Transitioning to Post-Quantum Cryptography in IAM

Udara Pathum

Senior Software Engineer - WSO2

udarap@wso2.com

Post-Quantum Cryptography Conference | 28-30 October, 2025 | Kuala Lumpur, Malaysia

What Encrypts Today Can Be Stolen and Broken by Tomorrow's Quantum Computers

Understanding Identity and Access Management

- Framework that manages digital identities and access control
- Core functions:
  - **Authentication**: Verifying user identity
  - **Authorization**: Granting appropriate permissions
  - **User Management**: Account lifecycle management
  - **Governance**: Monitoring and compliance

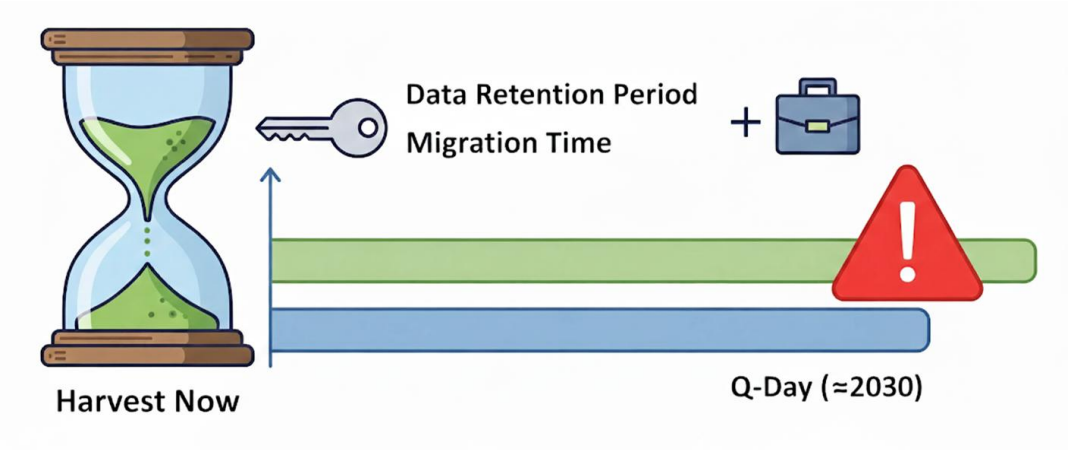
Every enterprise interaction flows through IAM - making it a critical target for quantum attacks.

IAM Cryptography Dependencies

IAM Component	Role	Current Algorithms	PQ Impact
TLS Connections	Secure communication	RSA/ECDHE	Vulnerable
PKI	Certificates, signatures	RSA/ECDSA	Vulnerable
SSO Signing (SAML/OIDC)	Assertion & token signing	RSA/ECDSA	Vulnerable
SSO Encryption (JWE)	Token encryption	RSA/ECDSA + AES	Vulnerable
IDP Secrets	Credential encryption	AES	Safe (For now)
Password hashing	Secrets (OAuth2, passwords)	PBKDF2 / SHA-2 / SHA-3 / bcrypt	Safe (For now)

Post-Quantum Risk Assessment in IAM

- **Harvest Now, Decrypt Later:** Encrypted traffic and IAM data can be captured today and decrypted in the future.
  - **High-risk:** Captured TLS traffic → PII, credentials, session tokens, and authorization info.
  - **Medium-risk:** Stored SAML assertions, JWTs, and ID tokens.
  - **Low-risk:** Password hashes, short-lived secrets — harder to exploit with PQ attacks.



Securing IAM via Hybrid Algorithms

Why Hybrid Algorithms?

