2026. 09. 14

KIST Quantum Technology :

Quantum Key Distribution toward Scalable Quantum Communication Networks and Photonic Integrated Systems

Director, Quantum Application Technology Hub in KIST
Principal Researcher at Center for Quantum Technology in KIST
Professor at KU-KIST

Sang-Wook Han

Korea Institute of Science and Technology

I

Security Technologies Resilient to Quantum Threats

From Conventional Public-Key Security to Quantum-Safe Alternatives

Conventional Security Systems

000111001**0??1??1?1**

Eavesdropping
or tempering

Quantum Threat

Quantum-Safe Alternative

01 Quantum Key Distribution (QKD)

Security based on
the physical laws of
quantum mechanics

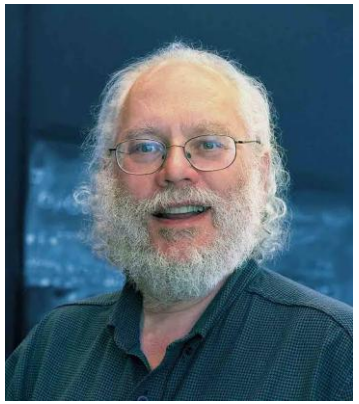
02 Post-Quantum Cryptography (PQC)

Security based on
computational hard
Mathematical problems

"Quantum Computing" advancements pose a critical threat to existing public-key security systems

I Shor's Algorithm

A Quantum Threat to Modern Public-Key Cryptography



[Peter Shore]

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1484–1509, October 1997

009

POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER*

PETER W. SHOR†

FOUNDATIONS OF WIDELY USED PUBLICK-KEY CRYPTOGRAPHY

RSA	DL	ECC
Integer factorization	Discrete logarithm	Elliptic-curve discrete logarithm

Shor's algorithm threatens widely used public-key cryptography
by efficiently solving factorization and discrete logarithm problems.

I

Is It Time for Alternative Technologies?

Threat Timeline

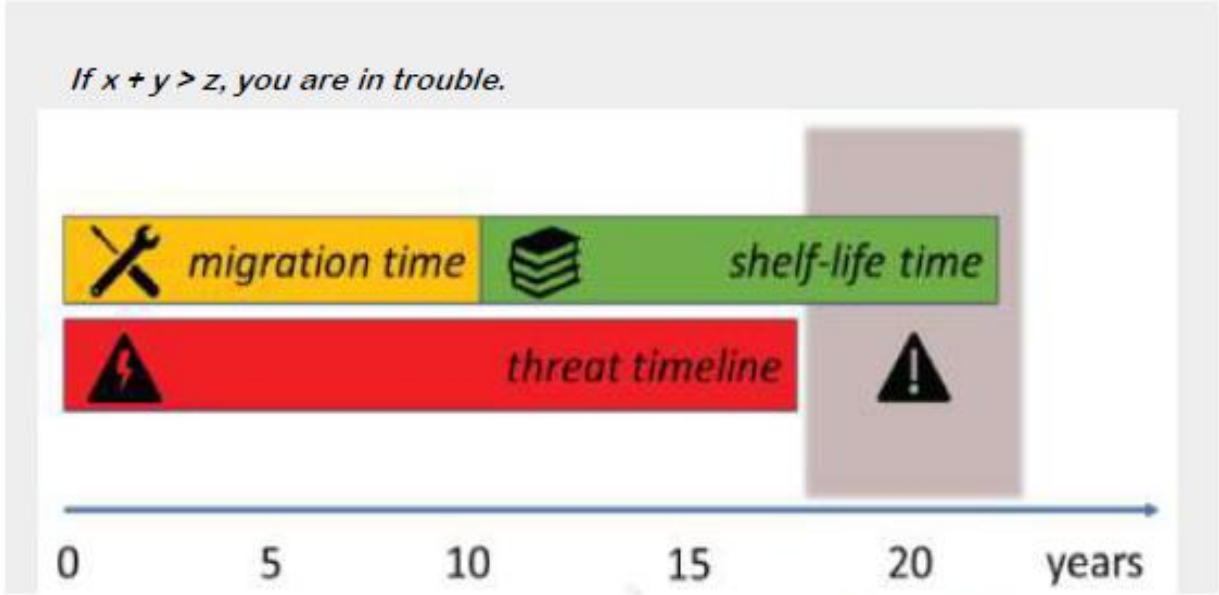
When cryptographic relevant quantum computer (CRQC) is available?

Shelf-life Time

How long data should remain protected?

Migration Time

How long does it take to migrate to PQC?



+ source: Dr. Mosca (Global Risk Institute)

The growing quantum computing threat and long migration timelines make early preparation for quantum-safe security essential.

I

Is the Quantum Threat Becoming Reality?

A 10,000-Qubit Estimate Changes the Timeline

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain[1,*,†], Qian Xu[1,2,*,‡], Robbie King[1], Lewis R. B. Picard[1], Harry Levine[1,3], Manuel Endres[1,2], John Preskill[1,2], Hsin-Yuan Huang[1,2], Dolev Bluvstein[1,2,§]
[1] *Oratomic, Pasadena, California 91125, USA*
[2] *California Institute of Technology, Pasadena, California 91125, USA*
[3] *Department of Physics, University of California, Berkeley, California 94720, USA*
[†] *mcain@oratomic.com,* [‡] *qxu@oratomic.com,* [§] *dbluvstein@oratomic.com*
[*] *These authors contributed equally*
(Dated: March 31, 2026)

Quantum computers have the potential to perform computational tasks beyond the reach of classical machines. A prominent example is Shor's algorithm for integer factorization and discrete logarithms, which is of both fundamental importance and practical relevance to cryptography. However, due to the high overhead of quantum error correction, optimized resource estimates for cryptographically relevant instances of Shor's algorithm require millions of physical qubits. Here, by leveraging advances in high-rate quantum error-correcting codes, efficient logical instruction sets, and circuit design, we show that Shor's algorithm can be executed at cryptographically relevant scales with as few as 10,000 reconfigurable atomic qubits. Increasing the number of physical qubits improves time efficiency by enabling greater parallelism; under plausible assumptions, the runtime for discrete logarithms on the P-256 elliptic curve could be just a few days for a system with 26,000 physical qubits, while the runtime for factoring RSA–2048 integers is one to two orders of magnitude longer. Recent neutral-atom experiments have demonstrated universal fault-tolerant operations below the error-correction threshold, computation on arrays of hundreds of qubits, and trapping arrays with more than 6,000 highly coherent qubits. Although substantial engineering challenges remain, our theoretical analysis indicates that an appropriately designed neutral-atom architecture could support quantum computation at cryptographically relevant scales. More broadly, these results highlight the capability of neutral atoms for fault-tolerant quantum computing with wide-ranging scientific and technological applications.

RESOURCE ESTIMATE

10,000

reconfigurable atomic qubits

Shor's algorithm targets RSA-2048.
Recent estimates suggest that fewer qubits may be needed than previously expected.

Cryptographically relevant quantum computing may require far fewer qubits than previously estimated.

arXiv:2603.28627v1[quant-ph]

I

PQC vs. QKD: Two Paths to Quantum-Safe Security

Trade-Offs in Security, Scalability, Infrastructure, and Cost

Post-Quantum Cryptography (PQC)

- Pros
  - Existing Infrastructure: Deployable over conventional networks
  - Scalability: Scales efficiently across large networks
  - Cost Efficiency: Requires minimal additional hardware
- Cons
  - Assumption-based Security: Relies on the hardness of mathematical problems
  - Performance Overhead: More computationally demanding than symmetric cryptography

Quantum Key Distribution (QKD)

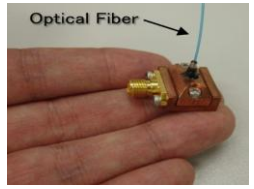
- Pros
  - Information-Theoretic Security: Secure under defined theoretical and implementation assumptions
- Cons
  - Distance Limitations: Point-to-Point fiber links are constrained by channel loss
  - Specialized Infrastructures: Requires dedicated optical hardware and network integration
  - Environmental Sensitivity: Performance depends on loss, stability, weather, and alignment

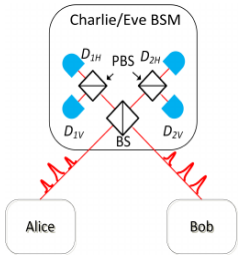
Need to explore QKD-PQC Hybrid Technology Development

I

Major Technology Areas of Quantum Cryptography

Need to Develop Core Technologies for Full-Scale Commercialization





System Advancement

Networking

Long-Distance Transmission

Commercial Services

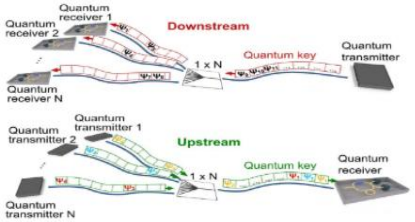
Quantum Cryptography

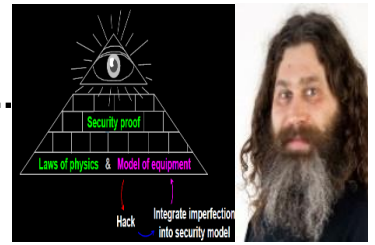
Security & Anti-Hacking

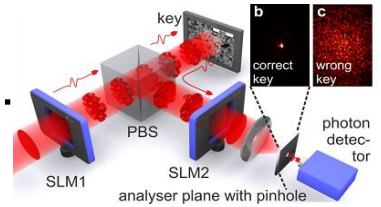
Standards Development

Protocols

Quantum Authentication & Signatures







I

Engineering Challenges in QKD Deployment

WHY THIS MATTERS

"QKD is mature—but deployment still faces three engineering barriers"

01

Network Scalability

Connect many users without multiplying expensive sources and detectors.

MORE USERS

02

System Miniaturization

Integrate active and passive optical functions on compact, reproducible chips.

SMALLER HARDWARE

03

Long-Distance Reach

Extend secure links beyond the repeaterless scaling of conventional QKD.

LONGER LINKS

Address system-level challenges beyond protocol design.

II

KIST's QKD System Innovation: Three Milestones

RESEARCH TRAJECTORY

2020

1 × N field network

WDM + PDM + Sub-ns Timing Control

SCALABILITY

2025

Monolithic TFLN QKD

Identical Tx/Rx Chips over Deployed Fiber

INTEGRATION

NEXT

Integrated TF-QKD

Phase Estimation + Pure Phase-Error Analysis

DISTANCE

One continuous goal: practical, scalable quantum communication infrastructure

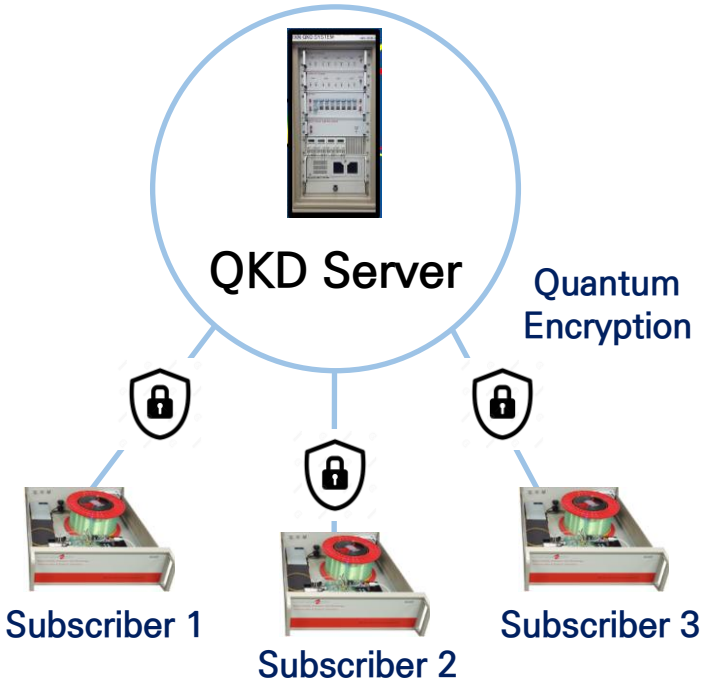
II

Quantum Cryptography Network System: 2014 ~ 2019

- 1xN Quantum Cryptography Network System Technology
  - Connects a single server to multiple subscribers rather than simply expanding 1x1 systems
  - Compact and cost-effective multi-subscriber network deployment

[Application Fields]

