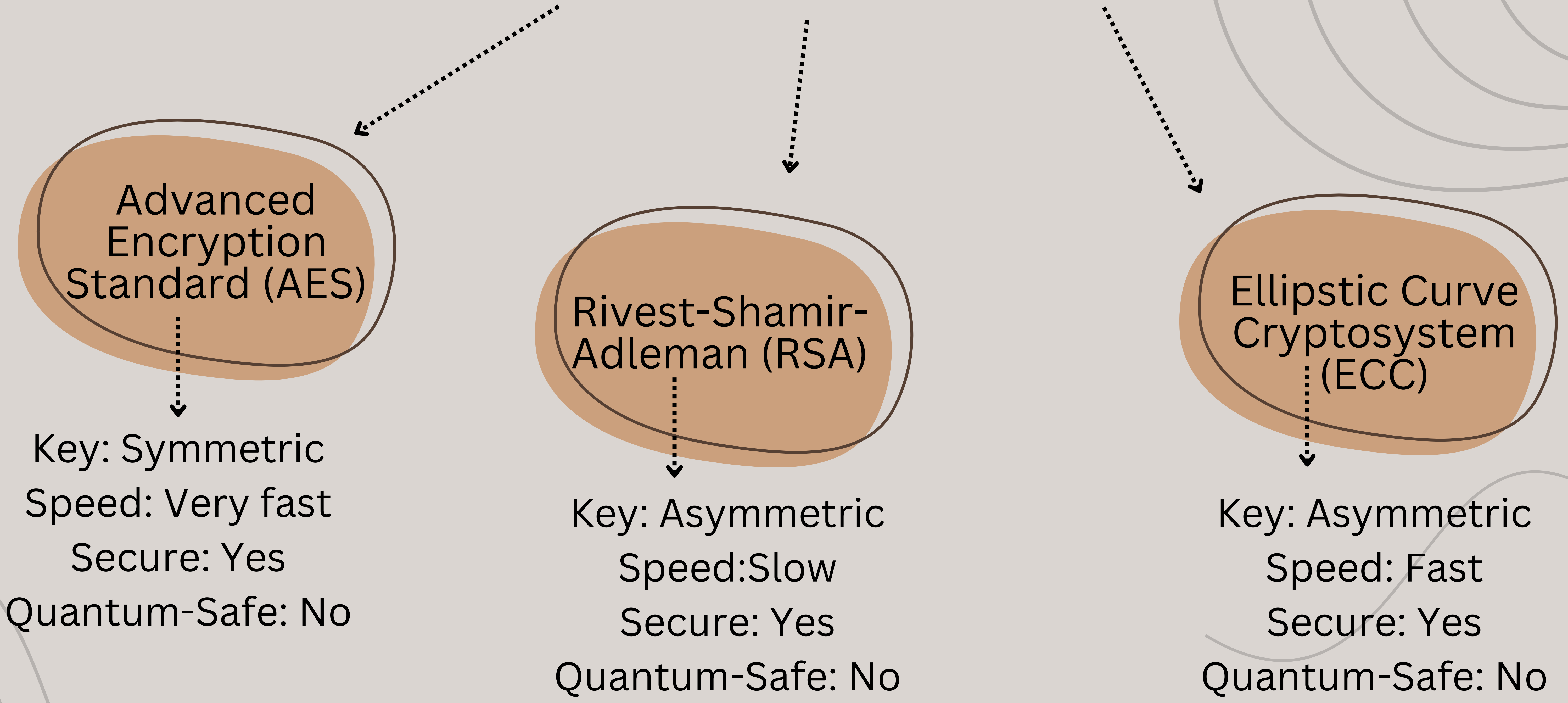
PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA

UNIT POLISI, PERUNDANGAN DAN KESEDARAN

Encryption Algorithms



Advanced Encryption Standard (AES)

Key: Symmetric
Speed: Very fast
Secure: Yes
Quantum-Safe: No

Rivest-Shamir-Adleman (RSA)

Key: Asymmetric
Speed:Slow
Secure: Yes
Quantum-Safe: No

Ellipstic Curve Cryptosystem (ECC)

Key: Asymmetric
Speed: Fast
Secure: Yes
Quantum-Safe: No

RSA

Type: Asymmetric encryption (Public Key Cryptography)

