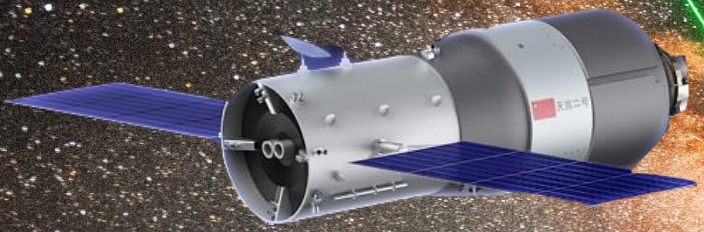
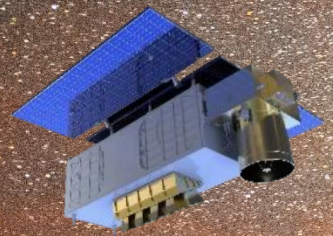
Micius



Tiangong-2



Jinan-1

Standardization and certification consideration of satellite-based Quantum Key Distribution

Weiyang Zhang，Shengkai-Liao
University of Science and Technology of China
Jinan Institute of Quantum Technology

17th,May, 2024

Content

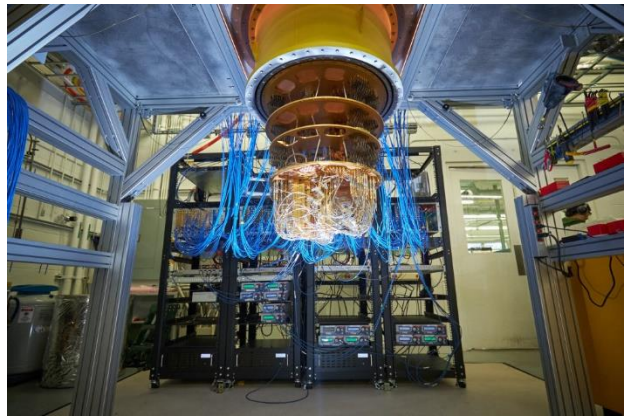
What is QKD and satellite-based QKD

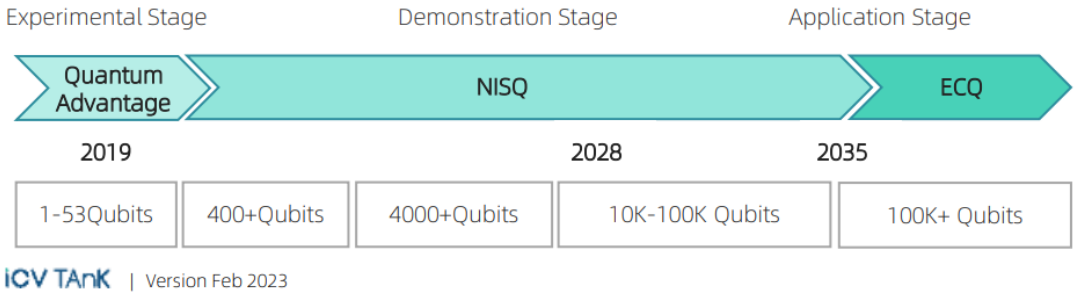
Standardization and Certification

Future plan

Challenge to cyber security

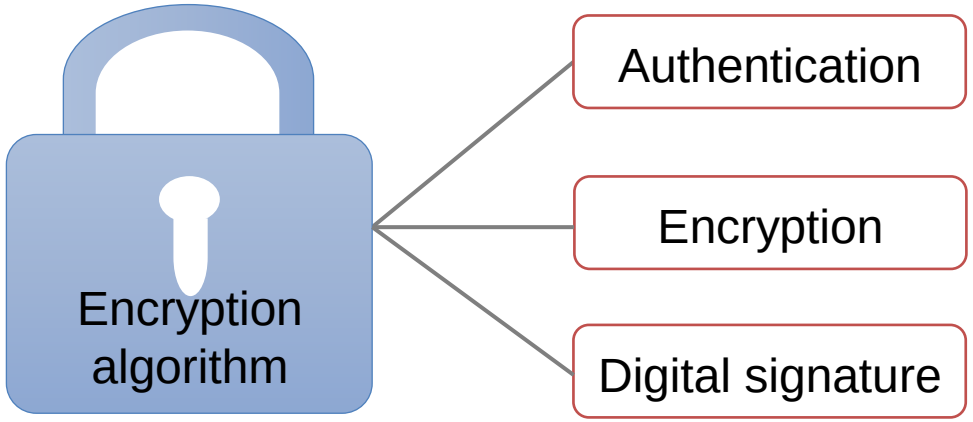
Quantum Computation





Threat

Cyber security ensured by encryption algorithm