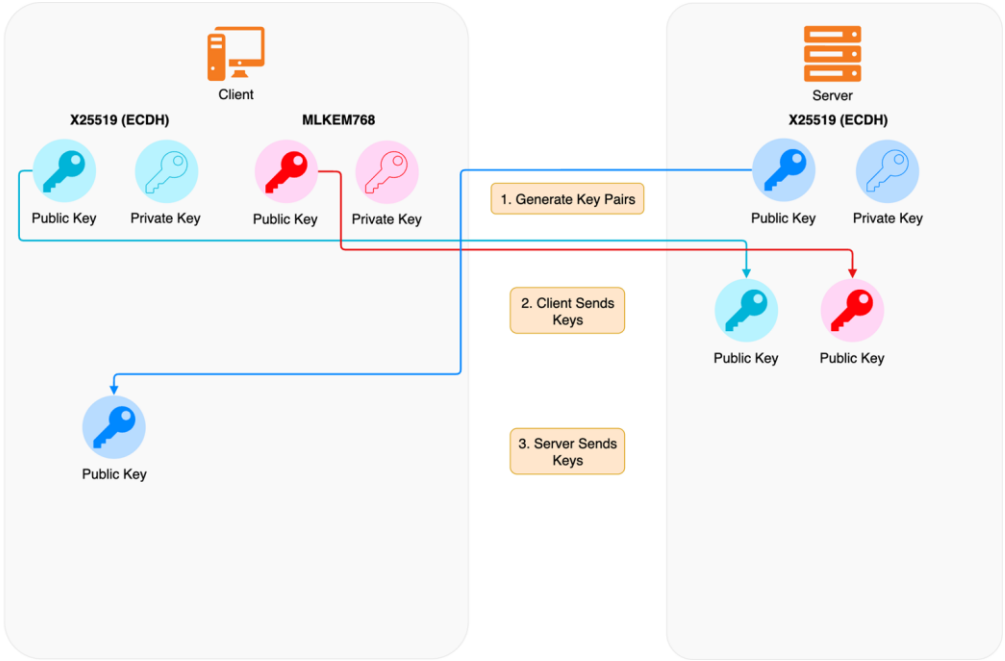
- Need to prevent Harvest Now, Decrypt Later (HNDL) Attacks
- Replacing classical algorithms with PQ algorithms is not **yet** recommendable
  - PQ algorithms could have hidden vulnerabilities (e.g. KyberSlash)
  - Difficulty to migrate from existing crypto infrastructure (e.g PKI, TLS configs)
  - Need to preserve compatibility with existing clients

Why Hybrid Algorithms?

- Need to prevent Harvest Now, Decrypt Later (HNDL) Attacks
- Replacing classical algorithms with PQ algorithms is not **yet** recommendable
  - PQ algorithms could have hidden vulnerabilities (e.g. KyberSlash)
  - Difficulty to migrate from existing crypto infrastructure (e.g PKI, TLS configs)
  - Need to preserve compatibility with existing clients
- **Hybrid algorithms:** Classical + post-quantum primitives.
- Currently used in:
  - TLS communication
  - Digital signatures
  - Hybrid encryption

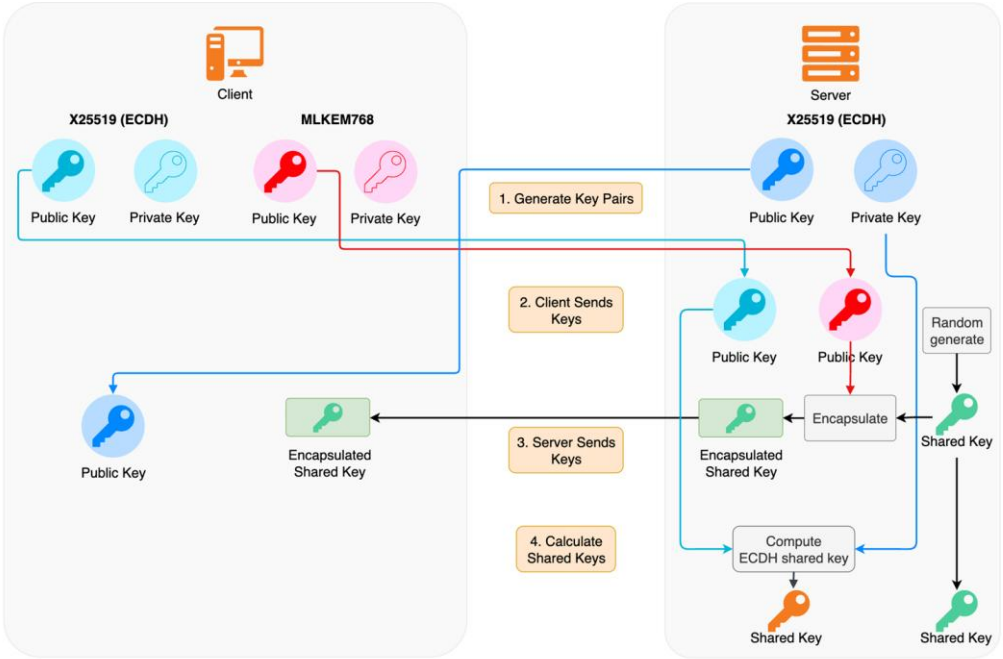
Post-Quantum TLS

- Combine classical key exchange (RSA/ECDHE) with PQ key exchange (ML-KEM)



