Considerations of using PQC in Telecommunication Networks

Junzhi YAN
China Mobile
yanjunzhi@chinamobile.com

Quantum Computing V.S. Classical Computing

- **Quantum computers** use the quantum mechanics to process information in quantum bits (qubits).

1 0

Classical bit is 0 and 1

$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \ \alpha^2 + \beta^2 = 1$

Quantum bit is superposition of 0 and 1

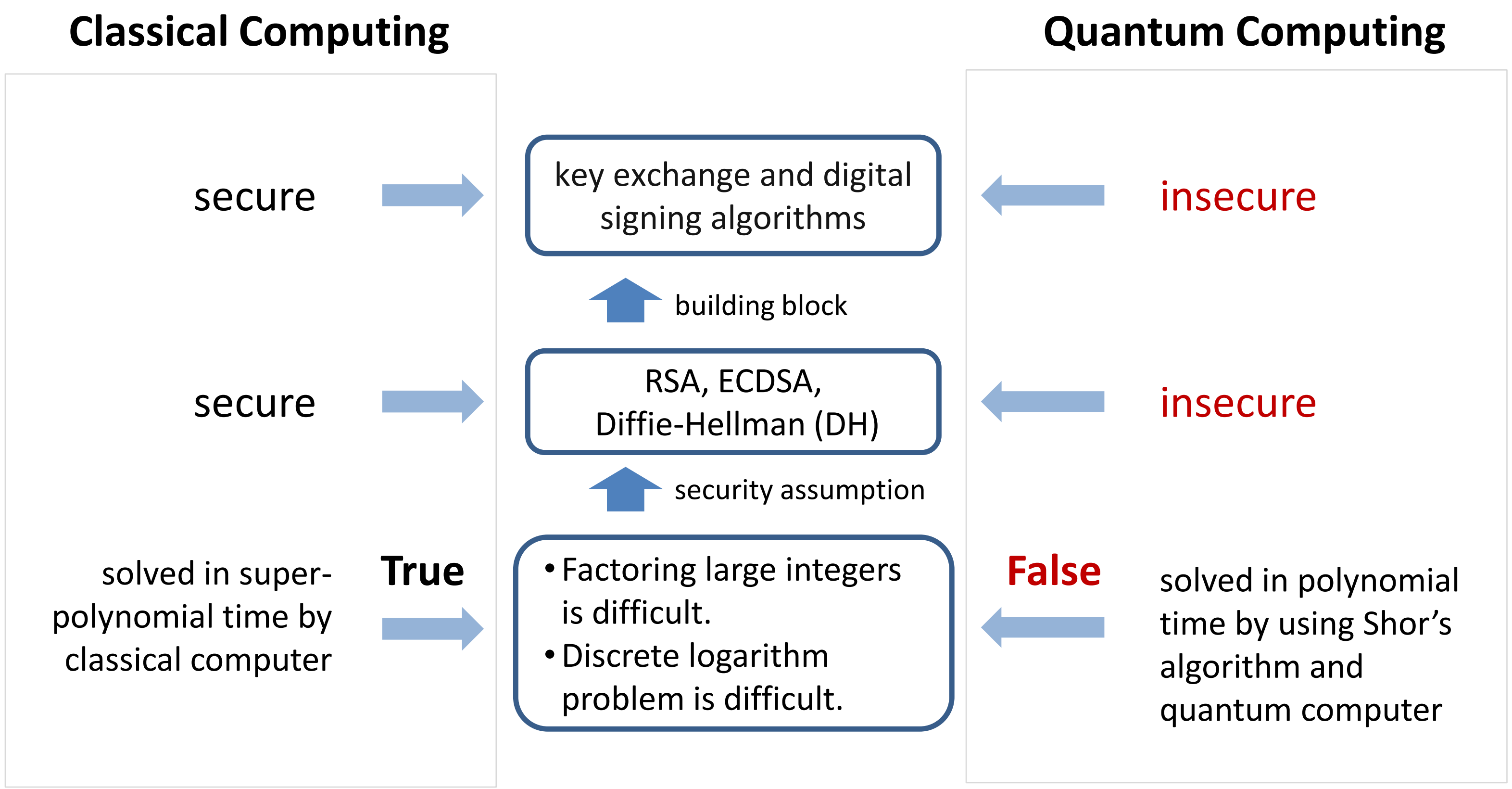
Classical bits can be either 0 or 1, while a qubit takes on a probability of being 1 or 0. For example,

- **2** qubits is superposition of **4** basis states (00,01,10,11)
- **3** qubits is superposition of **8** basis states (000,001,…,111)
- ***n*** qubits is superposition of $\mathbf{2^n}$ basis states

- Each qubit can be a combination of 0 and 1, a quantum computer can process variables exponentially faster than a classical, binary computer.

Quantum Computing V.S. Cryptographic Algorithms (1)

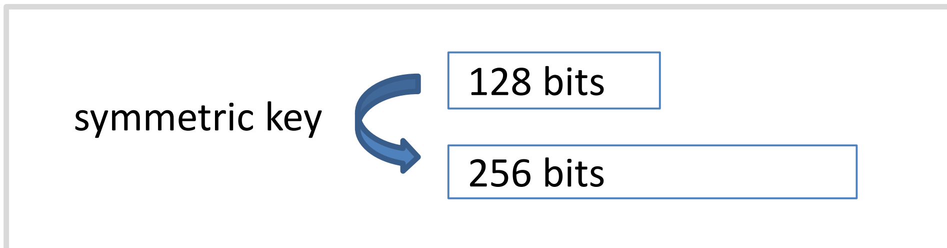
- **Shor's quantum algorithm** can solve integer factorization problem and discrete logarithm problem in polynomial time. It breaks the security assumption of widely used asymmetric cryptographic algorithms.



Quantum Computing V.S. Cryptographic Algorithms (2)

- **Grover's search algorithm** provides a quadratic speed-up to search in an unstructured data set over classic algorithms. This can be exploited to search the key in the key space of a symmetric key algorithm.

symmetric algorithm: double the key size



- **No known quantum algorithm** can find collisions in general hash algorithms more efficiently than classical algorithm.

hash algorithm: use secure algorithms under classical computing

NIST Post-Quantum Cryptography (PQC) Project

中国移动 China Mobile

Call for proposal
82 candidates
2016.12

1st round
69 candidates
2017.11

2nd round
26 candidates
2019.01

3rd round
15 candidates
2020.07

4 algorithms to be standardized
4 candidates advancing to the 4th round
2022.07

Post-quantum algorithm metrics

- **Security**
- **Cost and Performance**
  - public key, ciphertext, and signature size
  - computational efficiency of public and private key operations
  - computational efficiency of key generation
  - decryption failures
- **Algorithm and Implementation Characteristics**
  - flexibility
  - simplicity
  - adoption

- **Algorithms to be standardized**

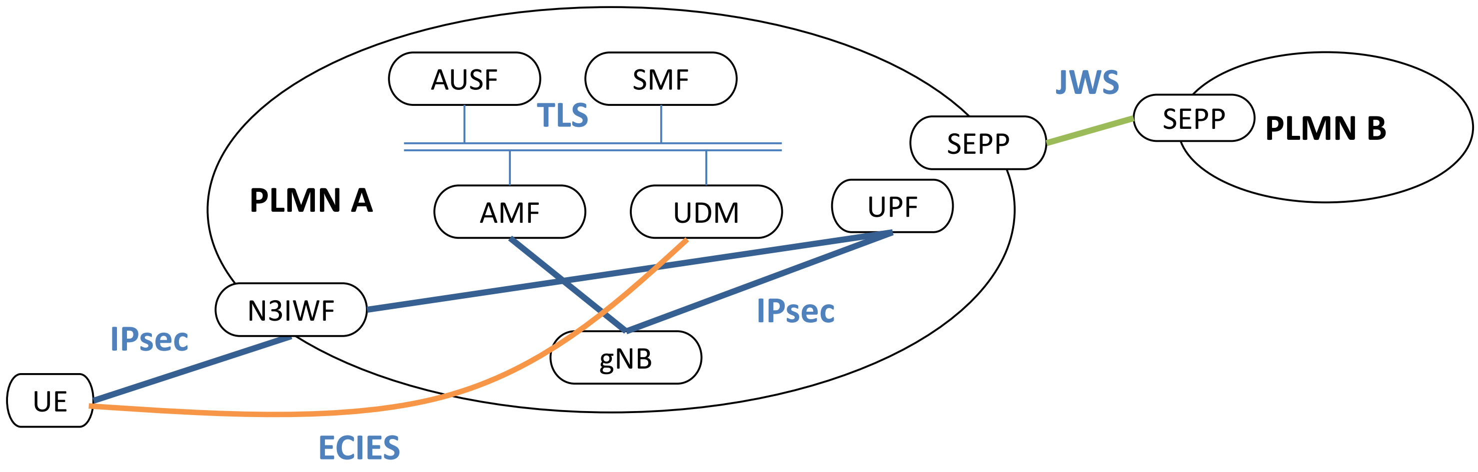
Public Key Encryption/KEMs	**Digital Signatures**
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

- **Candidates advancing to the 4th round**

Public Key Encryption/KEMs	**Digital Signatures**
BIKE	
Classic McEliece	
HQC	
SIKE*	

*SIKE was compromised in August 2022, refer to “an efficient key recovery attack on SIDH” and “an attack on SIDH with arbitrary curve”

Asymmetric algorithms in IMT-2020 network



	Protocols	Asymmetric algorithms
Infrastructure layer	TLS, IPsec	RSA, ECDSA, DH, ECDH
Network layer	ECIES, IPsec, IKEv2, TLS, JWS	RSA, ECDSA, DH, ECDH
Service layer	TLS	RSA, ECDSA, DH, ECDH
Management plane	TLS	RSA, ECDSA, DH, ECDH

Considerations of the transition of PQC (1)

1 Security

- **Inventory of critical data**
  - Identify the critical data or system which use classical may be affected by quantum computing
- **To what extent can the data using classical ciphers be affected**
  - The data and system using secure classical ciphers is secure today. However,
  - eavesdroppers may begun recording encrypted connections, the data in the connection may be stored and decrypted in the future.
- **Implementation of PQC**
  - Implementation related security in the telecommunication infrastructure

Considerations of the transition of PQC (2)

China Mobile

2 Performance

- **Throughput of the network (ex. access network)**
  - Key size of PQC is much bigger than classical ciphers, if affects the speed of data transmission
  - The maximum throughput at the access network when a large amount of subscribers access the network
  - computing and communication resource needed for the algorithm at the user's side
- **delays of the data transmission**
  - increased delay may affect user's experience

Candidate	Claimed Security	Public key	Private key	Ciphertext
KYBER512	Level 1	800	1 632	768
KYBER768	Level 3	1 184	2 400	1 088
KYBER1024	Level 5	1 568	3 168	1 568

Key and ciphertext sizes (in bytes)

Candidate	Claimed Security	Public key	Private key	Signature
Dilithium	Level 2	1 312	2 528	2 420
	Level 3	1 952	4 000	3 293
	Level 5	2 592	4 864	4 595
FALCON-512	Level 1	897	7 553	666
FALCON-1024	Level 5	1 793	13 953	1 280
SPHINCS$^+$-128s	Level 1	32	64	7856
SPHINCS$^+$-128f	Level 1	32	64	17 088
SPHINCS$^+$-192s	Level 3	48	96	16 224
SPHINCS$^+$-192f	Level 3	48	96	35 664
SPHINCS$^+$-256s	Level 5	64	128	29 792
SPHINCS$^+$-256f	Level 5	64	128	49 856

Key and signature sizes (in bytes)

----- adapted from NIST's report

As a reference, RSA-2048 uses keys and ciphertexts /signatures of size 256B, those of Curve25519 and Ed25519 are as small as 32B.

Considerations of the transition of PQC (3)

3 Flexibility

- **Implementation in constrained environment**
  - Can be implemented on a wide variety of platforms, including constrained environments
- **Compatibility**
  - Can be incorporated into existing protocols and applications
- **Replaceable**
  - Can be replaced once there is weakness

4 Interoperability

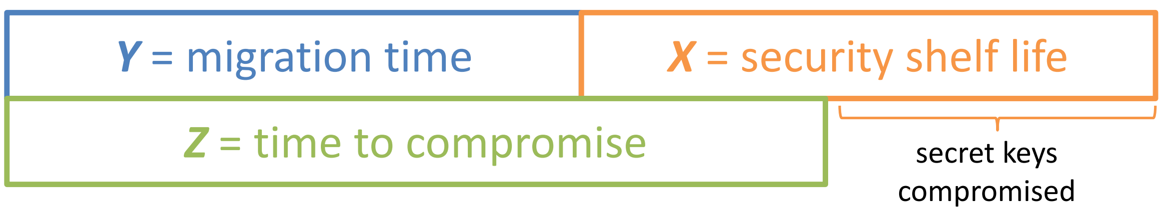
- **Multiple algorithms and cipher suite negotiation are needed**
  - Systems or networks may have different capabilities and support different algorithms

Considerations of the transition of PQC (4)

5 Cost

- **CAPEX and OPEX**
  - The costs associated with adopting post-quantum algorithms in the infrastructure.

6 When to begin migration



$$X + Y > Z$$

"We need to start worrying about the impact of quantum computers when the amount of time that we wish our data to be secure for (X) is added to the time it will take for our computer systems to transition from classical to post-quantum (Y) is greater than the time it will take for quantum computers to start breaking existing quantum-susceptible encryption protocols."

----- Mosca's theorem

中国移动
China Mobile

Thank you!