose:** Simulating complex quantum systems (molecules, materials).
  - **Impact:** Revolutionary for drug discovery, materials science, and chemistry.
- **Quantum Machine Learning:**
  - **Purpose:** Enhancing AI tasks like pattern recognition and optimization.
  - **Impact:** Could lead to more powerful AI models.

The Quantum Threat Timeline

Present Day

50-100 qubit systems with limited capabilities

3-5 Years

Error-corrected quantum computers emerge

5-10 Years

Cryptographically relevant quantum computers possible

10+ Years

Widespread computing

Organizations should start planning their quantum migration strategy now. The "harvest now, decrypt already active.

Cryptography in Application Security

Cryptography forms a critical security layer for web and mobile mobile applications. It protects data at rest, in transit, and in use. in use.

The global cryptography market is projected to reach $8.4 2025. This growth reflects increasing concerns as 87% of organizations experienced application security breaches in

Encryption 101

- **Definition:** Encryption is the process of transforming information (plaintext) into an unreadable format (ciphertext) to protect its confidentiality.
- **Key Concepts:**
  - **Plaintext:** The original, readable data.
  - **Ciphertext:** The encrypted, unreadable data.
  - **Key:** A secret value used by an encryption algorithm.
  - **Encryption Algorithm:** A mathematical process for encryption and decryption.
  - **Decryption:** The process of converting ciphertext back into plaintext.
- **Importance:** Encryption is essential for protecting sensitive data in web applications, including passwords, user data, financial transactions, and more.
- **Types of Encryption:**
  - Symmetric Encryption
  - Asymmetric Encryption

Encryption Types

- **Symmetric Encryption:**
  - **Description:** Uses the same key for both encryption and decryption.
  - **Example:** AES (Advanced Encryption Standard)
  - **Advantages:** Fast and efficient.
  - **Disadvantages:** Key distribution can be complex and requires a secure channel.
- **Asymmetric Encryption:**
  - **Description:** Uses a pair of keys: a public key for encryption and a private key for decryption.
  - **Examples:** RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography)
  - **Advantages:** Enables secure key exchange and digital signatures.
  - **Disadvantages:** Slower than symmetric encryption.
- **Encryption in Web Applications:**
  - **In Transit:** HTTPS/TLS encrypts data transmitted between web browsers and servers.
  - **At Rest:** Database encryption protects stored data; file encryption secures uploaded files.
  - **Hashing:** A one-way function used to store passwords securely.

Encryption, Hashing and Encoding

Feature	Encryption	Hashing	Encoding
Purpose	Protect data confidentiality	Ensure data integrity	Convert data into a readable format
Reversible	Yes (with the key)	No (one-way function)	Yes (decoding restores original data)
Use Case	Secure data transfer (e.g., messages, files)	Password storage, file checksums	Data transmission (e.g., Base64 in emails)
Key Required	Yes (for encryption and decryption)	No	No
Examples	AES, RSA, DES	SHA-256, SHA-1, MD5	Base64, ASCII, URL encoding
Security Focus	Confidentiality	Integrity and verification	Readability and transport
Output Format	Appears random	Fixed-length hash	Readable format (e.g., text, URL-safe)

Cryptography in AppSec

Symmetric Encryption

Uses same key for encryption and decryption. Includes AES-256 and ChaCha20-Poly1305 algorithms.

Asymmetric Encryption Encryption

- Uses key pairs for encryption and decryption. Provides foundation for digital signatures and secure key exchange.
- RSA (Public Key Encryption)
- ECC (Elliptic Curve Cryptography)

Hashing

- One-way functions that create fixed-length from variable input. for password storage data integrity.
- Hashing Functions 256, SHA-3)

Key Management

The process of generating, storing, and rotating cryptographic keys. Often the the weakest link in cryptographic implementations.