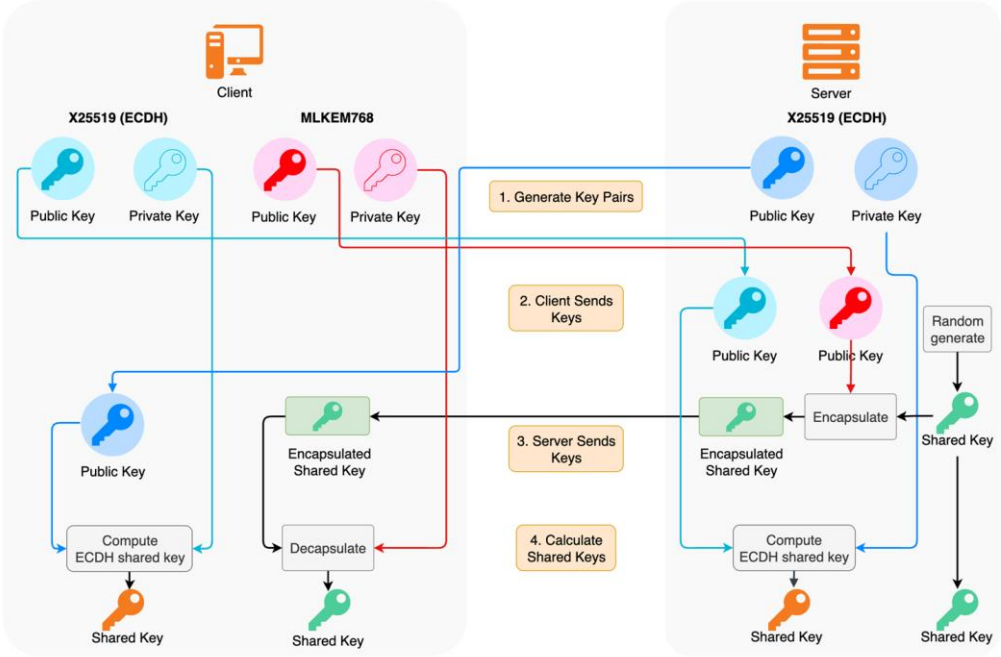
Post-Quantum TLS

- Combine classical key exchange (RSA/ECDHE) with PQ key exchange (ML-KEM)



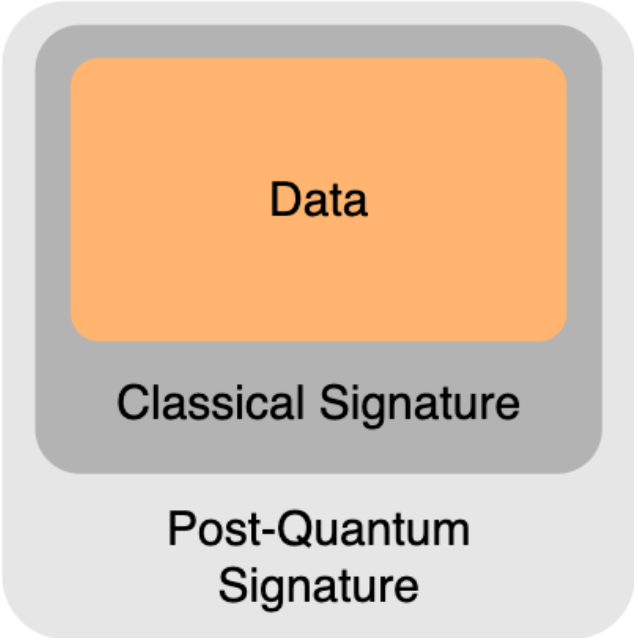
Post-Quantum TLS

- Combine classical key exchange (RSA/ECDHE) with PQ key exchange (ML-KEM)
- Maintains compatibility with legacy clients
- Protects IAM communications end-to-end



