ETSI/IQC Quantum Safe Cryptography Event

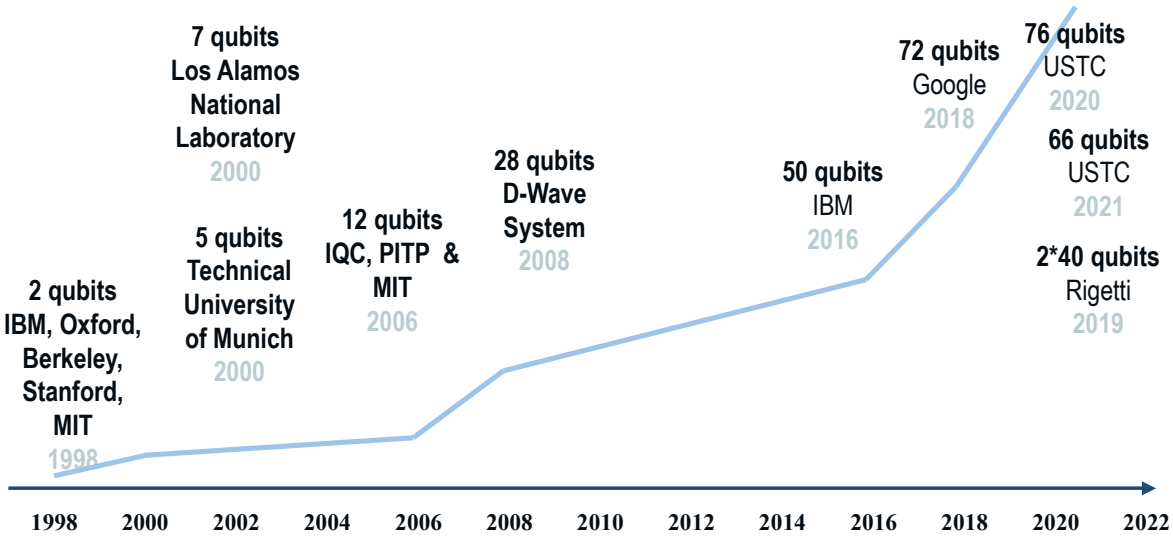
A Brief Introduction to the Latest Progress of China's QKD Industry

Dr. Wei Qi
CEO of CAS Quantum Network Co., Ltd.
Chairman of CCSA ST7

量子网络 QUANTUMNET
www.qtict.com

14/2/2023

Quantum Computing Will Bring New Security Risks



Quantum Computing R&D Is Accelerating

Different technical paths

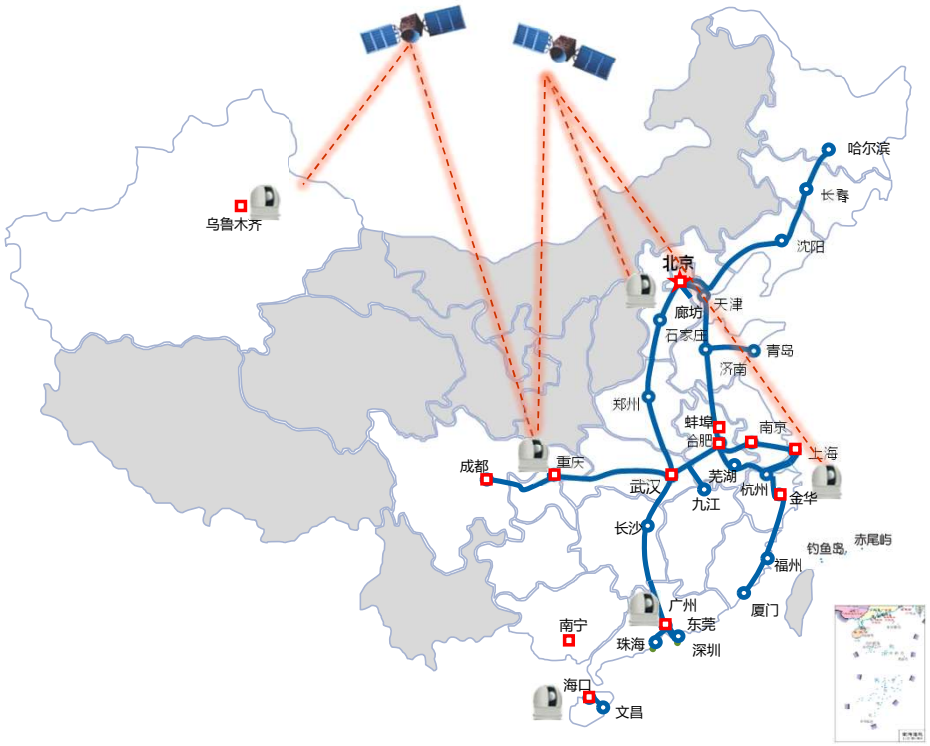
- Quantum communication with Quantum Key Distribution Network
- Migration to Post-Quantum Cryptography