First Few Milli Seconds of HTTPS

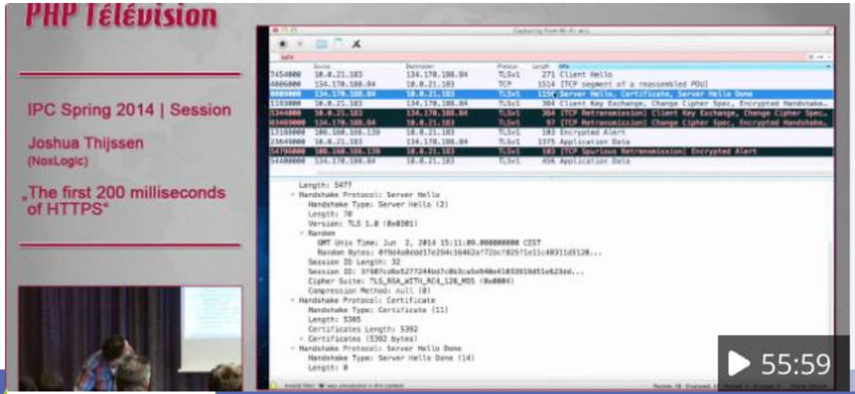
Information Security Stack Exchange

The First Few Milliseconds of an HTTPS Connection [TLS 1.2 / TLS_ECH...

In his blog post, 'The First Few Milliseconds of an HTTPS Connection', Jeff Moser does a wonderful job of walking through the TLS/SSL handshake process, and explaining...

[MIT CSAIL on Twitter / X]()

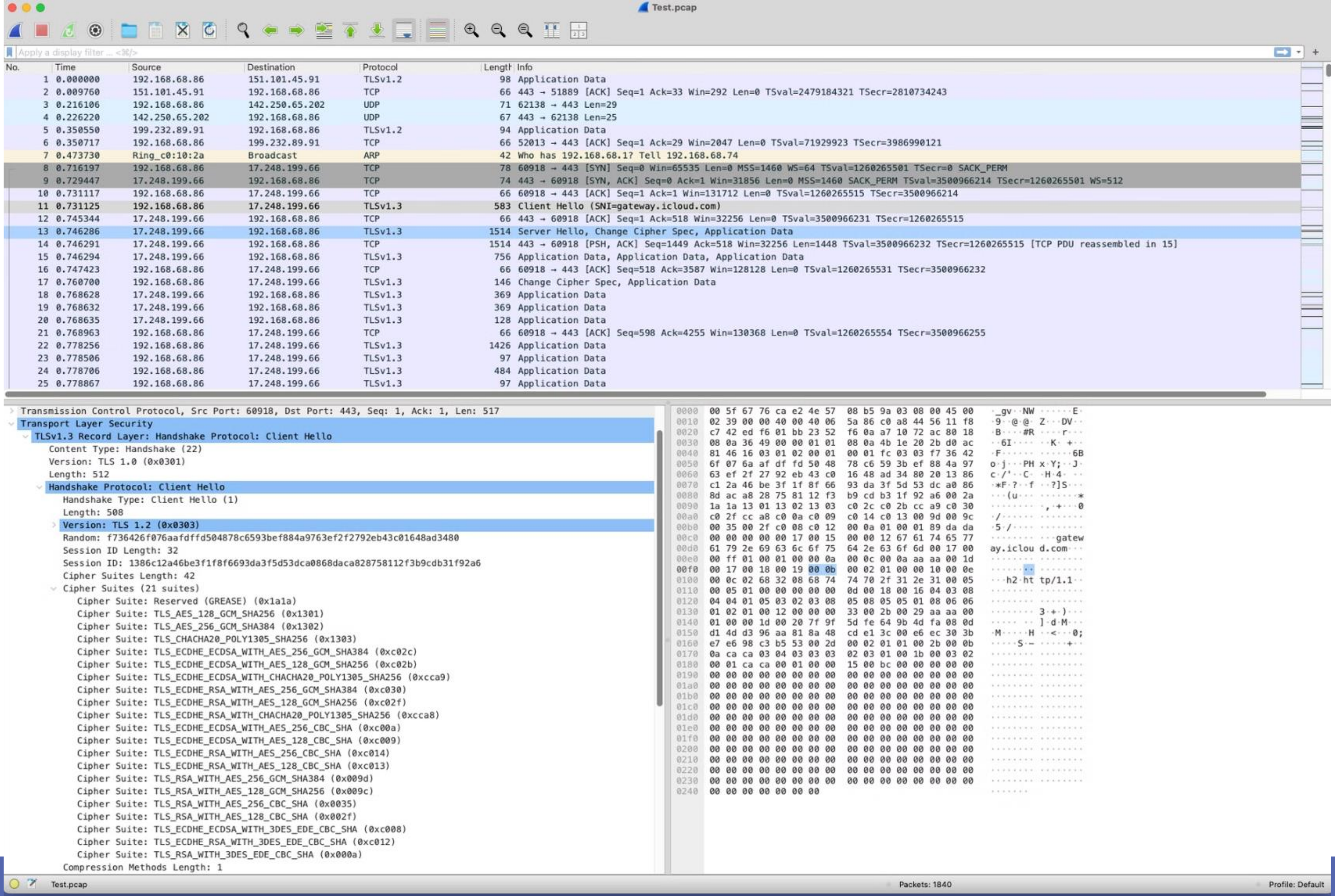
[The First Few Milliseconds of an HTTPS Connection]()