- Data Centers
- Military Secure Communications
- Central Control Centers



WDM × PDM × TDM Technology

Subscriber-Independent System Control Technology

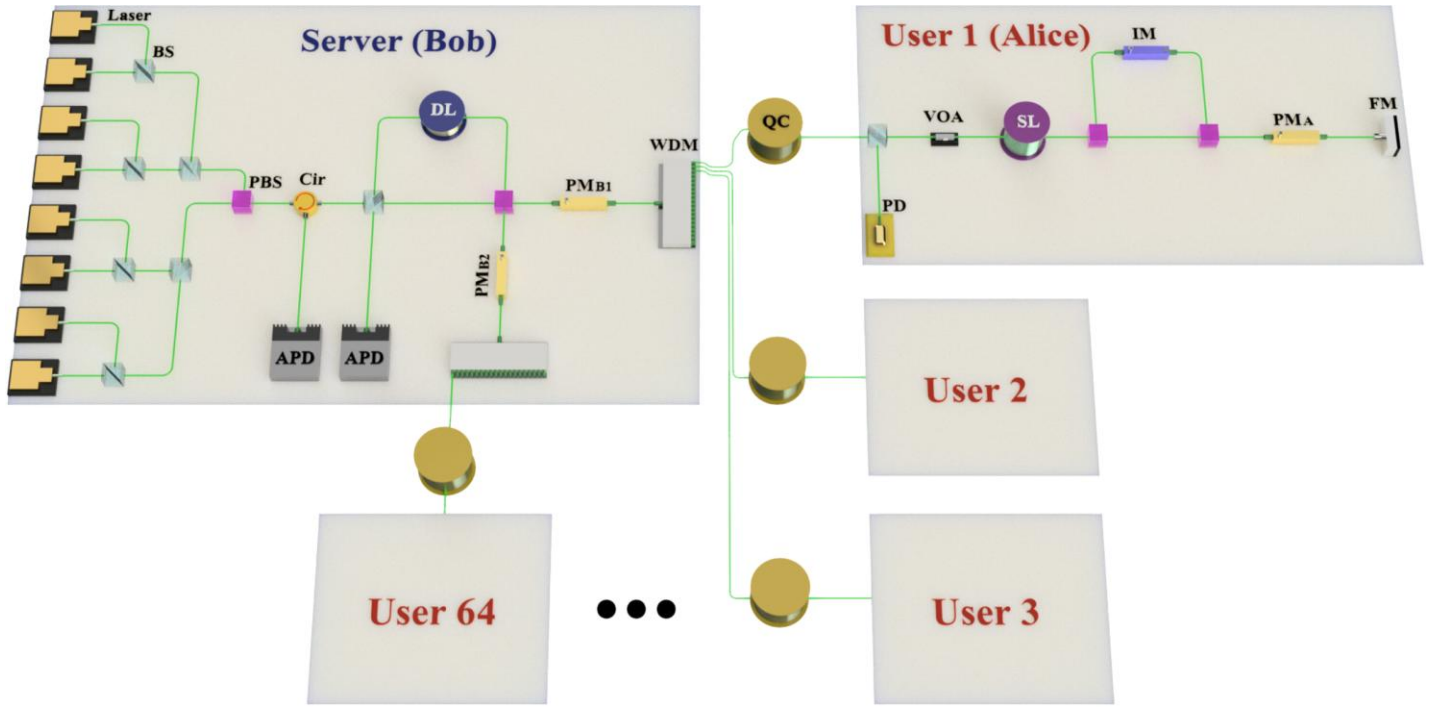
Decoy Protocol Implementation Technology

- Min Ki Woo, Byung Kwon Park, Yong-Su Kim, Young-Wook Cho, Hojoong Jung, Hyang-Tag Lim, Sangin Kim, Sung Moon and Sang-Wook Han*, “One to Many QKD Network System Using Polarization-Wavelength Division Multiplexing,” IEEE Access, 8, 194007 (2020)
- Byung Kwon Park, Min Ki Woo, Yong-Su Kim, Young-Wook Cho, Sung Moon, and Sang-Wook Han*, "User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1 × N quantum key distribution network system", Photonics Research 8, 296 (2020)

II

Multiplexing Enables One QKD Server to Support Up to 64 Users

SCALABLE QKD NETWORKS



Source figure: Park et al., Photonics Research 8, 296 (2020), Fig. 1

1 × 64

One server supports up to 64 users

1 Detector Pair

Shared across all user channels

WDM × PDM × TDM

Users are separated by wavelength, polarization, and time

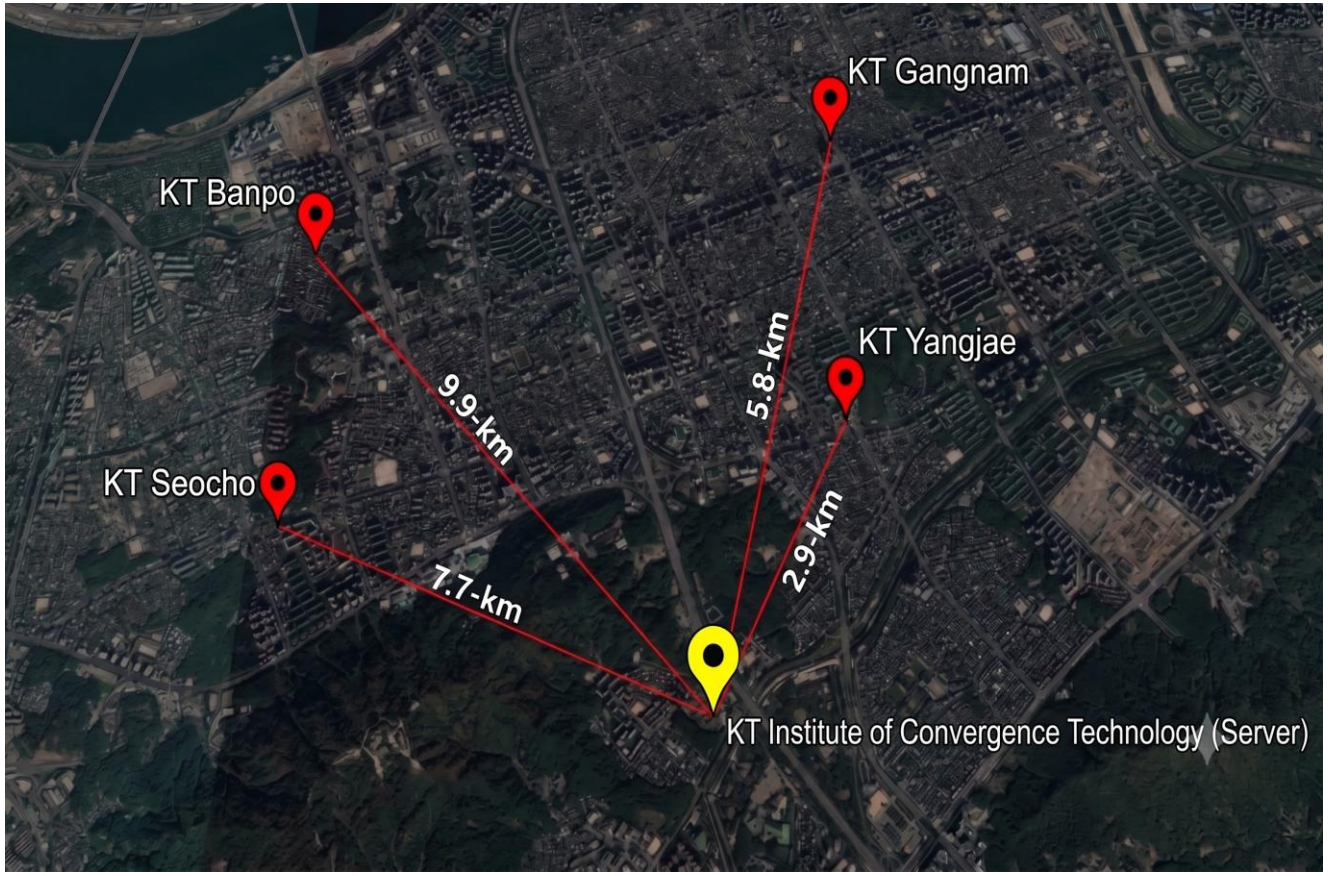
II

Quantum Key Distribution Testbed: 2018

Commercial-Fiber QKD Network Deployment

1x4 Quantum Key Distribution Network System & Commercial Network Verification

2018 KIST-KT 1x4 Quantum Cryptography Network Deployment (Seoul)



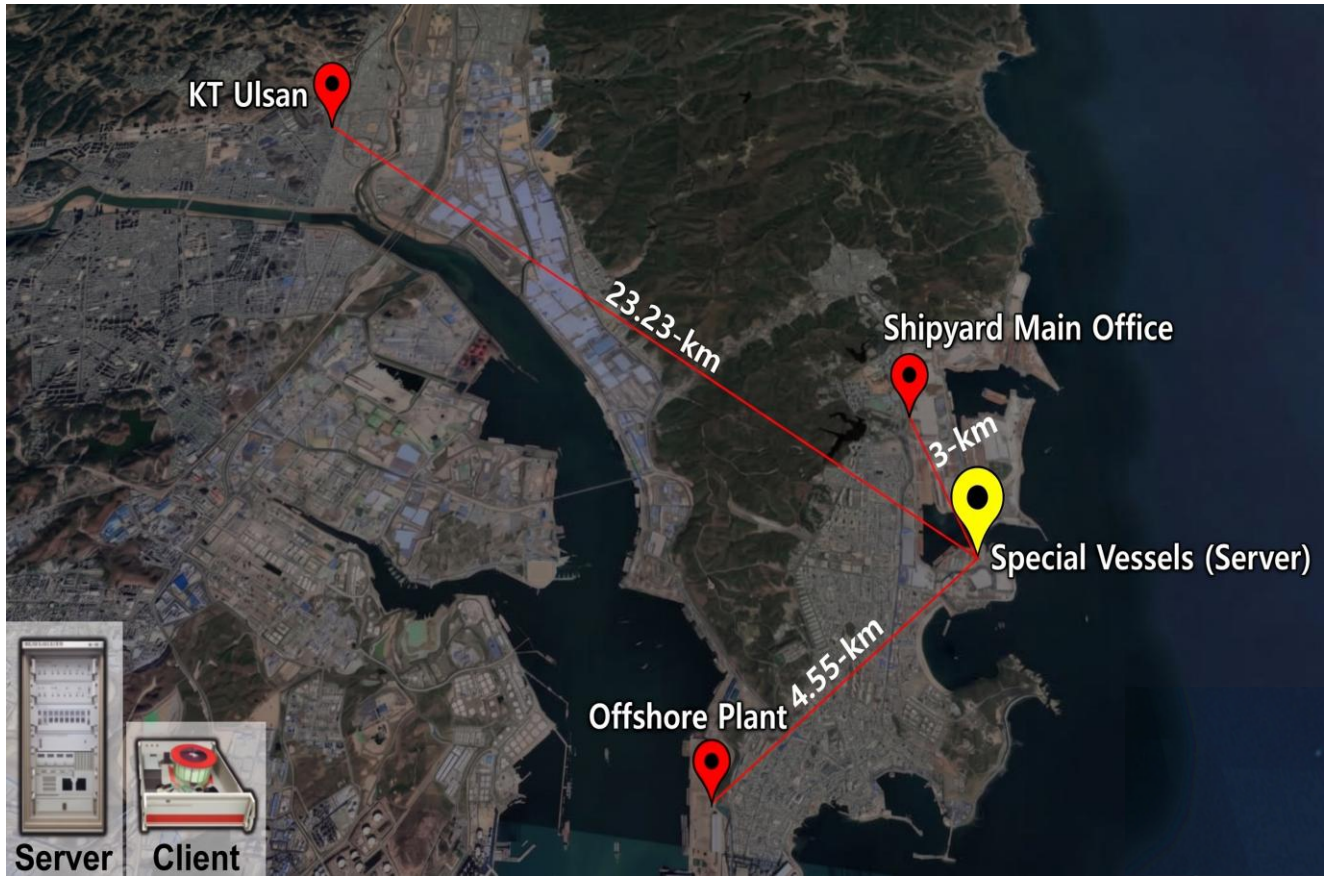
II

Quantum Key Distribution Testbed: 2021

Industrial-Site Network Validation

HD Hyundai Heavy Industries Shipyard Secure Communication Testbed in Operation

2021 KIST-HD Hyundai Heavy Industries 1×3 Quantum Network Deployment (Ulsan)



II

Technology Transfer: 2022

From Research to Commercialization

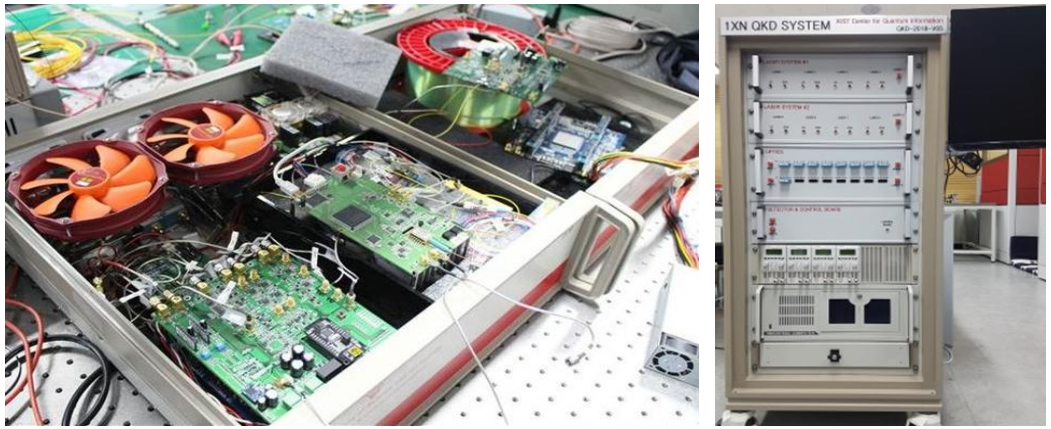
Promoting Full-Scale Commercialization via Technology Transfer to SDT Inc.

Major Communication Networks Including Defense and Public Safety

III

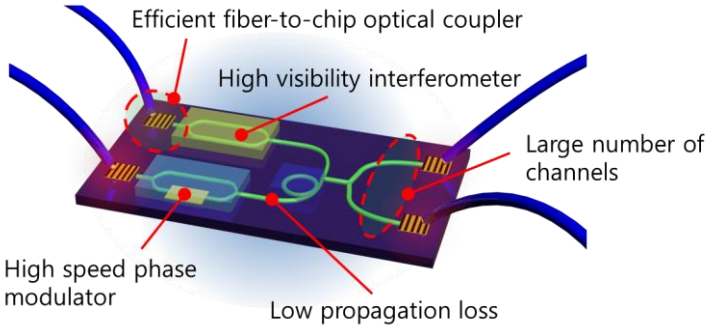
Integrated Photonics Enables Compact QKD Systems

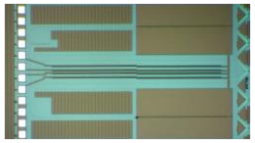
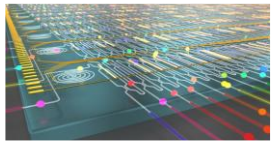
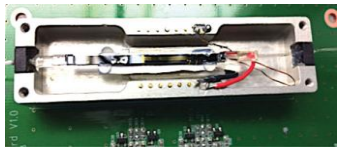
From bulk optical systems to scalable photonic integration



[KIST 1 x 64 Quantum Key Distribution System]

Ultra-Compact $LiNbO_3$/AlN QKD Chip



Category	Silicon (Si)	Silicon Nitride (SiN)	Silica (SiO_2)	TFLN($LiNbO_3$)
Optical bandwidth	1 – 16 um	0.3 – 8 um	0.2 – 2 um	0.4 – 2um
Loss	4 dB/cm	0.5 dB/cm	0.4 dB/cm	~0.1 dB/cm
Modulation Speed	10 GHz	~kHz (thermal)	~kHz (thermal)	~GHz
QKD Chip				

III

Thin-Film Lithium Niobate Enables Low-loss, High-Speed Control

PHOTONIC INTEGRATION

PASSIVE

Low-loss waveguides

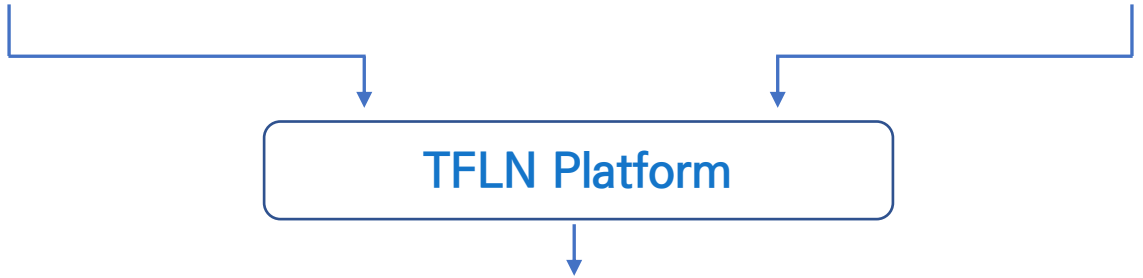
On-chip delay lines and stable interferometers

+

ACTIVE

Fast electro-optic modulation

Phase and intensity control for BB84 state preparation



One material platform can integrate the functions normally split across multiple chips.

0.13 dB/cm	~10 MHz	8 × 4 mm²
measured loss	demonstrated modulation	chip footprint

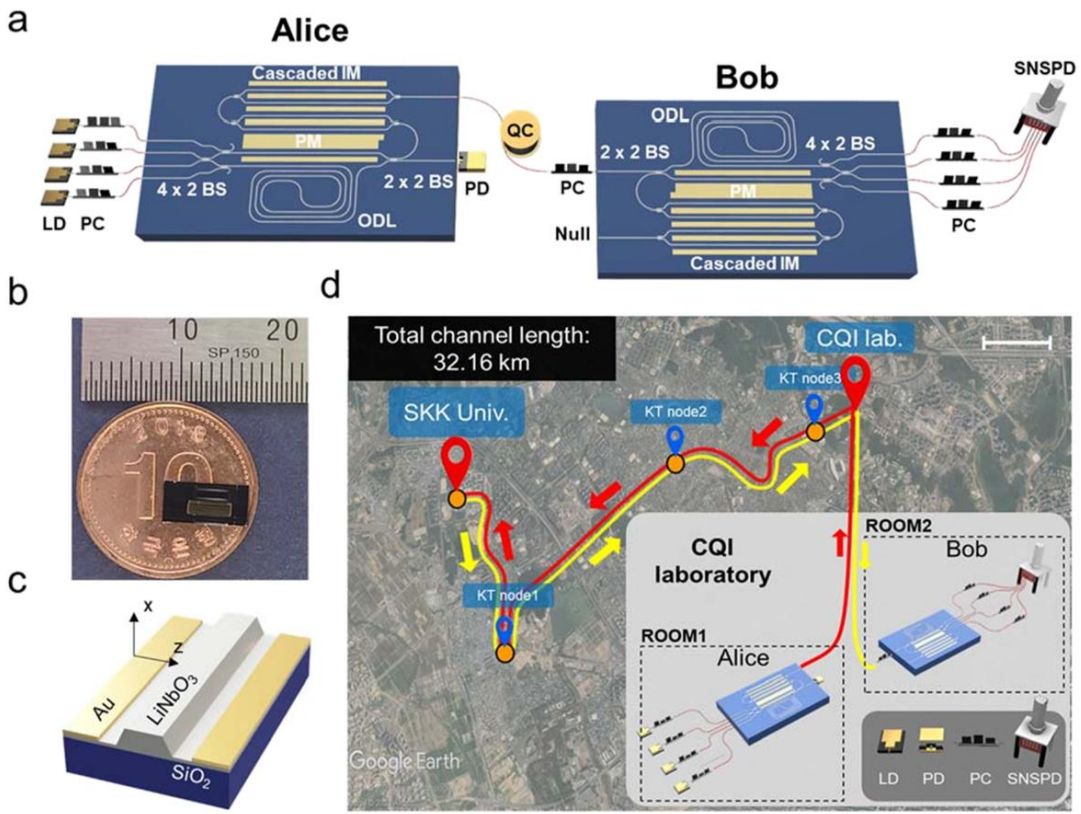
Reported device values: Heo et al., APL Photonics 10, 031301 (2025)

III

A Common TFLN Architecture Supports Both Alice and Bob

PHOTONIC INTEGRATION

Monolithic active–passive photonic integration



IDENTICAL ARCHITECTURE

Alice = Bob

8 × 4 mm²

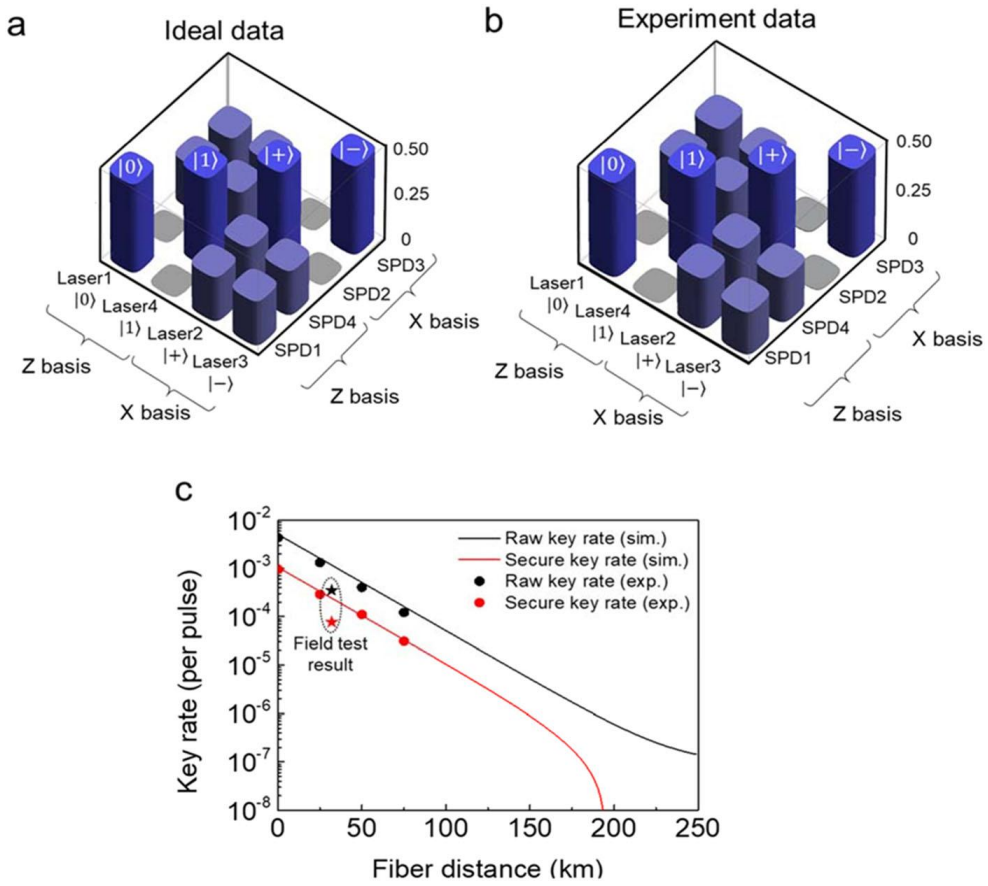
- Fewer device variants
- Simplified control
- Higher manufacturing yield
- Easier replacement and scaling

Source figure: Heo et al., APL Photonics 10, 031301 (2025), Fig. 1

III

On-Chip BB84 Demonstrated over a 32.16 km Field Link

PHOTONIC INTEGRATION



FIELD DEMONSTRATION

32.16 km

Field-deployed fiber link

0.58%

Overall QBER (measured)

0.77×10^{-4}

Secure key rate
Two-decoy state, asymptotic analysis

Source figure and values: Heo et al., APL Photonics 10, 031301 (2025), Fig. 4

IV

Twin-Field QKD Extends the Distance Limit

EXTENDING DISTANCE

Conventional QKD

$$R \propto \eta$$

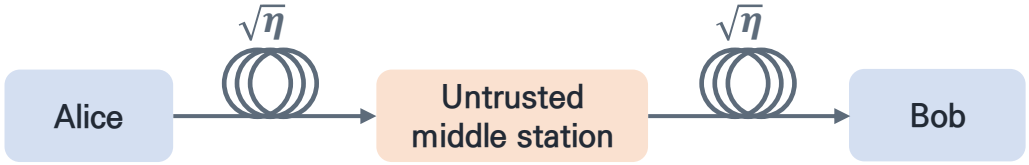
Direct transmission limits the key rate to the full channel transmittance.

Channel transmittance: η

Twin-field QKD

$$R \propto \sqrt{\eta}$$

Single-photon interference at an untrusted middle station improves the distance scaling.



Effectively splits the lossy channel into two shorter links.

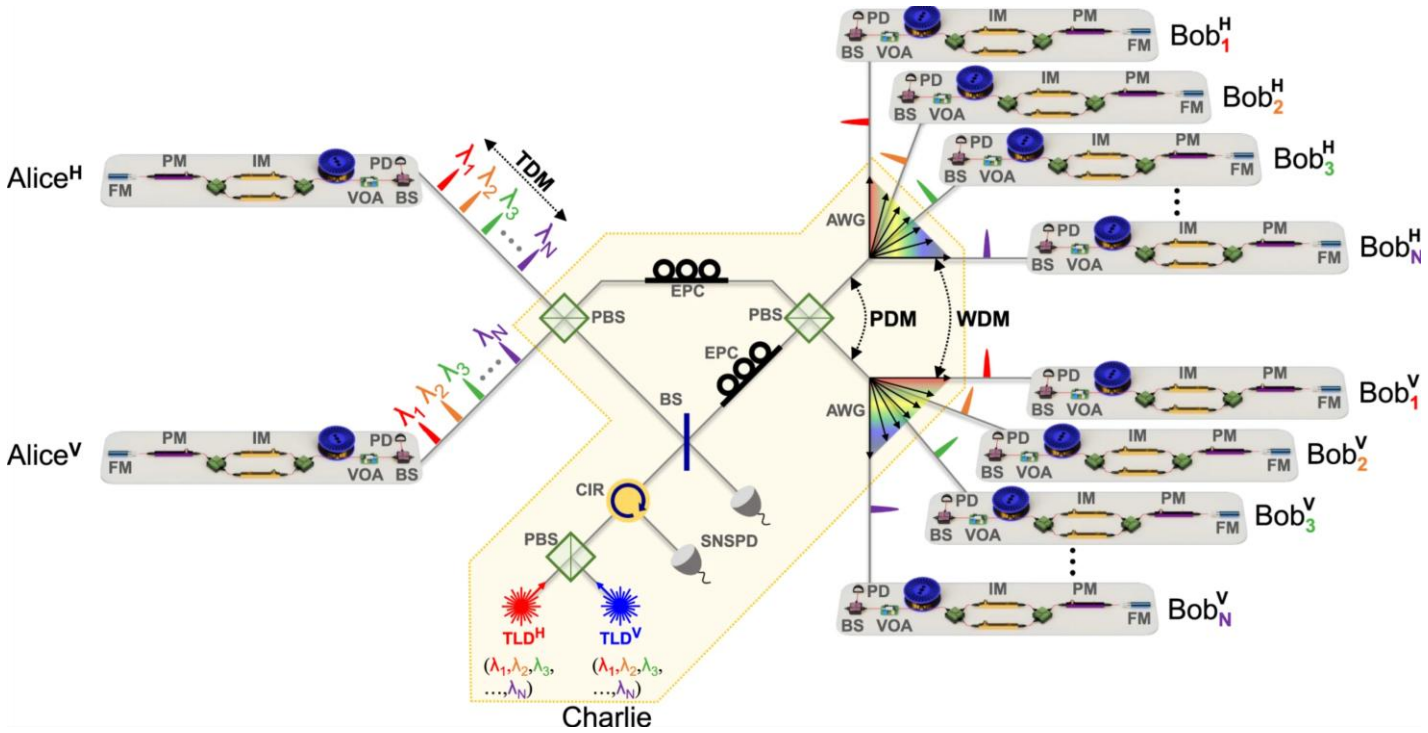
Longer reach requires precise phase stabilization between Alice and Bob.

TF-QKD concept summarized from Park et al., npj Quantum Information 8, 48 (2022)

IV

Scalable 2 × N TF-QKD Network Architecture

EXTENDING DISTANCE



SHARED NETWORK ARCHITECTURE

WDM × PDM × TDM

Wavelength × Polarization × Time

- 2 server nodes × N clients
- One SNSPD pair shared across the network
- Sagnac plug-and-play architecture
- Automatic mode matching with fewer active controllers

16 connections evaluated over
50 km fiber

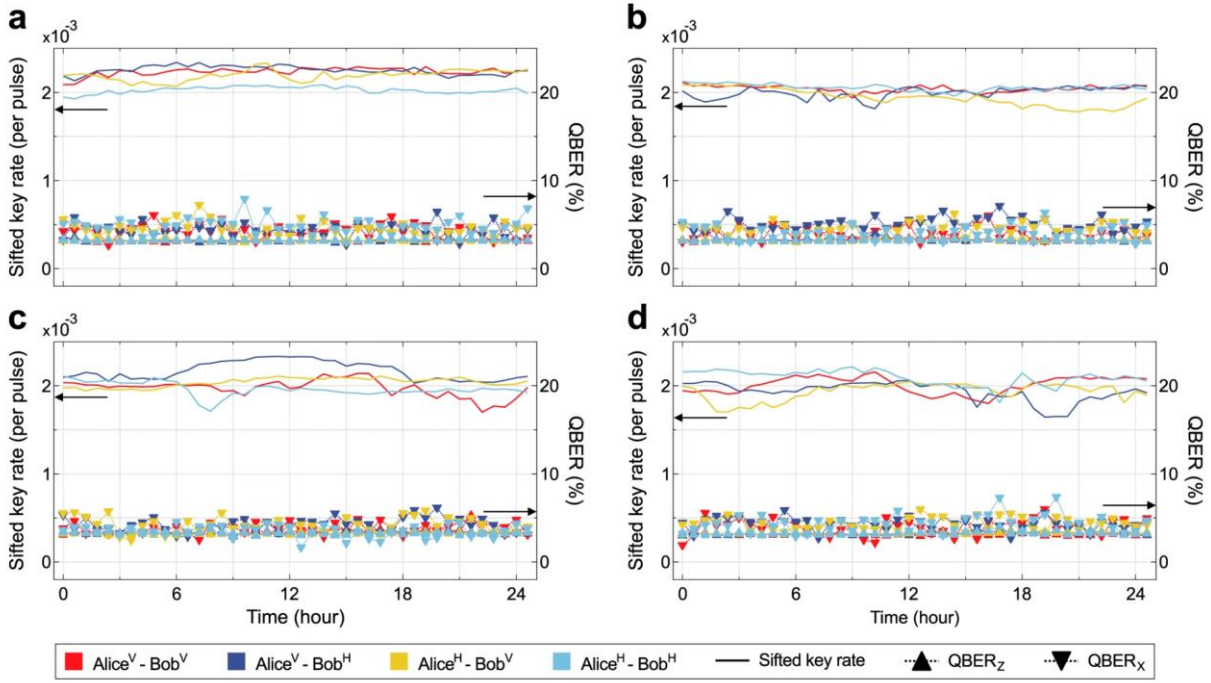
Source figure: Park et al., npj Quantum Information 8, 48 (2022), Fig. 1

IV

2 × N TF-QKD Network Performance

EXTENDING DISTANCE

One-day measurement for each of 16 configured connections



EXPERIMENTAL RESULTS

50 km fiber • 16 connections • SNS TF-QKD protocol

Average secure key rate across 16 connections

1.31×10^{-4} bit/pulse

1.52 bit/s

Complete finite-size analysis applied

Source figure and values: Park et al., npj Quantum Information 8, 48 (2022), Fig. 8

IV

Chip-Scale TF-QKD Development

CURRENT RESEARCH

PHASE	High-precision phase estimation	Estimate the Alice-Bob relative phase for stable single-photon interference.
SECURITY	Pure phase-error analysis	Estimate information leakage and derive a secure-key bound from measured data.
INTEGRATION	TFLN-based TF-QKD hardware	Integrate modulation, delay, monitoring, and control into a compact photonic platform.

Research Target: Stable TF-QKD operation over hundreds of kilometers.

V Summary

2020

1 × N field network

WDM + PDM + Sub-ns Timing Control

SCALABILITY

2025

Monolithic TFLN QKD

Identical Tx/Rx Chips over Deployed Fiber

INTEGRATION

NEXT

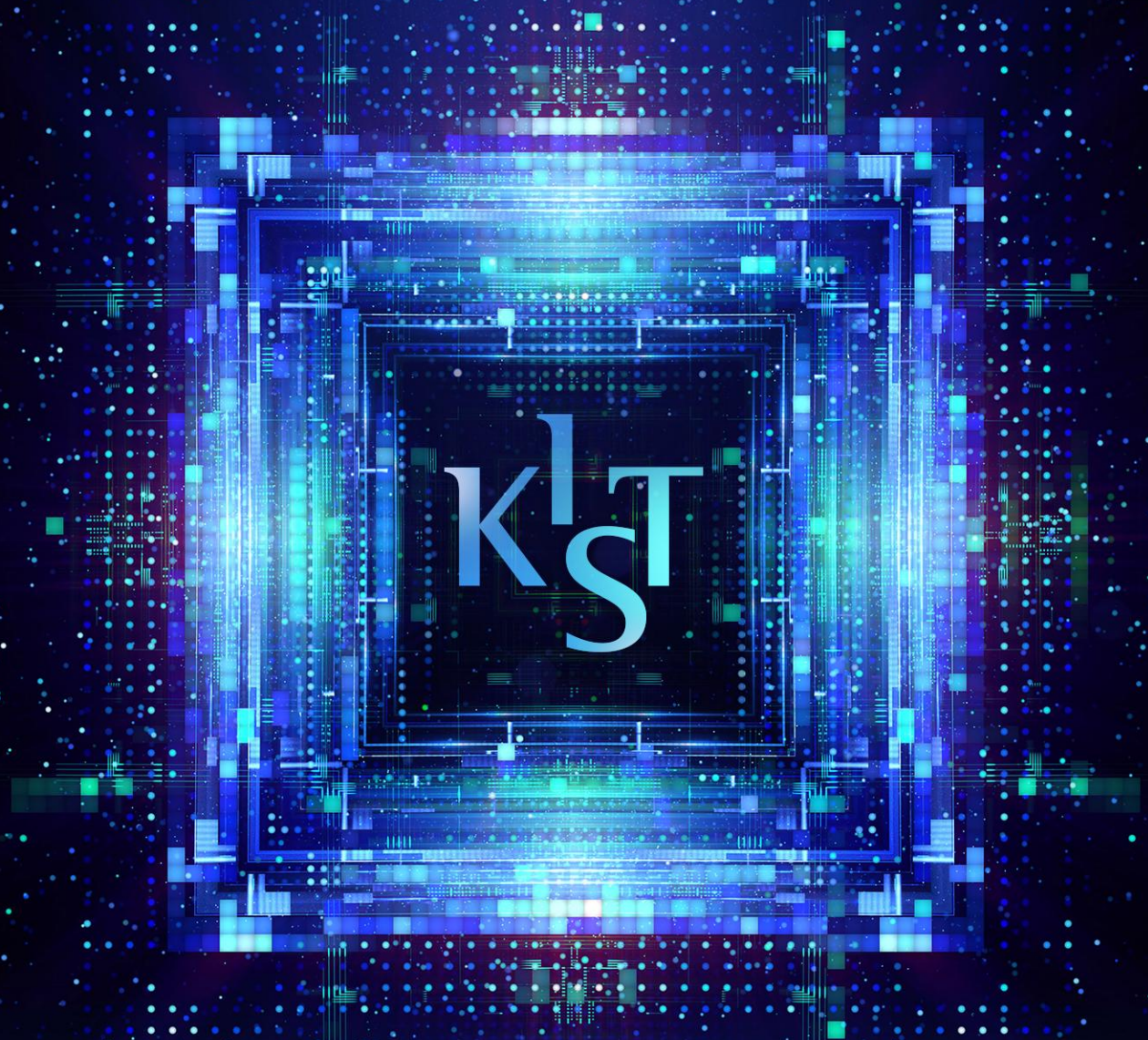
Integrated TF-QKD

Phase Estimation + Pure Phase-Error Analysis

DISTANCE

One continuous goal: practical, scalable quantum communication infrastructure

Thank you



KIST 한국과학기술연구원
Korea Institute of Science and Technology