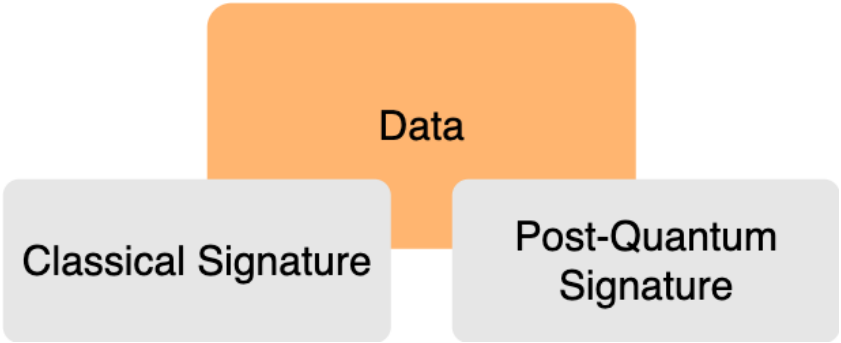
Hybrid Digital Signatures

- Combine classical digital signatures (RSA/ECDSA) with PQ digital signatures (ML-DSA)
- Two hybrid approaches:
  - Nested Hybrid Signature



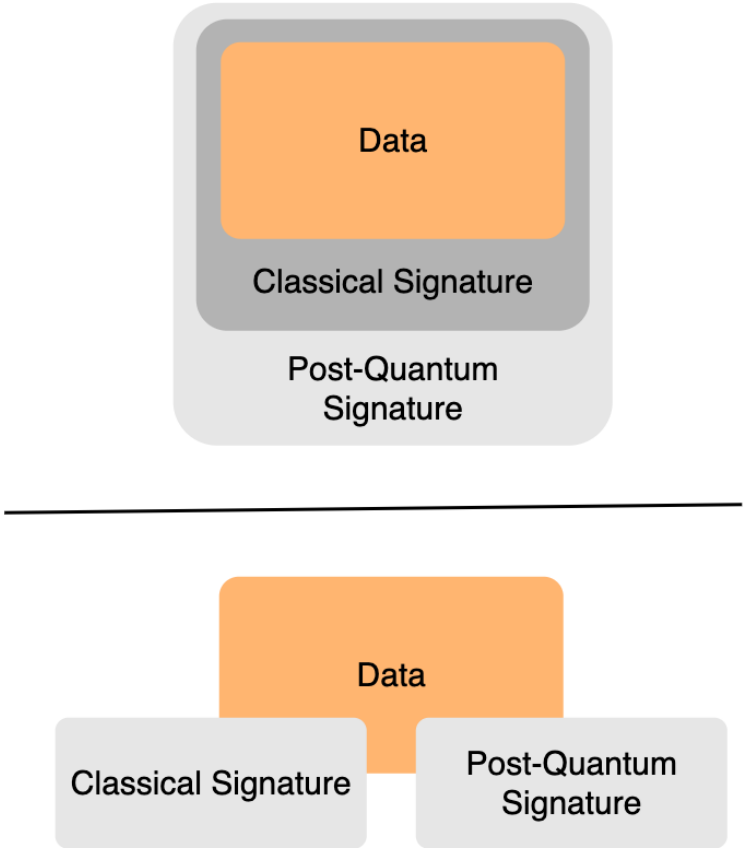
Hybrid Digital Signatures

- Combine classical digital signatures (RSA/ECDSA) with PQ digital signatures (ML-DSA)
- Two hybrid approaches:
  - Nested Hybrid Signature
  - Parallel Hybrid Signature