Organization were created to help industry address the threat of quantum computers

- Quantum Safe Cryptography (2013)
- European Quantum Industry Consortium (2016)
- …

Many countries or regions have made a lot of contributions to the QKD industry

Larger Quantum Network



From experimental to commercial

Beijing-Shanghai QKD backbone network (2013-2017)

National wide-area quantum secure communication network (2018-2022)

Feature

- **Exceeds 10,000 kilometers (6,214 miles) in length**
- **Commercial services have been provided in Beijing, Shanghai, Guangzhou, etc.**

More Advanced Quantum Satellites

July 2022: "Jinan-1" was launched

- Real-time satellite-to-ground quantum key distribution between micro-nano satellites and miniaturized ground stations.
- Lay the foundation for the construction of a low-cost, practical space-earth integrated wide-area quantum secure communication network.

The differences between "Jinan-1" and "Micius"

- Lighter weight: only 23 kg, 1/5 of the "Micius "
- The frequency of the light source: 6 times higher
- Key generation: 2-3 orders of magnitude higher

Smaller

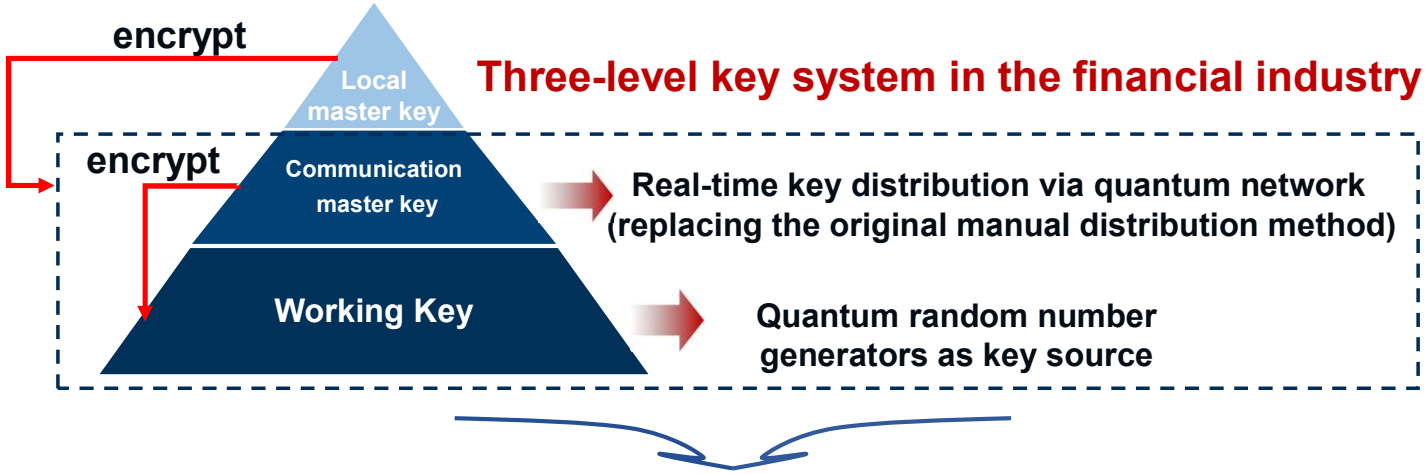
more economics

more practical

Backbone Applications: Quantum-enhanced financial security services

The People's Bank of China Clearing and Payment System

Key generation, distribution and update between bank clearing data center nodes based on quantum technologies



- **Security improvement:** root key security guaranteed, high-frequency large-scale key distribution enabled
- **Cost reduction:** All sub-service systems can share the common quantum-based security infrastructure via flexible APIs, needless for separate development

Backbone Applications: Quantum-encrypted calls

Commercial quantum secure applications for mobile telecom terminals were carried out in practice

中国移动 China Mobile 5G+ 量子网络 QUANTUMNET

May 17th, 2022 (World Telecommunication and Information Society Day)
China Mobile released
Quantum Encryption Call Service (VoLTE version)

- **End-to-end encryption with keys extracted from QKD network**
- **Achieve one-session-one-key for each call**

The growth of data scale has higher requirements for security

Trend

Massive Data

Emerging Digital Technologies

Metaverse, Blockchain, AI, etc.