How it works: Based on the difficulty of factoring large prime numbers

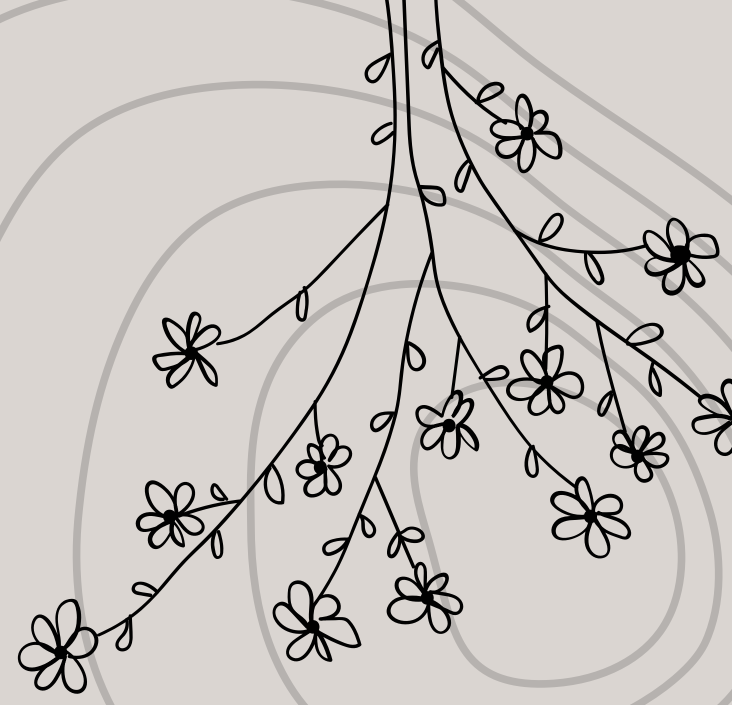
Common Uses: Secure web browsing (HTTPS), digital signatures, encrypted emails, VPNs

Strengths:

- Well-studied and widely used in security systems.
- Public-key cryptography allows secure key exchange.

Weaknesses:

- Slow performance compared to modern encryption.
- Vulnerable to quantum computers (Shor’s Algorithm can efficiently factorize large numbers).



ECC

Type: Asymmetric encryption (Public Key Cryptography)

How it works: Uses elliptic curve mathematics instead of prime factorization

Common Uses: Secure messaging (Signal, WhatsApp), digital signatures, blockchain

Strength:

- Stronger security per bit than RSA (256-bit ECC ≈ 3072-bit RSA).
- Faster and more efficient for mobile & IoT devices.

Weaknesses:

- Complex mathematics makes it harder to implement securely.
- Vulnerable to quantum attacks (Shor's Algorithm can break ECC).

Malaysian Industries

Financial & Banking Industry

Cybersecurity & Cryptography

Telecommunications & Networking

Manufacturing & Automation

AI & Big Data

E-Commerce & Logistics

Healthcare & Biotechnology

Financial & Banking Industry

Algorithms Used:

- **RSA (USA) & ECC (USA) (Elliptic Curve Cryptography)** : Used for securing online transactions, digital signatures, and e-wallets.
- **AES (Belgium) (Advanced Encryption Standard)**: Protects sensitive banking data from cyber threats.
- **Machine Learning (ML)**: Enhances fraud detection by analyzing transaction patterns and identifying anomalies.
- **Monte Carlo Simulation (Poland)**: Used in risk assessment and financial modeling.
- **Hedging Algorithms (USA)**: Optimize stock market trading strategies.

Cybersecurity & Cryptography

Algorithms Used:

- **Blum Blum Shub (BBS) (USA) & ChaCha20 (USA)**: Used in pseudorandom number generation for cryptographic applications.
- **SHA-256 & SHA-3 (USA)** : Secure hashing algorithms used in blockchain and password encryption.
- **Zero-Knowledge Proof (ZKP) (USA)**: Enables secure authentication without revealing private information, widely applied in fintech and blockchain security.
- **Public Key Infrastructure (PKI) (UK/USA)** : Ensures secure communications through encryption and digital certificates.

Telecommunications & Networking

Algorithms Used:

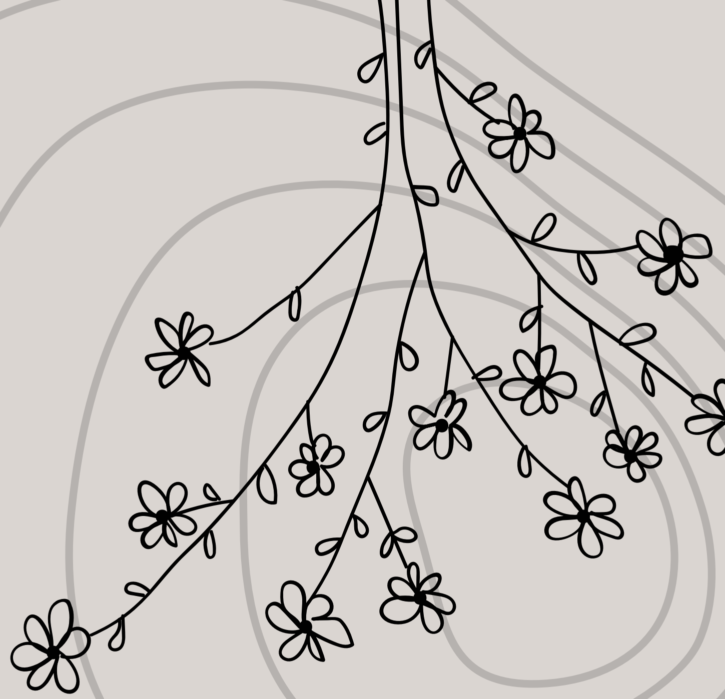
- **Dijkstra’s Algorithm (USA)**: Finds the shortest path in network routing to optimize data transmission.
- **RSA & Diffie-Hellman (USA)**: Ensures secure key exchange for encrypted communication.
- **Huffman Coding (USA)**: Reduces data size for efficient transmission and storage.
- **Error Detection & Correction (CRC, Hamming Code) (USA)**: Ensures data integrity in wireless communication.