YouTube

The first 200 milliseconds of HTTPS - Joshua Thijssen | IPC14

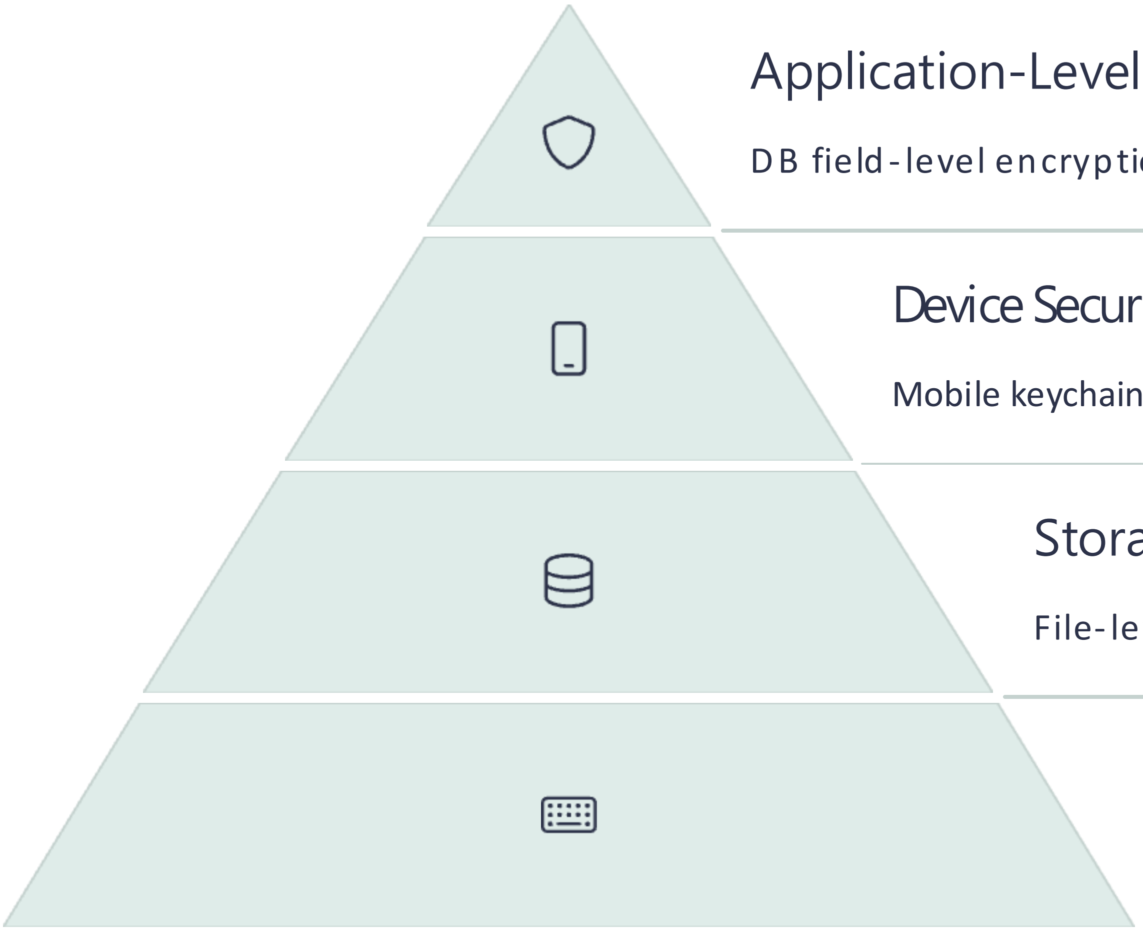
What happens when your browser connects to a HTTPS secure site? We all know it has to do something with certificates, blue and green address bars and sometimes...



ISC2 CHAPTER

SECON INTERNATIONAL

Data-at-Rest Protection



Application-Level Encryption

DB field-level encryption for sensitive web app data

Device Security

Mobile keychain/keystore with hardware-backed encryption

Storage Encryption

File-level and full disk encryption strategies

Key Derivation

Encryption keys derived from user authentication

Proper data-at-rest protection requires multiple layers of security working together.