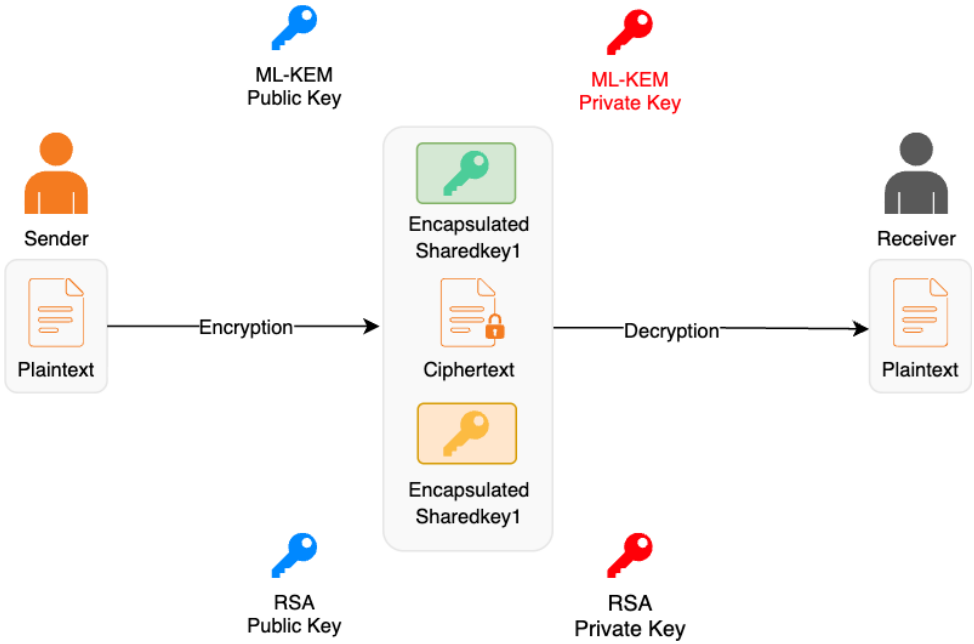
Hybrid Digital Signatures

- Combine classical digital signatures (RSA/ECDSA) with PQ digital signatures (ML-DSA)
- Two hybrid approaches:
  - Nested Hybrid Signature
  - Parallel Hybrid Signature
- Can be used for
  - OIDC / SAML assertion signing
  - OIDC / SAML request signing
  - Acces token / ID token signing



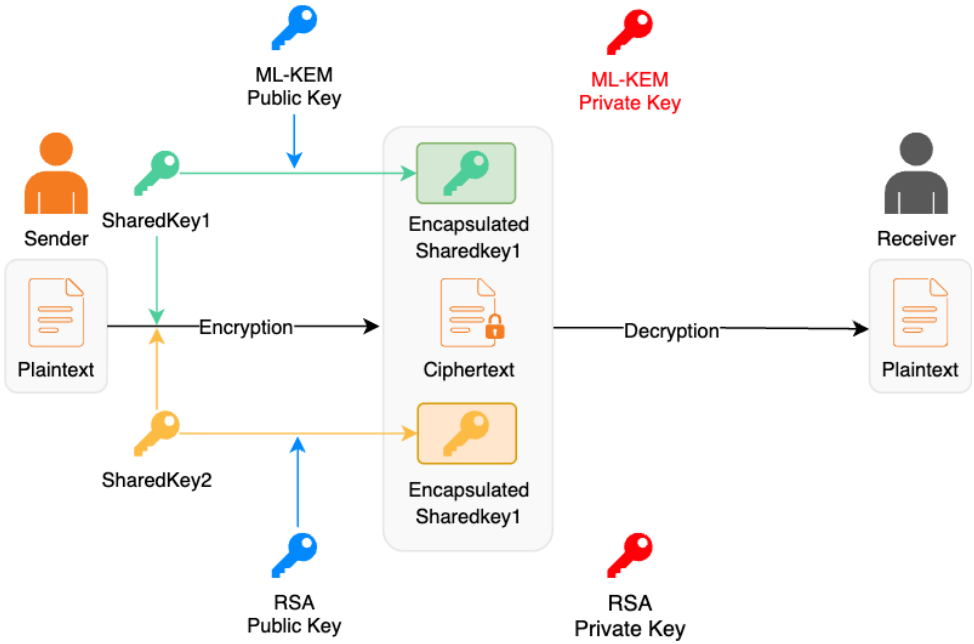
Post-Quantum Hybrid Public-Key Encryption (HPKE)

- Based on HPKE framework
- Composite KEM
  - Classical KEM (DH/ECDH) + PQ KEM (ML-KEM) combined in parallel