Manufacturing & Automation

Algorithms Used:

- **Genetic Algorithm (GA) (USA)**: Optimizes production scheduling and robotics path planning.
- **Fuzzy Logic (USA)**: Enhances automated control systems such as temperature regulation and energy efficiency in smart factories.
- **Neural Networks (USA)**: Used in predictive maintenance to detect machinery failures in advance.
- **Linear Programming (USA)**: Optimizes supply chain management and resource allocation.

AI & Big Data



Algorithms Used:

- **Neural Networks (ANN, CNN, RNN)**: Used for image and speech recognition in AI applications.
- **Random Forest & XGBoost**: Applied in data analytics and customer behavior prediction.
- **Clustering Algorithms (K-Means, DBSCAN)**: Helps in market segmentation and targeted marketing.
- **Reinforcement Learning**: Improves AI-driven automation and robotics decision-making.

E-Commerce & Logistics

Algorithms Used:

- **Apriori Algorithm**: Analyzes customer purchase patterns for personalized recommendations.
- **A Algorithm**:* Optimizes delivery routes for logistics companies.
- **Collaborative Filtering**: Used in recommendation systems (e.g., Shopee, Lazada).
- **Inventory Optimization Algorithms**: Predict demand and reduce stock wastage.

Healthcare & Biotechnology

Algorithms Used:

- **Support Vector Machine (SVM) & k-Nearest Neighbors (k-NN)**: Applied in medical image analysis and disease diagnosis.
- **Deep Learning (CNN)**: Used in MRI classification, tumor detection, and drug discovery.
- **Bioinformatics Algorithms**: Analyze DNA sequences for genetic research.
- **Logistic Regression**: Helps in predicting disease outbreaks based on historical data.

Post Quantum Cryptography (PQC)

Cryptographic algorithms are important for safeguarding confidential electronic information from unauthorized access. For decades, these algorithms have proved strong enough to defend against attacks using conventional computers that attempt to defeat cryptography. However, future quantum computing may be able to break these algorithms, causing data and information to become vulnerable. Countering this future quantum capability requires new cryptographic methods that can protect data from both current conventional computers and the quantum computers of tomorrow. These methods are referred to as post-quantum cryptography (PQC). PQC is a new class of cryptographic algorithms that are resistant to attacks from quantum computers. Unlike RSA and ECC, which can be broken by quantum computers using Shor’s Algorithm, PQC relies on mathematical problems that quantum computers cannot efficiently solve.

PQC

Type: Cryptographic algorithms that resist quantum attacks

How it works: Based on mathematical problems that quantum computers can't easily solve

Why it matters: Governments & industries are transitioning to quantum-safe encryption

Primary PQC algorithms:

- **Kyber (Encryption) –** Lattice-based encryption, replacing RSA/ECC
- **Dilithium (Signatures) –** Lattice-based digital signatures
- **SPHINCS+ (Signatures)** – Hash-based signatures
- **Falcon (Signatures) –** Alternative digital signature scheme

Main Goal:

Find encryption methods that remain secure even when large quantum computers exist.

PQC Standard

National Institute of Standards and Technology (NIST) - USA

Federal Information Processing Standards (FIPS) is official PQC standard created by NIST-USA

- **FIPS 203**: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, derived from CRYSTALS-KYBER).
- **FIPS 204**: Module-Lattice-Based Digital Signature Algorithm (ML-DSA, derived from CRYSTALS-Dilithium).
- **FIPS 205**: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA, derived from SPHINCS+).
- **Future Standards**: NIST is evaluating FALCON and other additional digital signature algorithms.

United Kingdom (UK)

WHO?

Government Communications Headquarters (GCHQ)

WHAT?

- Assesing Quantum Threats
- Providing PQC Roadmaps & Guidelines
- Selecting & Recommending PQC Algorithms
- Encouraging Industry & Government Adoption
- Ensuring Smooth Transition

HOW?