Authentication Cryptography

Password Hashing

- PBKDF2: Widely supported
- bcrypt: Adaptive work factor
- Argon2: Memory-hard function

Token-Based Auth

- JWT: JSON Web Tokens
- PASETO: Platform-Agnostic Security
- FIDO2: Passwordless authentication

Multi-Factor Authentication

- TOTP: Time-based One-Time Passwords
- Hardware security keys
- Biometrics with secure enclaves

62% of data breaches involve weak or stolen credentials.

Mobile App-Specific Cryptography

Android Keystore

Hardware-backed secure key storage system for Android applications

iOS Secure Enclave

Dedicated security processor that sensitive operations

Code Signing

Verifies app integrity and authenticity through cryptographic cryptographic signatures

Secure Storage

Encrypted SQLite databases and file systems for local data

Common Cryptographic Vulnerabilities

Hard-coded Keys
Found in 35% of vulnerable apps

Weak Algorithms
Insufficient key lengths and outdated ciphers

Insecure RNG
Predictable random number generation

Side-Channel Attacks
Exploiting timing, power, or electromagnetic emissions

Certificate Validation Issues
Affects 27% of apps

Strengths and Limitations

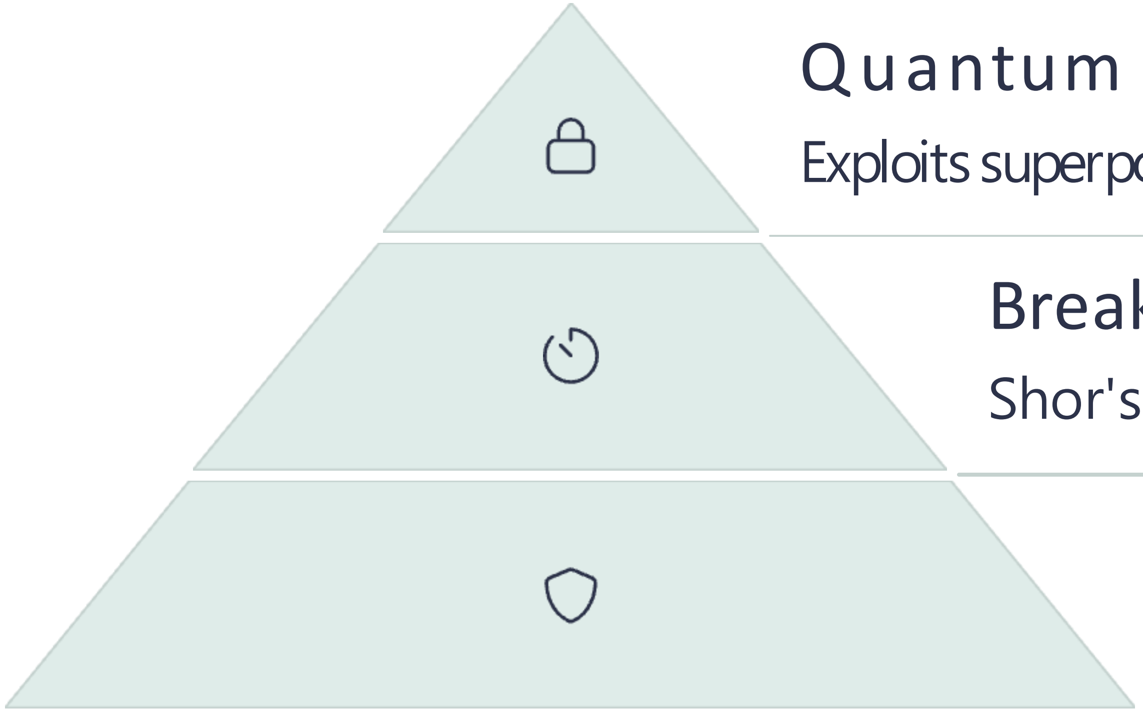
- Based on computational difficulty
- Efficient in classical environments
- Limited resilience against quantum attacks

Post-Quantum Cryptography: The Frontier

Quantum computers threaten today's cryptography standards. Post-quantum cryptography (PQC) will protect sensitive data data from future quantum attacks.

A global cryptographic transition is now Organizations must prepare for this security paradigm shift.

Why Classical Cryptography Is at Risk



Quantum Advantage

Exploits superposition and entanglement

Breaking Encryption

Shor's algorithm breaks RSA and ECC in hours

Critical Vulnerabilities

Communications and infrastructure at risk

Breaking Modern AppSec

Shor's Algorithm

Can break RSA and ECC encryption
than classical methods

Authentication Risk

Digital signatures and certificates become vulnerable

TLS Vulnerable

Secure communications channels could be compromi

Data Exposure

Encrypted data stores may be decryptable retroactively

Attack Scenarios

Attack Scenario 1 - HTTPS/TLS Interception

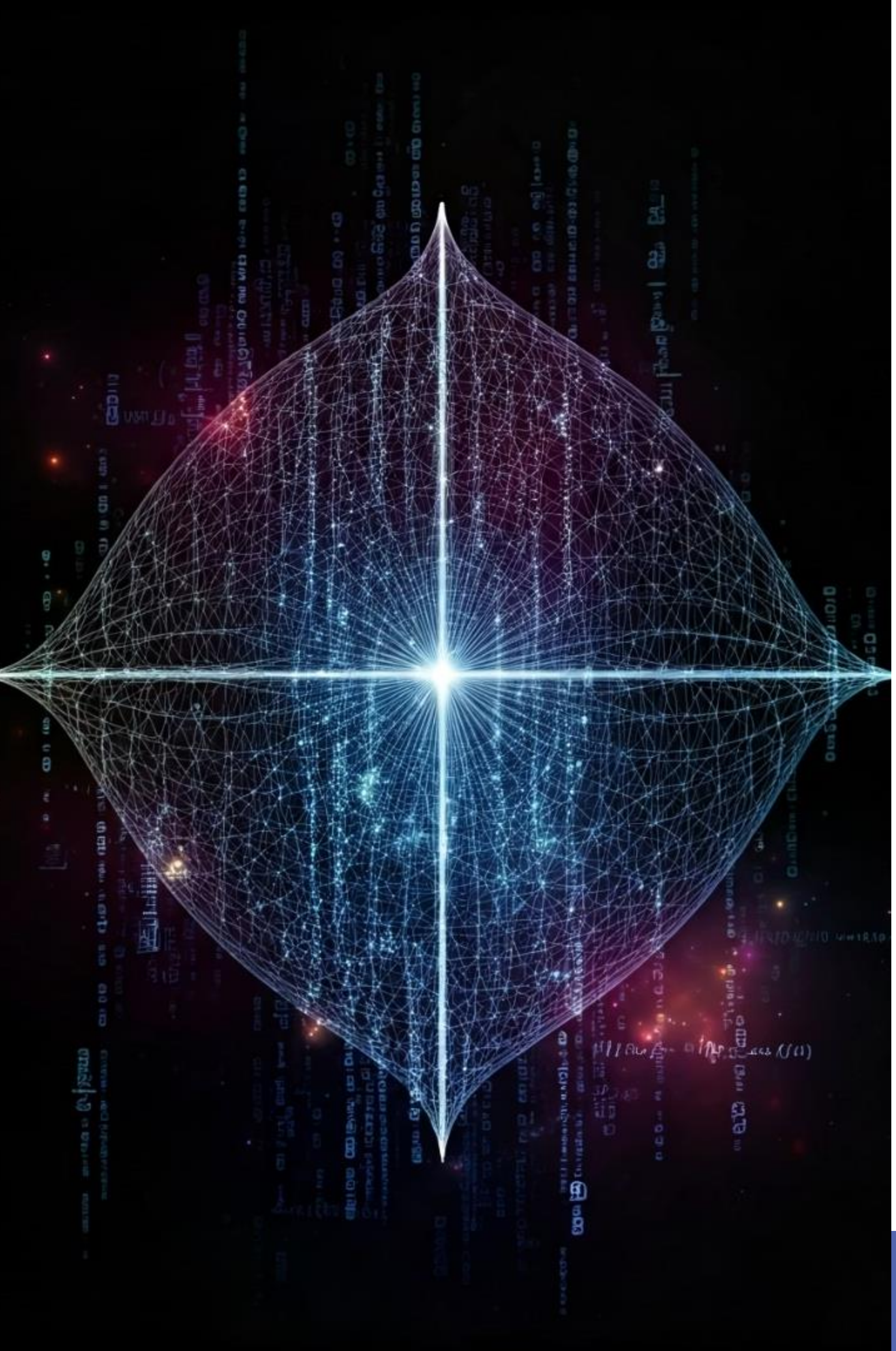
- Harvest now, decrypt later
- Long-term confidentiality risk

Attack Scenario 2 - Mobile Authentication

- Forging digital signatures
- Compromising app logins and messages

Attack Scenario 3 - Blockchain & Crypto

- Breaking wallet security
- Stealing crypto-assets



What Is Post-Quantum Cryptography (PQC)?