Challenge

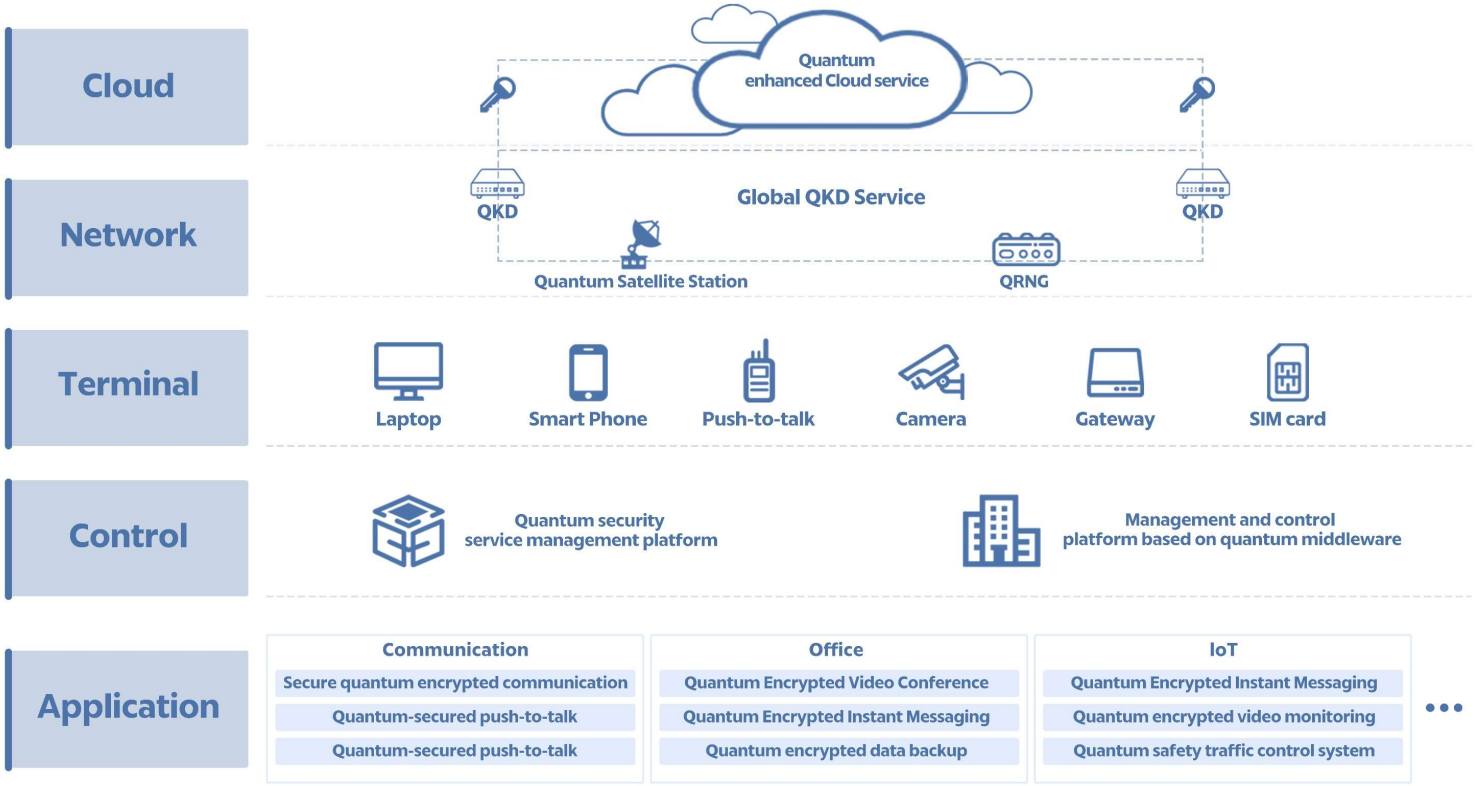
Information infrastructure

Network architecture

Over One Billion Records Leaked in Shanghai (2022)