National Cyber Security Centre (NCSC)

WHEN?

- By 2028: Identify services that require upgrades.
- By 2031: Prioritize and implement critical overhauls.
- By 2035: Complete the migration to new encryption systems.

United States (US)

WHO?

National Security Agency (NSA) / Central Security Service (CSS)

WHAT?

- Assessing Quantum Computing Threats
- Providing Encryption Guidelines
- Selecting and Approving Quantum-Resistant (PQC) Algorithms
- Guiding US Government and Defense Systems

HOW?

National Institute of Standards Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA)

WHEN?

- 2022: Release of CNSA 2.0 (Quantum-Safe Guidance begins).
- 2024-2025: Finalisation of NIST PQC standards (FIPS 203-205).
- By 2025: Begin adoption in national security systems.
- By 2030: Complete migration to PQC for all US national security systems.

Australia (AUS)

WHO?

Australian Signals Directorate (ASD) / Australian Cyber Security Centre (ACSC)

WHAT?

- Assessing Quantum Threats to Australian Systems
- Developing PQC Roadmaps
- Providing Advice and Alerts on Encryption Best Practices
- Supporting Industry and Government to Transition to Quantum-Safe Solutions
- Working to Ensure a Secure Migration to PQC Over the Coming Years

HOW?

Australian Cyber Security Strategy 2023-2030

WHEN?

- 2023-2025: Awareness and initial planning for PQC transition.
- 2026-2028: Develop clear national guidance for PQC implementation.
- 2030: Begin formal PQC migration across government and key industries.

Canada (CND)

WHO?

Canadian Centre for Cyber Security

WHAT?

- Assessing Quantum Computing Threats to Canadian Systems
- Providing Guidance to Quantum-Safe Encryption
- Selecting, Recommending and Supporting PQC Algorithm Adoption
- Assisting Government and Critical Infrastructure Sectors in Secure Transitions

HOW?

Close partnership NIST-US, GCHQ-UK, ASD-Australia

WHEN?

- 2023-2025: Promote awareness, begin assessing crypto dependencies.
- 2026-2028: Issue detailed PQC migration guidance to federal agencies.
- By 2030: Begin widepsread implementation of PQC across government and key sectors.

China (CHN)

WHO?

China Academy of Information and Communications Technology (CAICT)

WHAT?

- Researching Quantum Computing Threats and Cryptographic Vulnerabilities
- Developing and Testing PQC Algorithms
- Publishing Technical Whitepapers and Roadmaps for Post-Quantum Cryptography
- Support China National Standard on Encryption and Cybersecurity

HOW?

State Cryptography Administration (SCA)

WHEN?

- 2018- 2022: Initiated national level quantum communication and PQC research.
- 2023-2025: Develop and refine domestic PQC standards and algorithms.
- By 2030: Integrate PQC into national infrastructure, 5G/6G, cloud and telecom systems.
- Beyond 2030: Aim for global leadership in quantum communication and cryptography.

Singapore (SG)

WHO?

Defense Science Organisation (DSO)

WHAT?

- Research Advanced Cybersecurity
- Assessing Threats from Quantum Computing and Emerging Digital Warfare
- Developing Secure Encryption System for Defense and National Security
- Supporting the Adoption of Quantum Safe Algorithms and PQC Standards
- Collaborating with Local and International Partners to Strengthen Cyber Defense

HOW?

Centre for Strategic Infocomm Technologies (CIST)

WHEN?

- 2015-2022: Initial R&D in quantum cryptography and secure communications.
- 2023-2025: Begin transitioning to quantum-safe cryptography in classified systems.
- By 2030: Full integration of PQC and quantum- ready systems in national defense.

United Arab Emirates (UAE)

WHO?

Cryptography Research Centre (CRC), Technology Innovation Institute (TII), Advanced Technology Research Council (ATRC)

WHAT?

- Conduct Cutting-Edge Research in Cryptography
- Designing Secure, Scalable Encryption Systems for National Use
- Contributing to Global PQC Standard and Developing UAE-Specific Solutions

HOW?

R&D teams at CRC, partner with NIST

WHEN?

- 2020: CRC launched as part of TII to push cryptographic innovation.
- 2021-2023: Active research on PQC and crypto modernisation begins.
- 2024-2026: Contribute to PQC implementation for critical UAE systems.
- By 2030: Full adoption of quantum resistant systems across UAE government and infrastructure.

NIST Post-Quantum Cryptography Standardization Project

Process:

In 2016, NIST select public-key cryptographic algorithm through a public competition-like process

After 3 rounds of evaluation, the selected KEM algorithm is CRYSTAL-Kyber, and the chosen digital signatures are CRYSTALS-Dilithium, Falcon, and SPHINCS+.

In the fourth round in 2022, NIST reviewed four KEM candidates which are BIKE, CLassic McEliece, HQC and SIKE which then HQC was chosen to be standardized

NIST Post-Quantum Cryptography Standardization Project

Evaluation Criteria:

Security

Cost and Performance

Algorithm and Implementation Characteristic

Summary Of the Evaluation Process in the Fourth Round

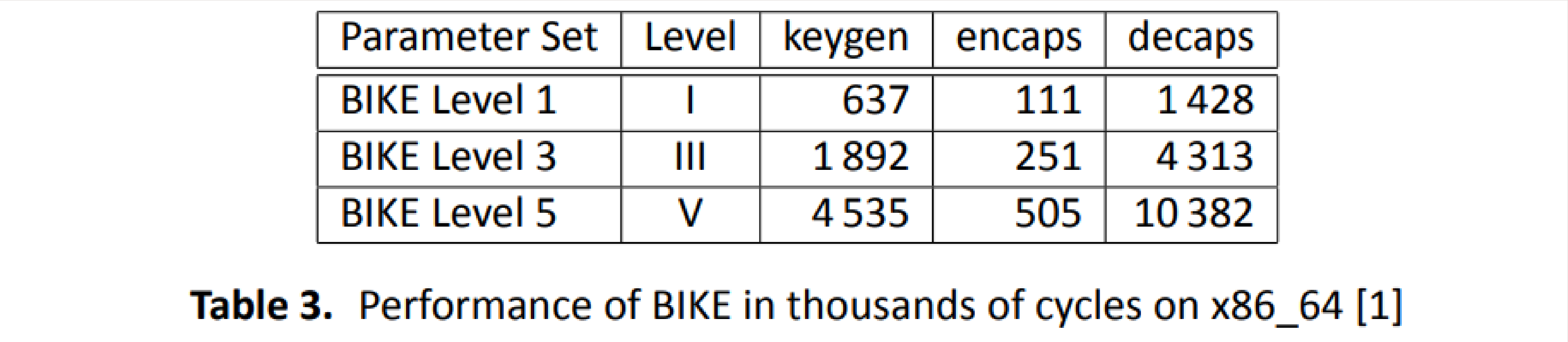
SECURITY

- In the third round, Kyber (ML-KEM) was standardized.
- In the fourth round, NIST selected candidates whose security was based on totally different computational assumptions as ML-KEM (Isogeny-based KEM: SIKE, Code-based KEM: BIKE, HQC, Classic McEliece).
- The candidates are evaluated according to the IND-CCA2 security standard.
- In the third round, ML-KEM was believed to satisfy the IND-CCA2 security. In the fourth round, SIKE did not fulfil this security standard and thus was removed from the candidate list.
- BIKE satisfies the IND-CCA2 with minor modification while HQC passed without any modification, leading NIST to have higher confidence in IND-CCA2 security of HQC.

Summary Of the Evaluation Process in the Fourth Round

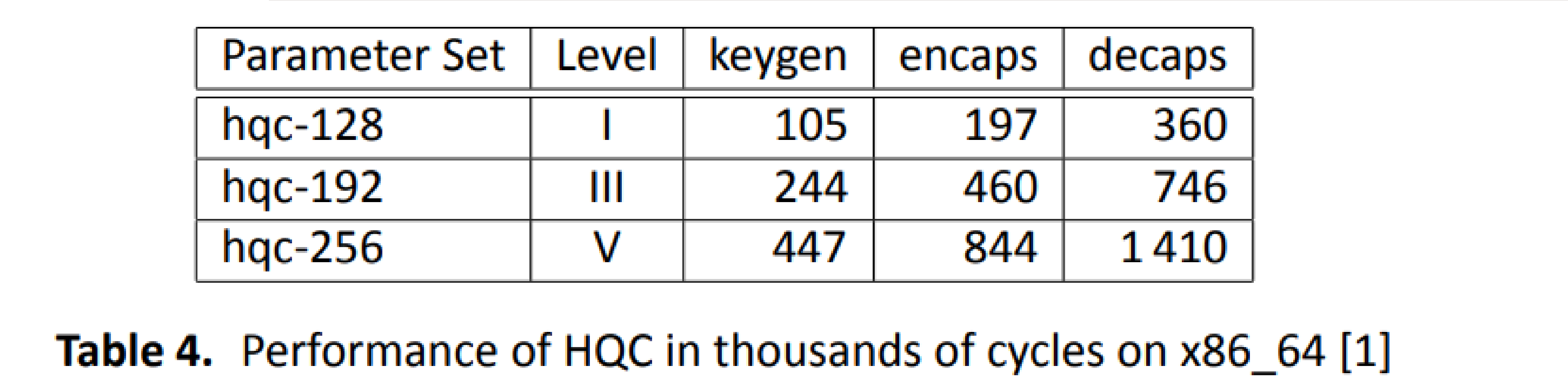
COST AND PERFORMANCE

- The performance characteristics:
    - Sizes of encapsulation keys and ciphertext.
    - Computational efficiencies of encapsulations, decapsulations, and key generations (speed of the algorithms)
- BIKE is 6-10 times slower than HQC in key generation, 5-7 times slower in decapsulation and approximately twice as fast as HQC in encapsulation.
- McEliece is an exception as it is three orders of magnitude more costly than HQC.