Quantum-Resistant Security

Secure against both quantum and classical classical attack vectors vectors

Complex Mathematics

Uses problems quantum can't easily solve

Practical Implementation

Designed for seamless integration with existing IT systems

Post-Quantum Cryptography

Lattice-Based

Uses high-dimensional mathematical lattices. NIST's top for standardization.

Hash-Based

Builds signatures using hash functions. Simple but larger signature sizes.

Code-Based

Relies on error-correcting codes. Well-studied but requires large

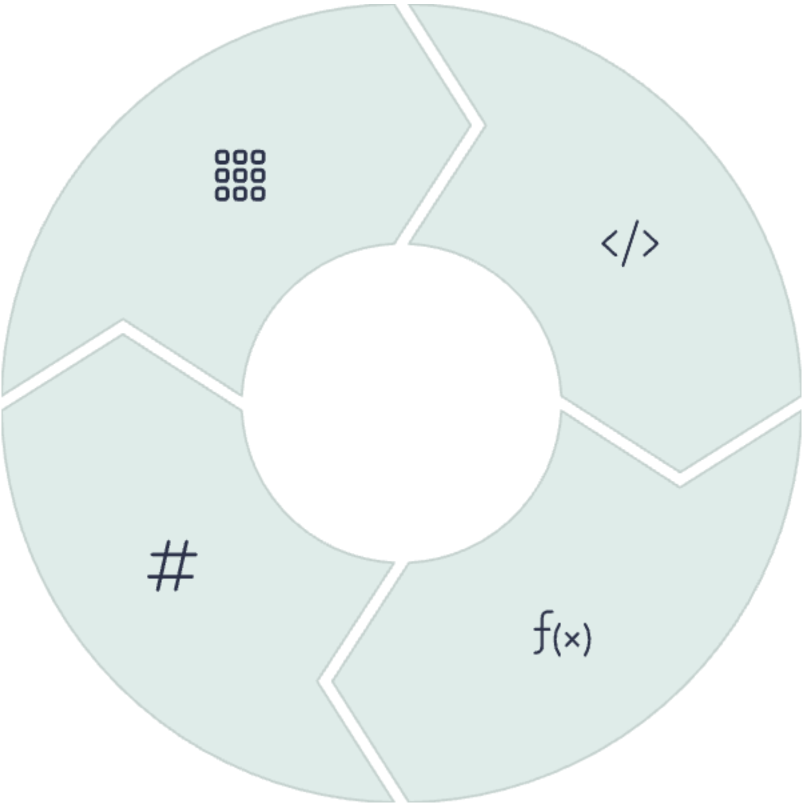
Multivariate

Based on difficulty of solving multivariate polynomial equations. equations. Compact signatures.

Main Categories of PQC Algorithms

Lattice-based

Uses math problems based on dimensional grids (lattices), like short vector problem. CRYSTALS-Kyber (ML-KEM), Dilithium (ML-DSA)



Code-based

Based on the difficulty of decoding error-correcting codes (used in data transmissi
Classic McEliece

Hash-based

Builds digital signatures using secure hash functions; very reliable but large.
SPHINCS+

Multivariate

Involves solving a complex polynomial equations over finite fields.

CRYSTALS - Cryptographic Suite for Algebraic Lattices. All of these have different variants.

NIST PQC Standardization: Leading Algorithms

CRYSTALS-Kyber

Selected for encryption and key exchange. excellent balance of security and performance.

- Lattice-based security
- Compact keys
- Efficient processing

CRYSTALS-Dilithium

Selected for digital signatures. Provides strong verification with reasonable size requirements.

- Fast verification
- Strong security proofs
- Implementation flexibility

NIST-Selected PQC Algorithms (2022):

Algorithm	Purpose	Type
Kyber	Encryption & key exchange	Lattice-based
Dilithium	Digital signatures	Lattice-based
SPHINCS+	Digital signatures	Hash-based

Real-World Applications and Migration Challeng

Federal Mandates

U.S. agencies preparing for quantum-safe systems

Global Banking

Financial networks upgrading encryption standards

Cloud Infrastructure

Providers implementing quantum-resistant protocols

IoT Devices

Resource constraints require optimized algorithms

The Future: Safeguarding Safeguarding Data in a Quantum World

Awareness

Organizations must recognize quantum threats now. Security Security planning should include PQC roadmaps.

Collaboration

Government, industry, and academia must work Standards development requires diverse expertise.

Implementation

Proactive adoption is crucial. Organizations that start start early gain security advantages.

Future of Cryptography in AppSec

Post-Quantum Cryptography

gorithms resistant to quantum computing attacks

Zero-Knowledge Proofs

Verify without revealing underlying data

Homomorphic Encryption

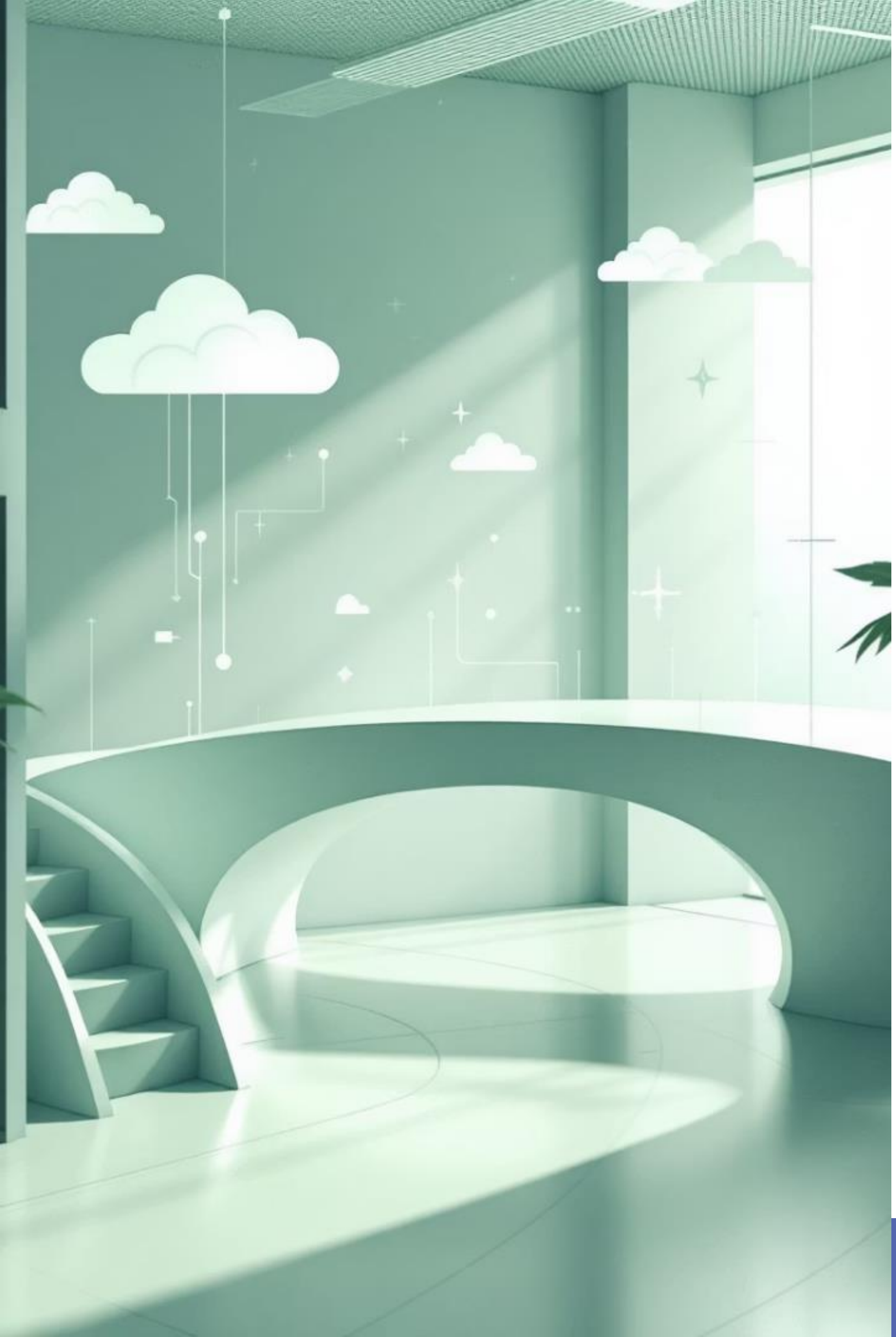
Compute on encrypted data without decryption

Secure Multi-Party Computation

Joint computation while keeping inputs private

Shift-Left Security

utomated crypto-testing in development pipeline



Quantum-Safe Migration Strategy Strategy

Cryptographic Inventory

Identify all crypto-dependent assets and algorithms

Risk Assessment

Evaluate data lifespan and quantum threat exposure

Crypto Agility

Implement systems that can rapidly switch encryption methods

Hybrid Approach

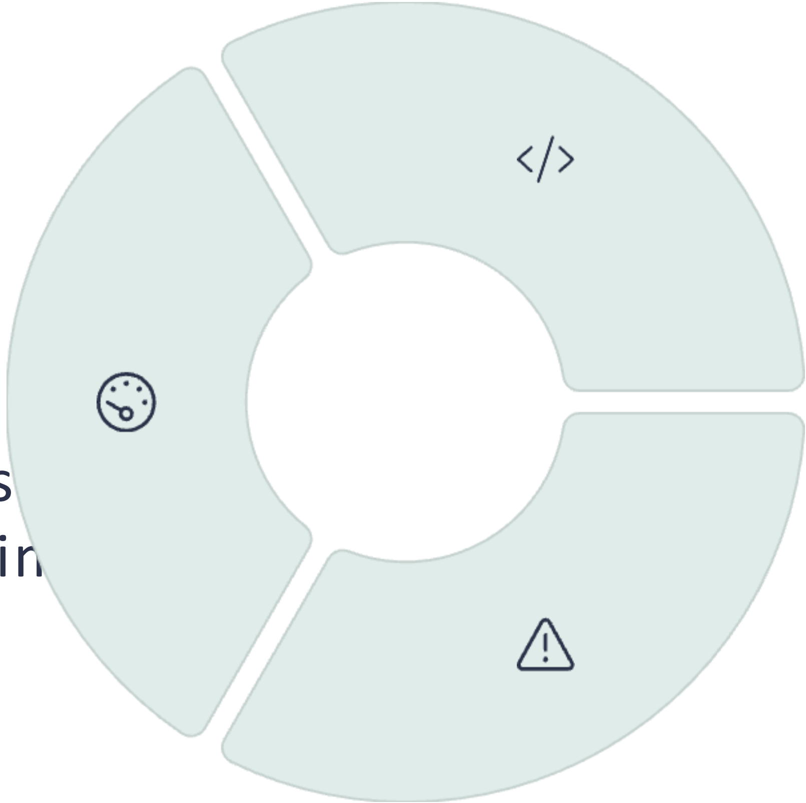
Deploy classical + post-quantum algorithms togethe

Implementation Challenges

Performance Impact

PQC algorithms require require more computational resources resources

- Larger keys and signatures
- Increased processing tin



Integration Complexit

Legacy systems present present migration challenges

- Hardware dependencies
- Third-party components

Immature Standards

PQC standards still evolving

- Implementation uncertainty
- Potential algorithm vulnerabilities

Action Plan for AppSec Teams

Educate Your Organization

Build quantum computing awareness. Train security and and development teams on PQC basics.

Update Security Requirements

Add quantum-resistance to security policies. vendor evaluations.

Start Proof-of-Concept Projects

Experiment with PQC libraries. Test performance and and integration in non-production environments.

Engage with Standards Bodies

Follow NIST and other standardization efforts. Participate in industry working groups.

References

- https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
- https://csrc.nist.gov/projects/post-quantum-cryptography
- https://quantumai.google/quantumcomputer
- https://research.ibm.com/blog/ibm-quantum-characterization-lab-tour
- https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/
- https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip
- https://blogs.iu.edu/sciu/tag/superposition/
- https://ncase.me/qc-outline/
- https://www.youtube.com/watch?v=ni1x44mCgWE
- https://www.youtube.com/watch?v=RQWpF2Gb-gU

Thank You


Sheshananda Reddy Kandula
Sr Security Engineer at Adobe | AppSec |
Product Securtiy | OSWE | OSCP | CISSP

SECON 2025
NEW JERSEY

Thank You

ISC2 CHAPTER
SECON INTERNATIONAL