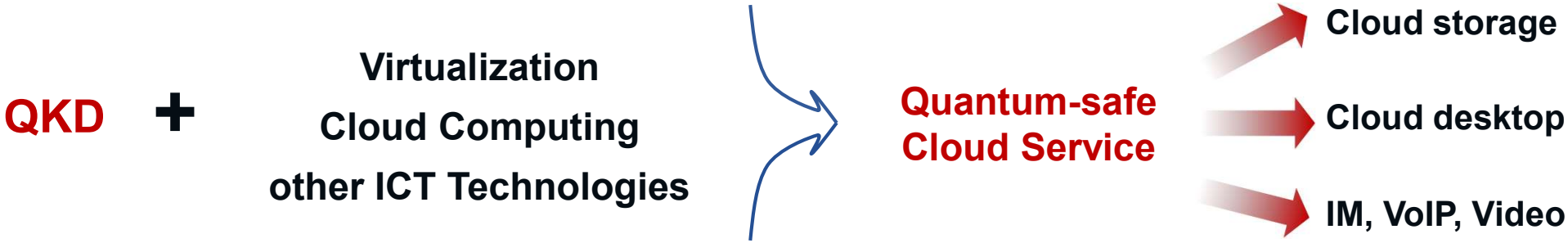
Opportunities for Quantum Encryption Technology Development

The integration of QT and ICT may be a new solution



Practice case: Quantum-safe Cloud Service

Quantum-safe Cloud Service (QCS) is to embed quantum security services into the basic components of ICT cloud platforms, where quantum secure communication plays an essential role of its overall ICT architecture, to provide generic cryptographic services based on unified quantum key generation and management capabilities



- QCS can provide quantum-security-enhanced computing, storage, network and other digital resources through the flexible quantum key management and control mechanisms
- QCS is adopted as an important security solution for the "east-data-west-computing project"

Promote the development of standardization

In June 2017, the CCSA[1] of the MIIT[2] led the establishment of the Quantum Communication and Information Technology Ad Hoc Task Group (ST7).

CCSA members include 56 companies or universities

Published (more than 20 standards are being developed)

- **Key components and modules for QKD based on BB84 protocol**
- **Test methods for QKD system**
- **Technical requirements for QKD system**

Published (2020~2022)

Orchestration Interface for Software Defined Networks
Control Interface for Software Defined Networks
Application Interface

1. CCSA, China Communications Standards Association
2. MIIT, Ministry of Industry and Information Technology

Actively participates in international standard

FG-QIT4N established — **2019.10**

Complete all research topics Released 9 research reports — **2021.11**

JCA-QKDN established — **2022.12**

In SG13 and SG17, China released 9 standards including QKD network framework and security framework, and is developing standards such as QKD network interconnection and interface protocols to accelerate the combination of quantum technology and next-generation network technology

Integrate the PQC algorithm into the commercial QKD system

PQC
authentication
short-term security

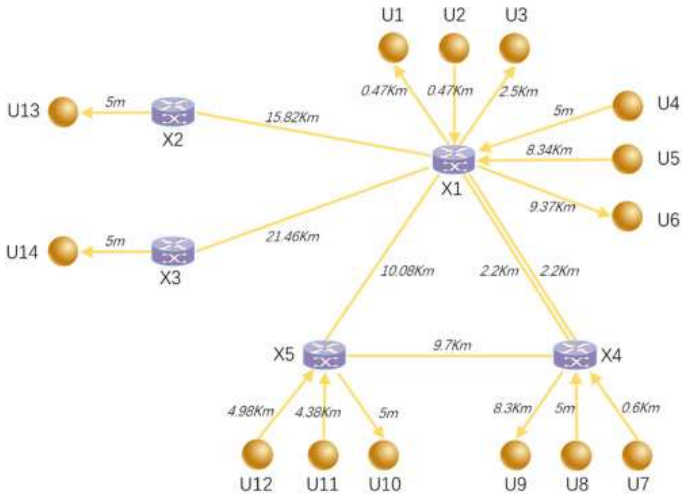
+

QKD
information transmission
long-term security

Verified the feasibility, effectiveness and stability

Replace trusted relays with optical switches

- **Simplify the network topology**
- **Reduce the security dependence of the trusted relay**
- **Reduce the cost of the device**
- **Improve the interoperability between the QKD nodes**



the Jinan field metropolitan QKD network
(14 user nodes and 5 optical switching nodes)

The combined scheme will be promoted in scenarios such as finance, electricity, etc.

1. All optical metropolitan quantum key distribution network with post-quantum cryptography authentication, Optics Express, 2021

Call for cooperation

Like climate change and public health, information security is a global issue. After a three-year delay caused by the pandemic, we call for more international communication and cooperation

the international cooperation

Standardization **ETSI, ITU, etc.**

Industrialization **Infrastructure and Applications**

We believe that the combination of QKD and PQC will have a bright future

ETSI/IQC Quantum Safe Cryptography Event

Thanks

Looking forward to international cooperation

liminghan@qtict.com