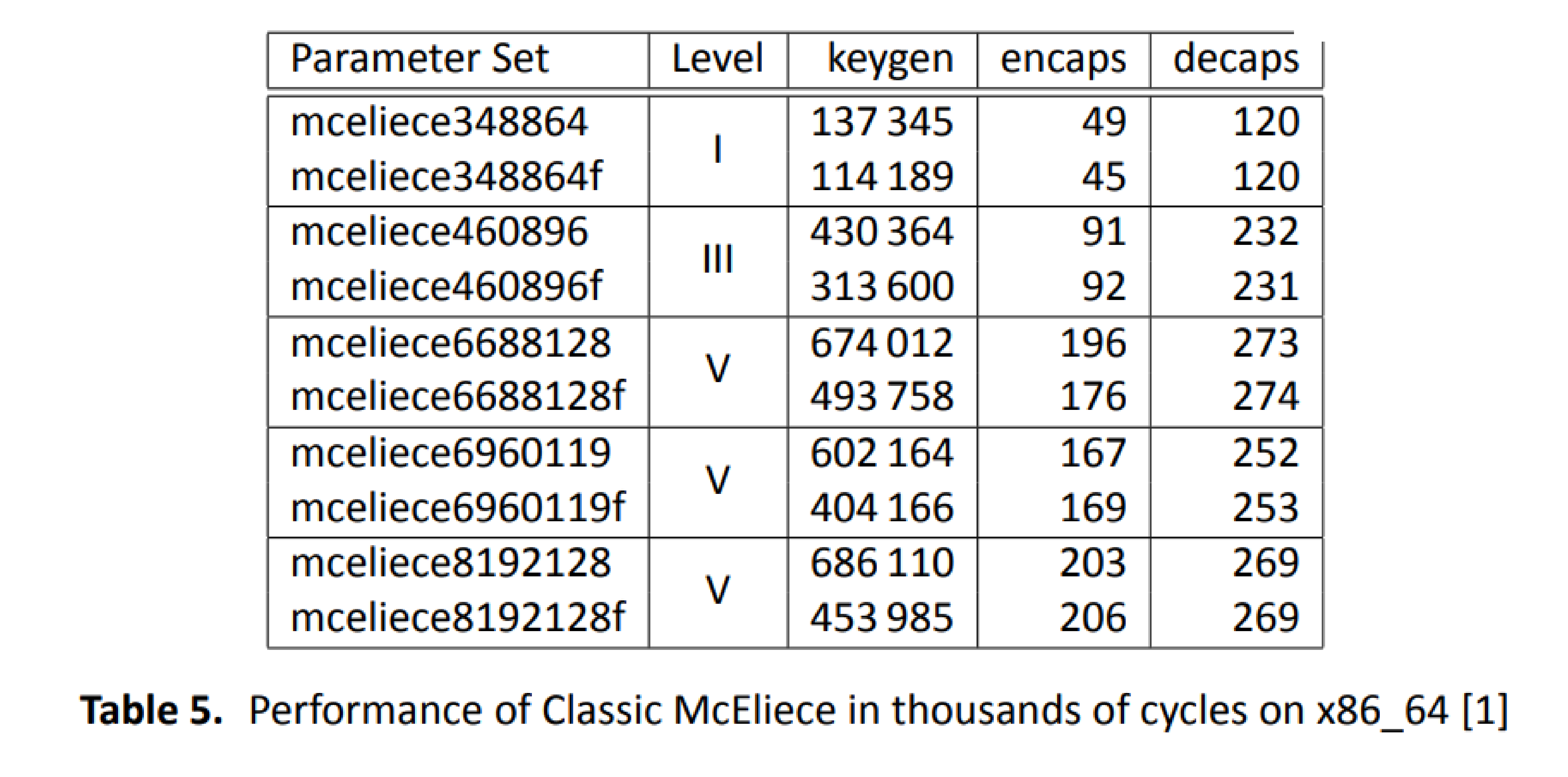
Parameter Set	Level	keygen	encaps	decaps
BIKE Level 1	I	637	111	1 428
BIKE Level 3	III	1 892	251	4 313
BIKE Level 5	V	4 535	505	10 382

Table 3. Performance of BIKE in thousands of cycles on x86_64 [1]



Parameter Set	Level	keygen	encaps	decaps
hqc-128	I	105	197	360
hqc-192	III	244	460	746
hqc-256	V	447	844	1 410

Table 4. Performance of HQC in thousands of cycles on x86_64 [1]



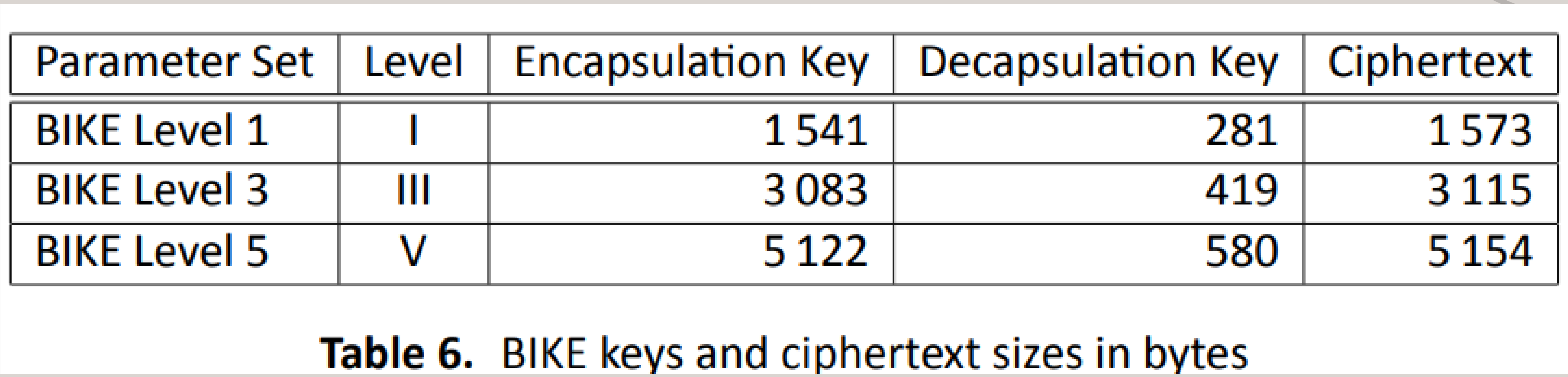
Parameter Set	Level	keygen	encaps	decaps
mceliece348864	I	137 345	49	120
mceliece348864f		114 189	45	120
mceliece460896	III	430 364	91	232
mceliece460896f		313 600	92	231
mceliece6688128	V	674 012	196	273
mceliece6688128f		493 758	176	274
mceliece6960119	V	602 164	167	252
mceliece6960119f		404 166	169	253
mceliece8192128	V	686 110	203	269
mceliece8192128f		453 985	206	269

Table 5. Performance of Classic McEliece in thousands of cycles on x86_64 [1]

Summary Of the Evaluation Process in the Fourth Round

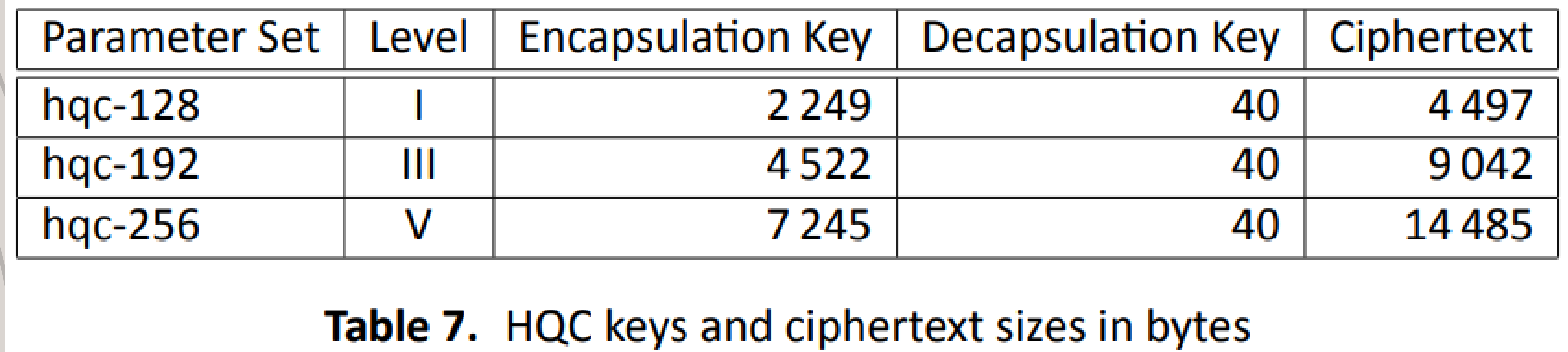
COST AND PERFORMANCE

- The encapsulation keys of HQC are about 41-47% larger than those of BIKE.
- The ciphertexts of HQC are about three times larger than BIKE.