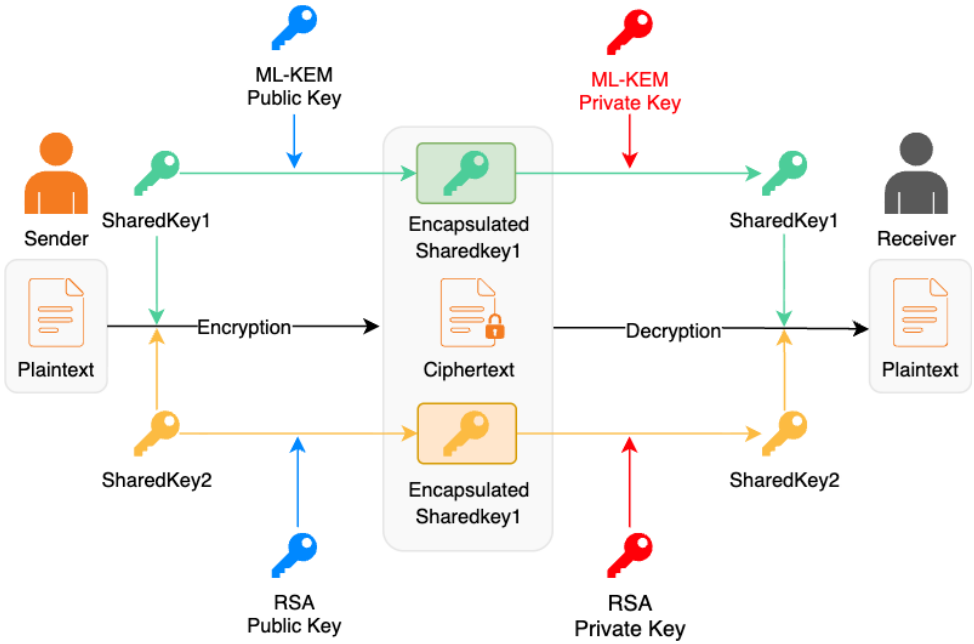
Post-Quantum Hybrid Public-Key Encryption (HPKE)

- Based on HPKE framework
- Composite KEM
  - Classical KEM (DH/ECDH) + PQ KEM (ML-KEM) combined in parallel



Post-Quantum Hybrid Public-Key Encryption (HPKE)

- Based on HPKE framework
- Composite KEM
  - Classical KEM (DH/ECDH) + PQ KEM (ML-KEM) combined in parallel
- Can be used for
  - Encrypted JWE ID tokens in OIDC / SAML flows



Towards Quantum-Safe IAM

Why Migration to PQC is Hard

- Lack of Standards for IAM Protocols
  - OIDC, SAML, JWS, JWE PQ specifications are still in progress
- Web Browser Compatibility
  - PQ certificate signing and PQ TLS may not be fully supported
- Client & Application Compatibility
  - OIDC/SAML clients may not yet handle PQ algorithms
- Cloud Provider Support
  - Many cloud providers have adopted PQ algorithms; full support is pending
- Limited PQ Libraries
  - PQ implementations are missing for some programming languages and frameworks

Ensuring Crypto Agility in IAM

- **Crypto Agility:** The ability to easily switch cryptographic algorithms in production systems with minimal effort
- More algorithms will be vulnerable tomorrow. Better play it safe
- Best Practices
  - Use abstraction layers for crypto libraries
  - Avoid hardcoding algorithms or key sizes
  - Plan for data migration (e.g. encryption key rotation)
  - Plan for certificate updates
  - Plan password migration to avoid forced reset

Reinforcing IAM with Zero Trust

- **Zero Trust Principle:** Never trust, always verify
  - Continuously Monitor and Validate
  - Enforce Least Privileged Access
  - Assume Breach
- Why it matters for PQC
  - Limits damage even if quantum-compromised credentials are used
  - Helps enforce cryptographic compliance at every boundary


ATTACKERS DON'T WAIT,
NEITHER SHOULD YOU

Thanks!

wso2.com




Post-Quantum

Cryptography Conference

Transitioning to Post-Quantum Cryptography in IAM

Udara Pathum
Senior Software Engineer at WSO2

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium