LG U+

GROWTH LEADING AX COMPANY

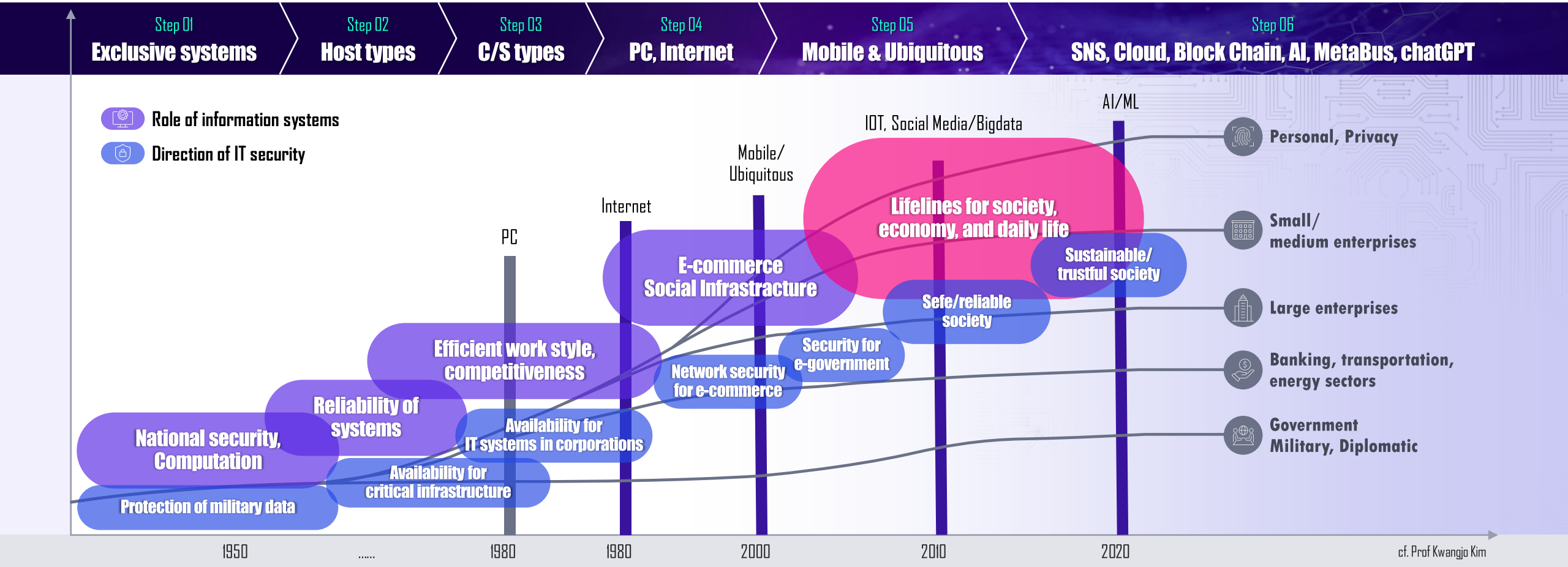
PQC Technology

2024. 06.

Jaehwan Jin

01 Overview

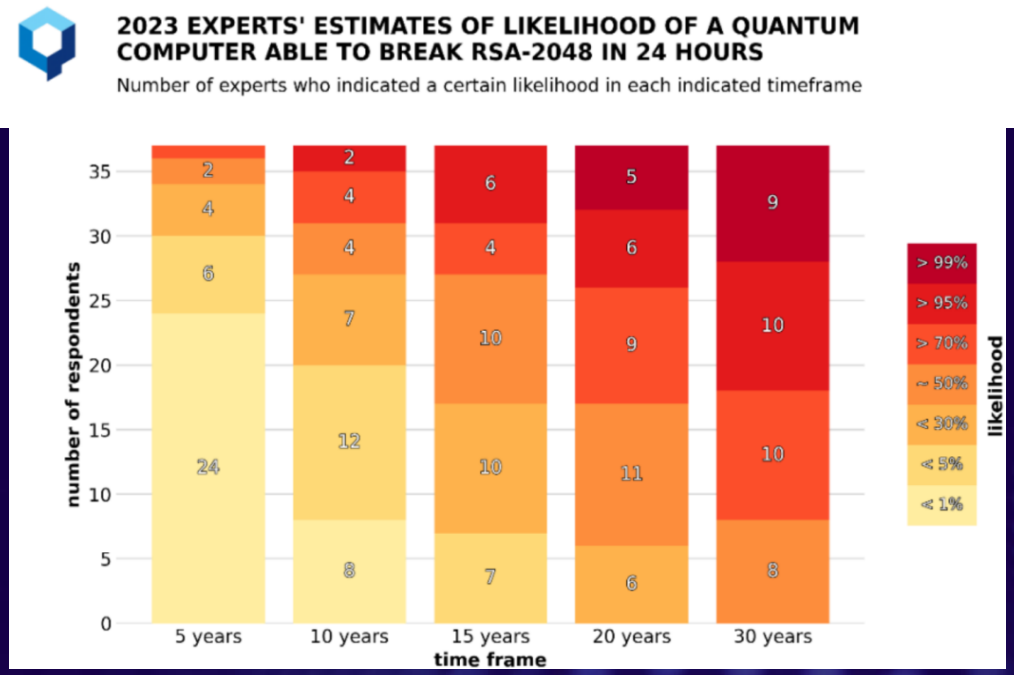
Modern cryptography has evolved into more complex and secure algorithms with the advancement of computers, evolving from restricted systems to personalized services.

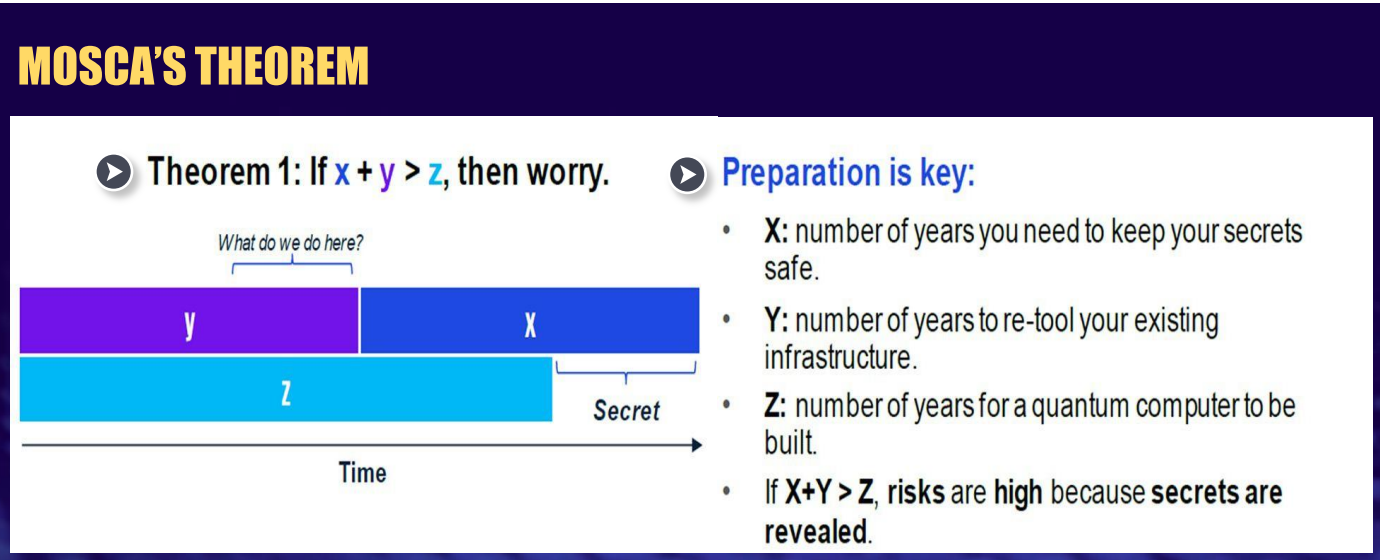


Quantum Computer is coming. necessitating a migration to quantum cryptography.

- Peter Shor's Algorithm(1994) > a quantum algorithm for efficiently factorizing large numbers.
- Lov Grover's Algorithm(1996) > a quantum algorithm for searching unsorted database.

Mosca's Theorem suggests the timeframe required to protect data. Dr. Michele Mosca's theorem stresses the need for organizations to begin applying diligence in the post-quantum space right away.

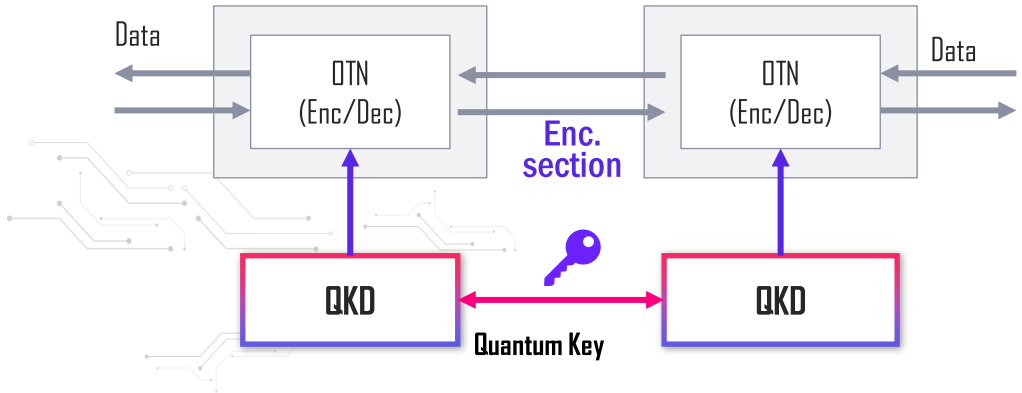




01 Overview

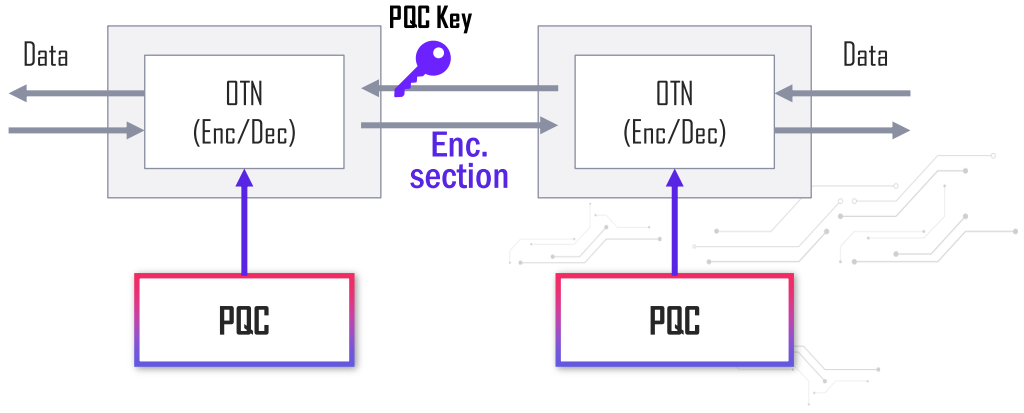
QKD and PQC are technologies that are designed to counter quantum computers.
QKD has physical limitations when providing services, while PQC does not.

Quantum Key Distribution (QKD)



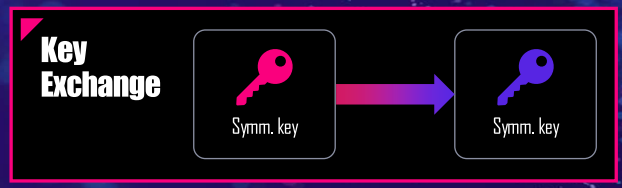
- ✓ Key distribution using quantum properties
- ✓ Additional optical path for QKD
- ✓ Limit on key transport distance using QKD

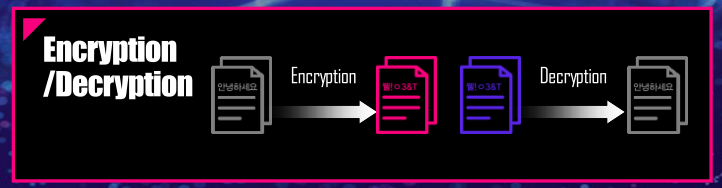
Post Quantum Cryptography (PQC)



- ✓ Based on quantum-resistant math problems
- ✓ No additional setup for key distribution
- ✓ No limit to the transport distance

Three factors of Cryptography

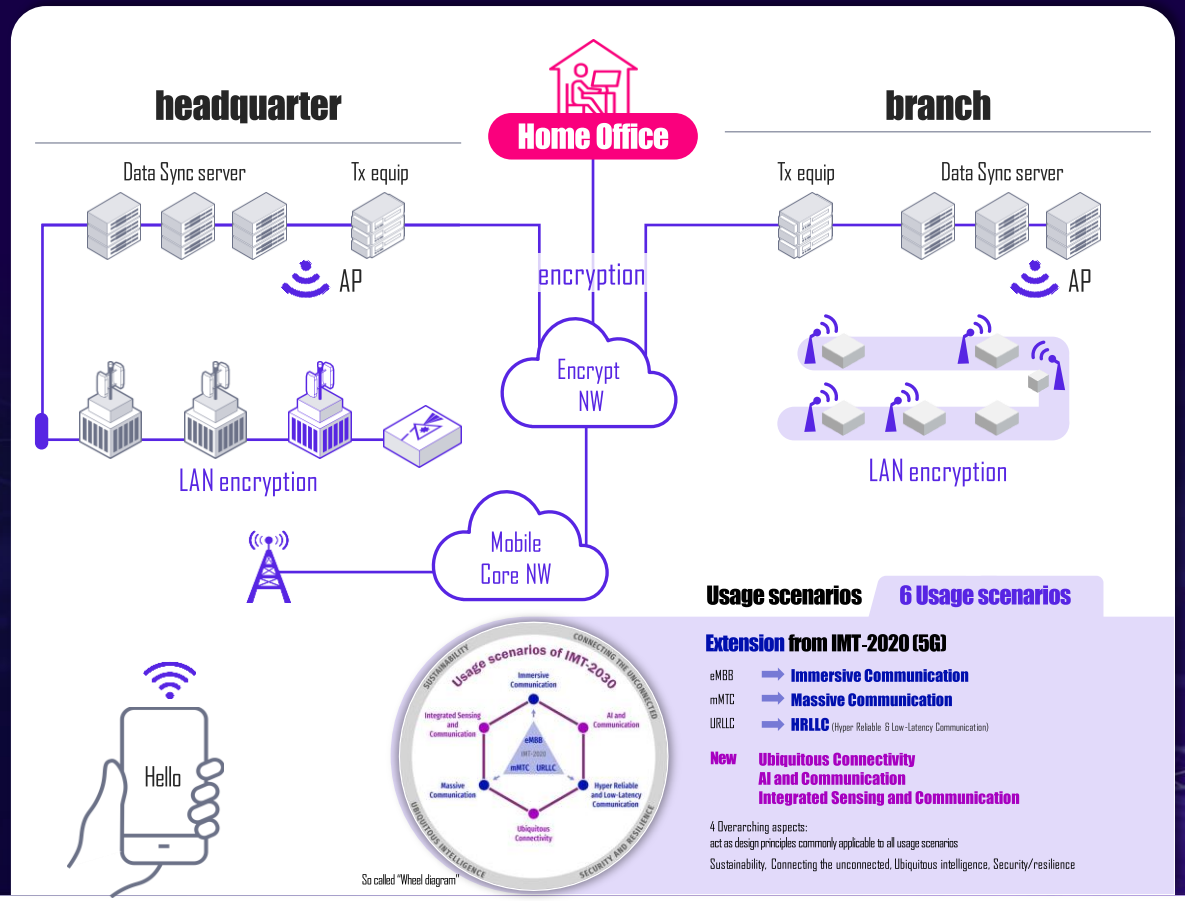


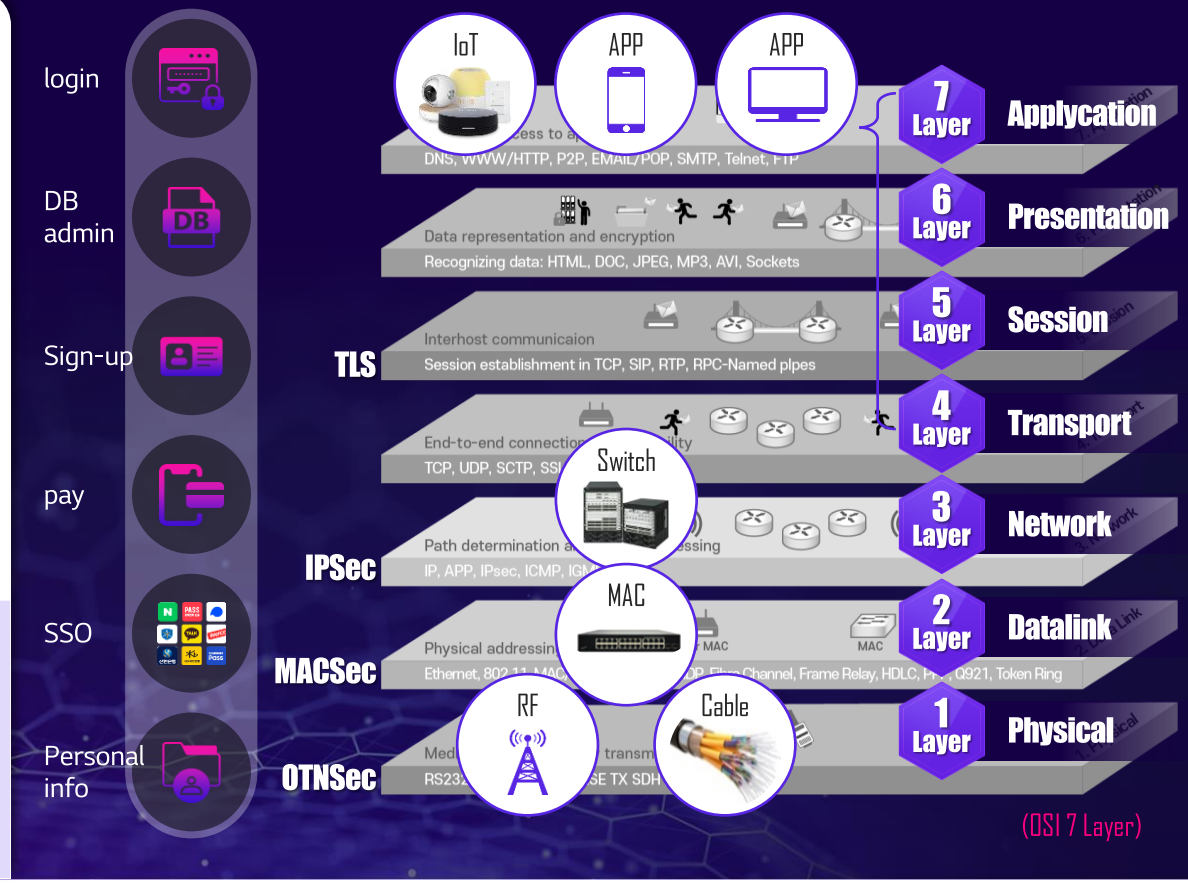


02 Network Requirement for Cryptography

Need for Cryptography Techniques that can securely transmit data against quantum threats

in various environments such as wired, wireless, Datacenter etc. OTN(Optical Transport Network), Internet and application in OSI-7 Layer.





03 Progress in PQC

NIST initiated the PQC Standardization Project in 2016

- CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, SPHINCS+ in Round 3, continuing for additional PQC algorithms in Round 4.

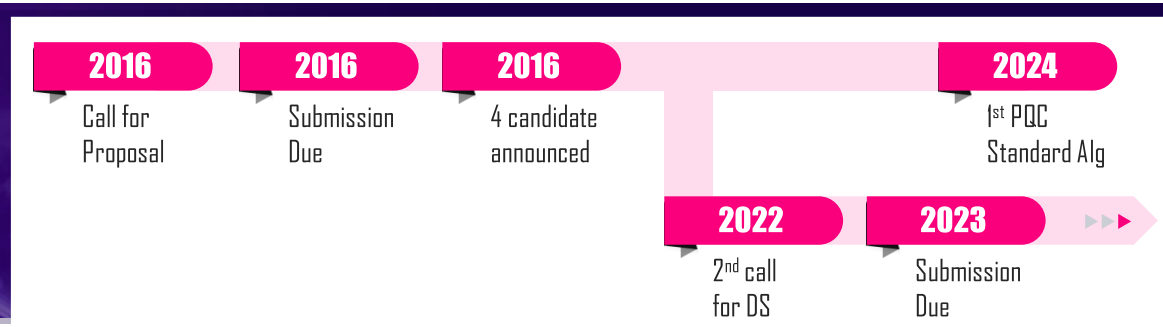
The Korea Post-Quantum Cryptography(KpqC) Competition was launched in 2021

- 4 KEM, 4 DS in Round 2

NIST PQC Competition

- In 2020, Round3 Candidates announced – 7 Finalists, 8 Alternates
- In 2022, 1 KEM and 3 DS announced for Standardization

https://csrc.nist.gov/projects/post-quantum-cryptography



Korea PQC Competition

- In 2023, Round 1 Candidates announced – 4 KEM, 4 DS

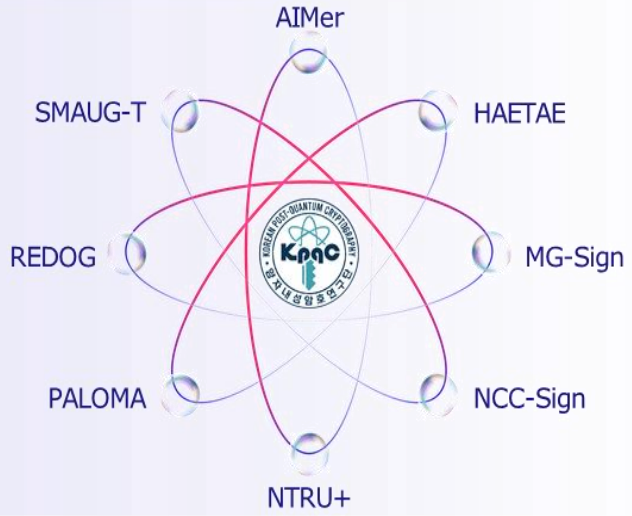
https://kpqc.or.kr/

Round1 Submission
Oct. 2022

Round1 Result
Dec. 2023

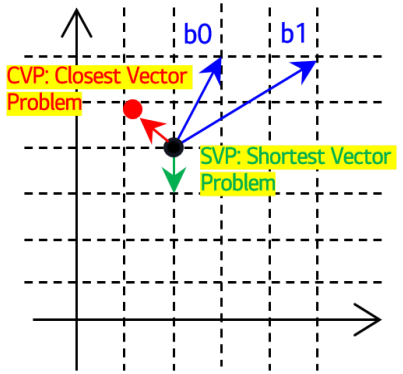
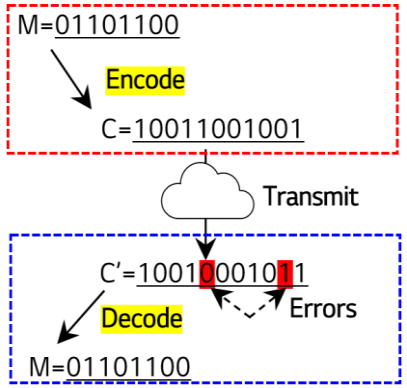
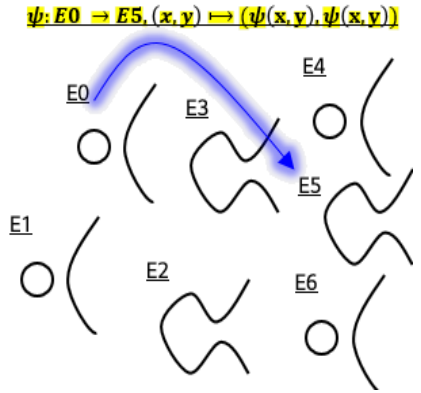
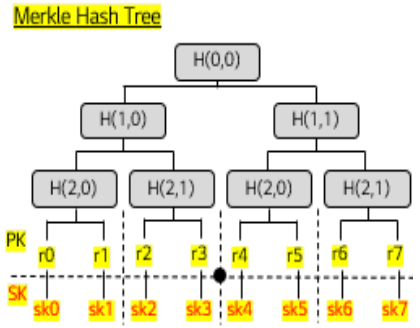
Round2 Submission
Feb. 2024

Round2 Result
Nov. 2024



03 Progress in PQC

NIST considered proposals for algorithms based on various mathematical problems but selected only lattice-based and hash-based algorithms, exploring new types of algorithms.

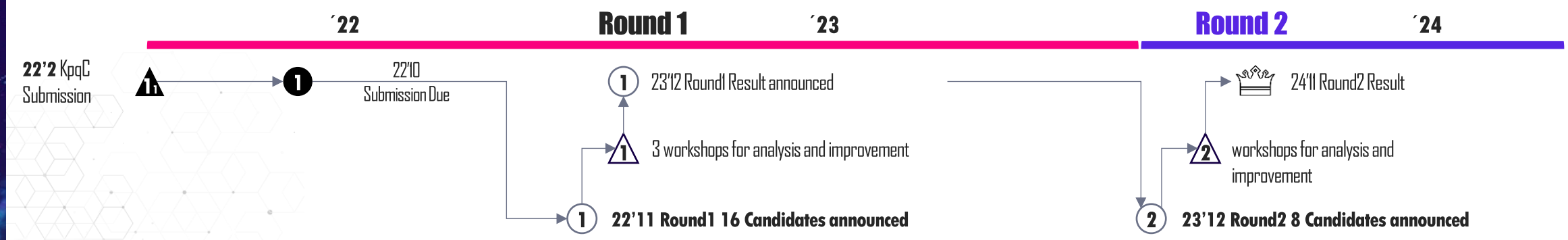
Lattice-based	Code-based	Isogeny-based	Hash-based	Multivariate-based
				[Multivariate Quadratic Problem] $p^{(1)}(x_1, \cdots, x_n)$ $p^{(2)}(x_1, \cdots, x_n)$ $\vdots$ $p^{(m)}(x_1, \cdots, x_n)$
Based on hard problems like SVP, CVP, LWE, LWR (NP-hard)	Inject errors into messages. allowing only users who know the error to recover the message	Based on problem of finding isogenies between two elliptic curves	Digital Signature based on hash function security, uniquely proven to be secure	Digital Signature based on MQ problem and extended isomorphism problem
CRYSTALS-KYBER	BIKE, Classic McEliece, HQC			
CRYSTALS-DILITHIUM, FALCON			**SPHINCS+**	

03 Progress in PQC

In the KPQC competition round 2, lattice-based algorithms, code-based algorithms, multivariate-based algorithms, and zero-knowledge proof(ZKP)-based algorithms **are competing candidates.**

Korea PQC Competition(`22.2~`24.11)

Security | Efficiency | Usability



KEM (key-encapsulation mechanism)

	Based-problem	Algorithms
PKE/KEM	Lattice	**NTRU+**
	Code	**REDOG**
	Graph	IPCC
	Lattice	**SMAUG-T(SMAUG + TiGER)**
	Code	Layered ROLLO-I
	Code	**PALOMA**

DS (Digital Signature)

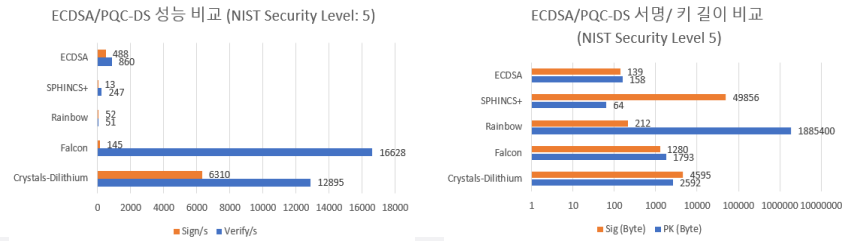
	Based-problem	Algorithms
PKE/KEM	Lattice	GCKSign, **HAETAE, NCC-Sign,** Peregrine, SOLMAE SOLMAE
	Multivariate	**MQ-Sign**
	Isogeny	FIBS
	Code	Enhanced pqsigRM
	ZKP	**AIMER**

03 Progress in PQC

We are optimizing PQC algorithms to ensure that they function without performance degradation in diverse communication environments**, working to obtain** cryptographic certifications of PQC.

Performance – Speed / Memory

- High memory requirements
- Implementation Difficulties in constrained environments



[Performance Comparison: Classical PKE vs PQC]

Implementation Environment

- Packets over 1500 bytes
- Reliable data transmission

[UDP –based Protocol eg. IPSec VPN]

Standardization – CMVP, X.509 ...

- CMVP(Korea Cryptographic Module Validation Program) for PQC.
- PQC Standard Specifications for certificates(X.509) in key exchange and signatures

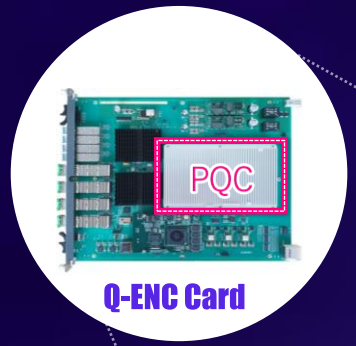
KCMVP-validated cryptographic algorithms

Block Cipher: LEA, HIGHT, SEED, ARIA
MAC: GMAC, CMAC, HMAC
PKC: RSAES
Key Exchange: DH, ECDH
Hash: SHA2, SHA3, LSH
RNG: CTR_DRBG, HASH_DRBG,
DS: RSA-PSS, ECDSA, KCDSA,
EC-KCDSA

04 PQC Development for OTN equipment

PQC KEM was applied to ROADM(OTN) in 2020.

In a national project, PQC was applied as a hybrid approach combining PQC and classical PKE algorithms.

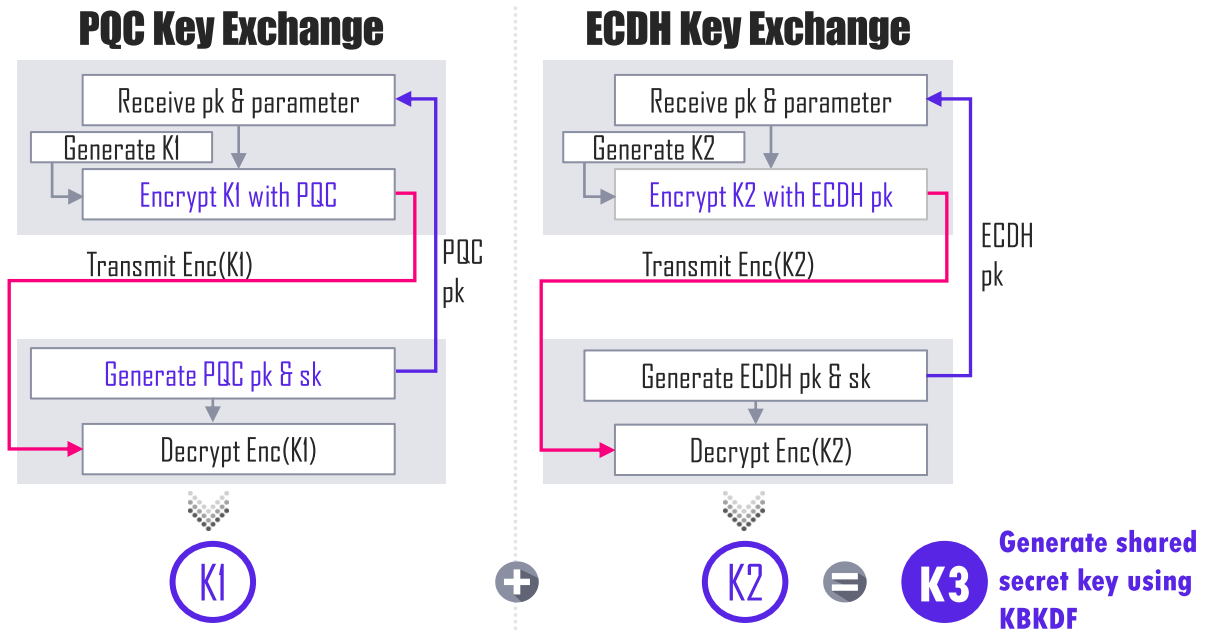


Q-ENC Card

Q-ROADM

- 1G/10G, 100G OTN/Ethernet interface
- 3.2/16Tera(16/88ch OADM@200G) Add/Drop Capacity
- Colorless, Directionless, Flexible Grid

PQC Implementation(Hybrid)

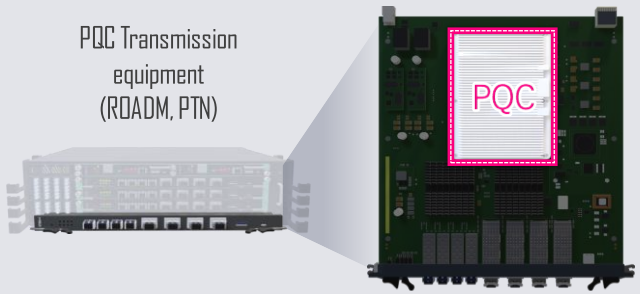


05 Expansion of PQC Development

Expanding PQC application fields to PTN(Packet Transport Network), wired/wireless routers, and IoT device

Transmission Equipment

- Encryption: **block cipher**(ARIA)
- PQC **algorithms**: KEM, DS (Digital Signature)
- PUF chip: **Embedded authentication module chips**



Wired/Wireless LTE Routers

- NIST PQC algorithms (CRYSTALS-KYBER, CRYSTALS-DILITHIUM)
- PUF chip

IoT Device Authentication(PUF-eSIM)

- PUF chip
- PQC algorithm (CRYSTALS-KYBER, CRYSTALS-DILITHIUM)
- eSIM chip

PUF-eSIM(KTC Certified)

Mitigating Side-Channel Attack (e.g. DPA, SPA)

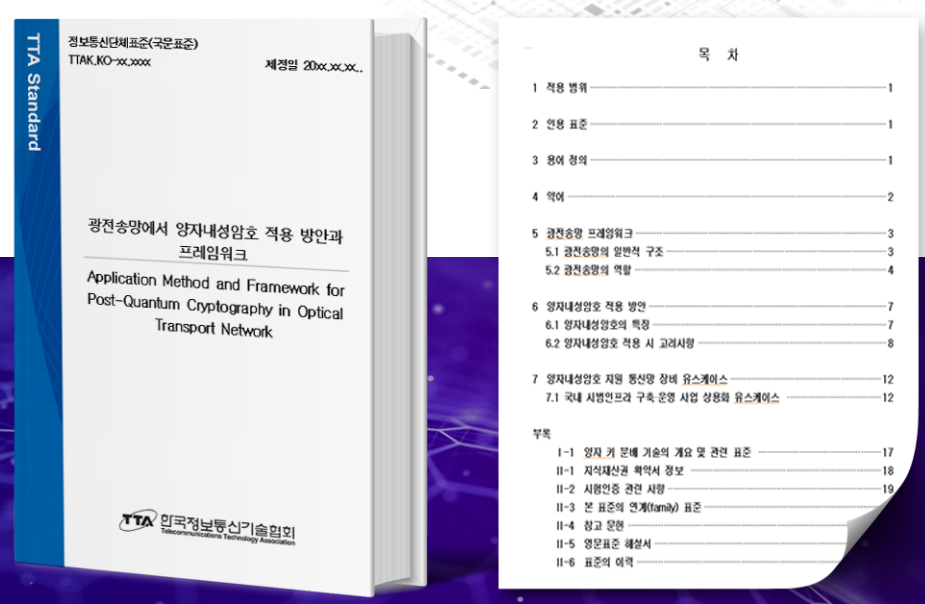
PQC Application Cases – TTA Standard

Application Method and Framework for PQC in Optical Transport Network.
including PQC-applied use cases implemented as a part of the national project.

Scope

This standard outlines guidelines and use cases for implementing network services based on post-quantum cryptography. It aims to assist companies and organizations seeking to establish PQC supported network equipment by providing necessary information and application use cases, for building PQC-supported network efficiently.
The scope of this standard includes:

- **Optical Transport Network Framework**
- **Considerations for Implementing PQC in OTN**
- **Use Cases for PQC-supported network equipment**



07 National Plan for Transition to PQC

The South Korean government has been actively promoting quantum cryptography technology through a national project since 2020. LG U+ launched the PQC leased line service in April 2022.

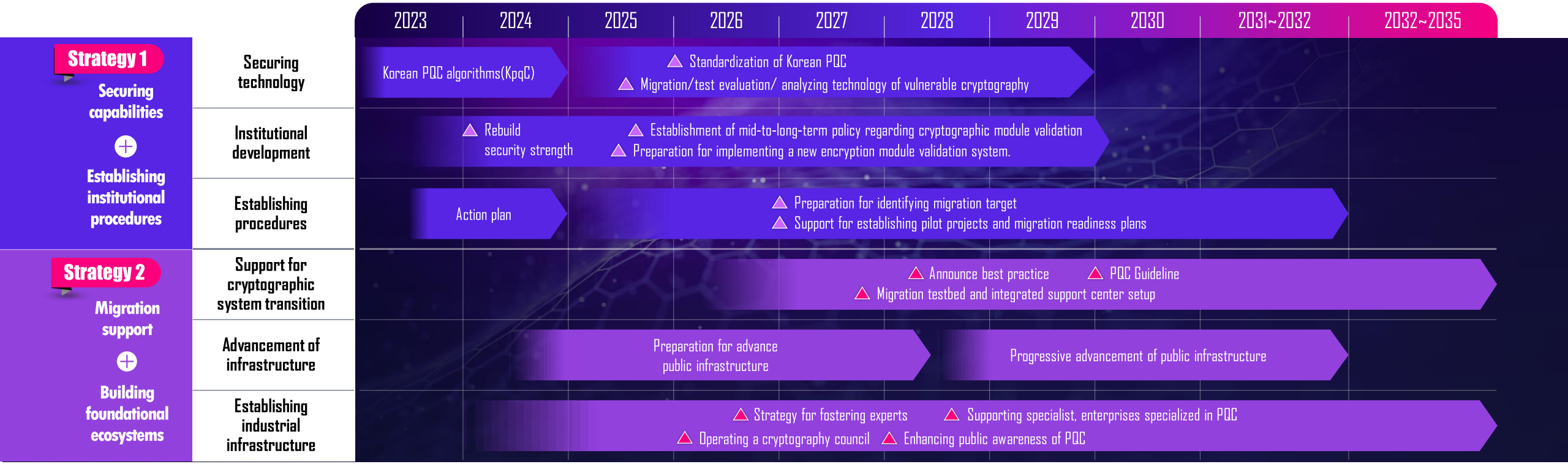
Let's join the national PQC plan to drive the migration to PQC.

2020~2022 — Quantum Cryptographic Communication Pilot Infrastructure

2023.7.12 — Comprehensive Plan Announcement for full Migration of the national cryptographic system to PQC

2023, NIS — Security Verification for adopting PQC equipment in national and public institutions

2024~2025 — National Project for build and operation of open quantum testbed



LG U+

Thank you

GROWTH LEADING AX COMPANY