Parameter Set	Level	Encapsulation Key	Decapsulation Key	Ciphertext
BIKE Level 1	I	1 541	281	1 573
BIKE Level 3	III	3 083	419	3 115
BIKE Level 5	V	5 122	580	5 154

Table 6. BIKE keys and ciphertext sizes in bytes



Parameter Set	Level	Encapsulation Key	Decapsulation Key	Ciphertext
hqc-128	I	2 249	40	4 497
hqc-192	III	4 522	40	9 042
hqc-256	V	7 245	40	14 485

Table 7. HQC keys and ciphertext sizes in bytes

Summary Of the Evaluation Process in the Fourth Round

COST AND PERFORMANCE

- Performance of Post-Quantum XML encryption and SAML SSO
  - For hybrid XML encryption, Classic McEliece slightly outperforms BIKE in decryption time and total time but with larger data sizes.
  - When used for SAML SSO, BIKE is generally faster than McEliece and produces much smaller bandwidths.
- Performance under certain condition of network
  - Generally when network conditions (transmission rates and packet loss) are ignored or good, HQC results in faster handshakes.
  - In contrasts under the opposite conditions, BIKE outperforms HQC.

Summary Of the Evaluation Process in the Fourth Round

SELECTION OF THE CANDIDATES FOR THE STANDARDIZATION

- SIKE
  - Was insecure thus removed.
- Classic McEliece
  - May provide better performance than BIKE or HQC for applications in which a public key can be transferred once and then used for several encapsulations due to its small ciphertext size and fast encapsulation and decapsulation. However, the interest in this algorithm was limited and having more standards to implement added complexity to the protocols and PQC migration.
- HQC
  - Lower decryption failure rate (DFR) as well as BIKE with minor modifications, but NIST does not consider BIKE's DFR analysis to be mature compared to HQC.
  - It is also not believed to require additional modifications to achieve the IND-CCA2 security thus it is selected for standardization.

Global Transition to PQC

Country	Key Initiatives	Year	Leading Organizations	Progress
United States	NIST PQC Standardization Process (Round 4)	2025	NIST	NIST selected HQC (Hamming Quasi-Cyclic) to be the only key-establishment algorithm
European Union	PQC migration roadmap	2024	NIS Cooperation Group (consists of EU Member States, European Commission and ENISA)	A dual roadmap (PQC-QKD) for quantum cybersecurity
China	Launched a global initiative to develop PQC algorithm that diverges from US	2024	China's Iwncomm	Proposed a draft quantum-proof communication encryption protocol

Global Transition to PQC

Country	Key Initiatives	Year	Leading Organizations	Progress
United Kingdom	National Quantum Strategy	2023	Department for Science, Innovation & Technology	Published a 10-year plan for the UK to be a world leading quantum-enabled economy by 2033.
Australia	Monitor PQC standardization efforts by NIST, monitor alternate methods of securing communications	2024	ASD, ACSC	Still in the planning stage
Canada	Quantum-Safe Canada Initiative	2017	The Governing Board, The Academic Steering Committee, the Advisory Council	Accepting the US NIST Post-Quantum Standardized Process, reinforcing the foundation and currently preparing for wide-scale deployment

MIGRASI PQC MALAYSIA

Akta dan garis panduan Malaysia

- **Akta Perlindungan Data Peribadi 2010 (PDPA)**: Akta ini mengawal pemprosesan data peribadi dan menekankan kepentingan melindungi data tersebut. Migrasi kepada PQC perlu memastikan pematuhan terhadap keperluan keselamatan data yang ditetapkan dalam PDPA.

- **Garis Panduan Keselamatan Siber**: Agensi Keselamatan Siber Malaysia (NACSA) dan Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) mungkin mengeluarkan garis panduan berkaitan keselamatan siber yang perlu diikuti semasa migrasi kepada PQC.

Merujuk kepada standard antarabangsa

- **Institut Piawaian dan Teknologi Kebangsaan (NIST)**: NIST sedang membangunkan standard untuk algoritma kriptografi pascakuantum. Organisasi di Malaysia boleh merujuk kepada standard ini untuk memastikan amalan terbaik diikuti.

Melibatkan Pakar keselamatan Siber

Mendapatkan khidmat nasihat daripada pakar keselamatan siber tempatan yang berpengalaman dalam PQC dapat membantu dalam memahami implikasi teknikal dan perundangan migrasi tersebut.

Latihan dan Peningkatan kesedaran

Mengadakan sesi latihan untuk kakitangan mengenai PQC dan kepentingannya dalam melindungi data daripada ancaman komputer kuantum.

Penilaian Risiko dan Audit Keselamatan

Melaksanakan penilaian risiko untuk mengenal pasti kelemahan dalam sistem semasa dan memastikan langkah-langkah mitigasi yang sesuai diambil semasa proses migrasi.