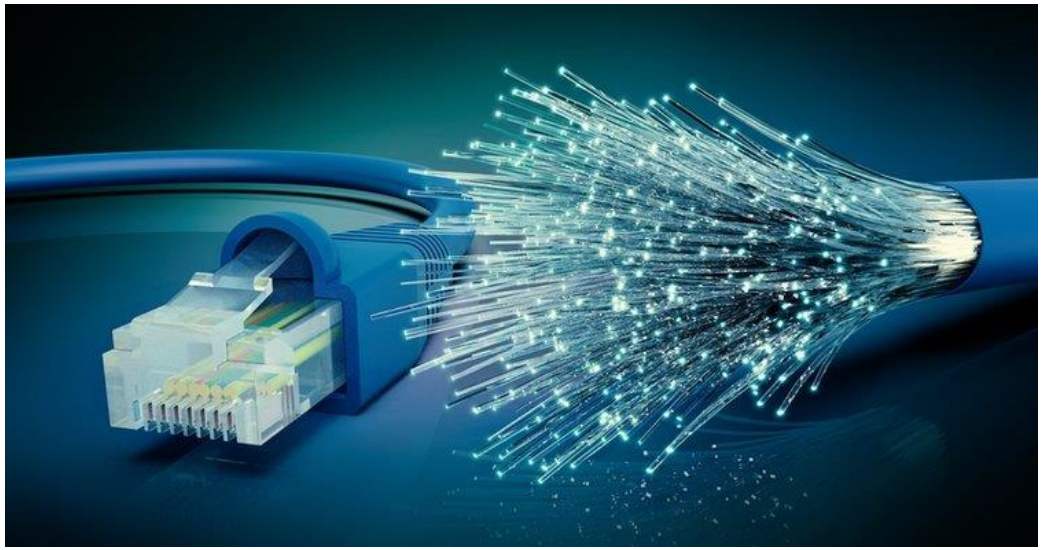


Solutions

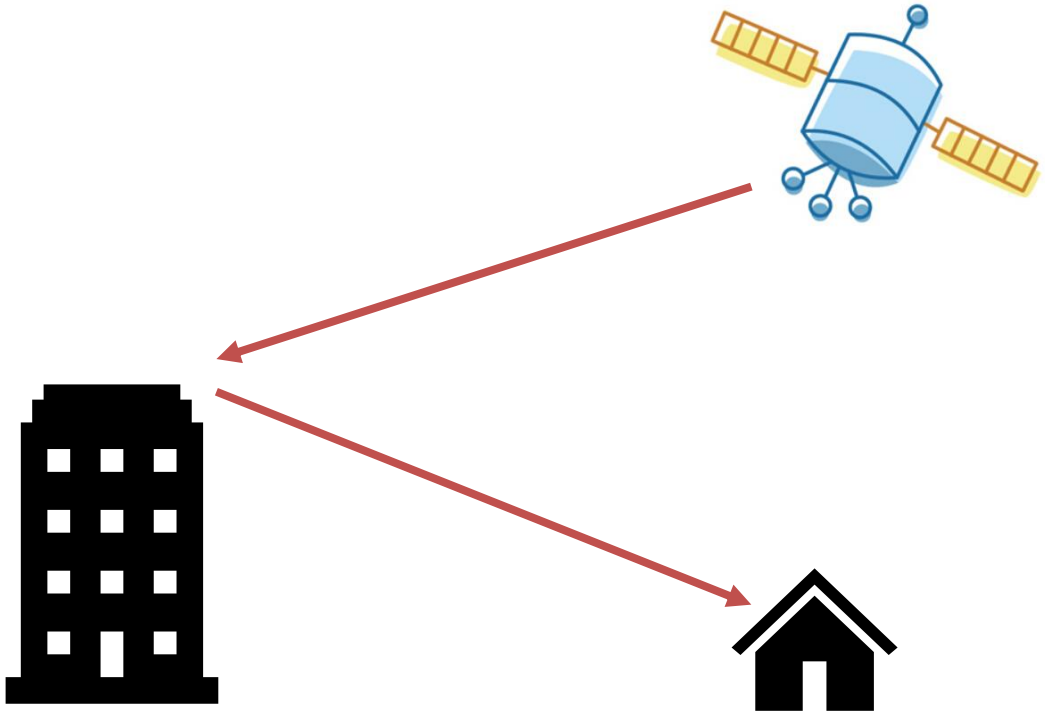
- PQC: Post-Quantum Cryptography
- QKD: Quantum Key Distribution

Quantum mechanics + One-time-pad → Information-theoretic security

QKD channels



Fiber channel



Free-space channel

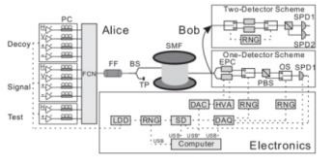
Fiber-based QKD

☑ Fiber channel

- Easy implementation, low cost, can share fiber with exiting network
- Attenuation 0.2 dB/km, 1/100 photons left after 100 km, cannot be transmitted thousands of kilometers point to point

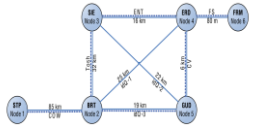
BB84&E91

1984/1991



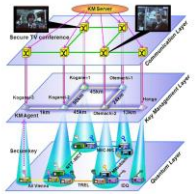
>100 km Decoy experiment

2007



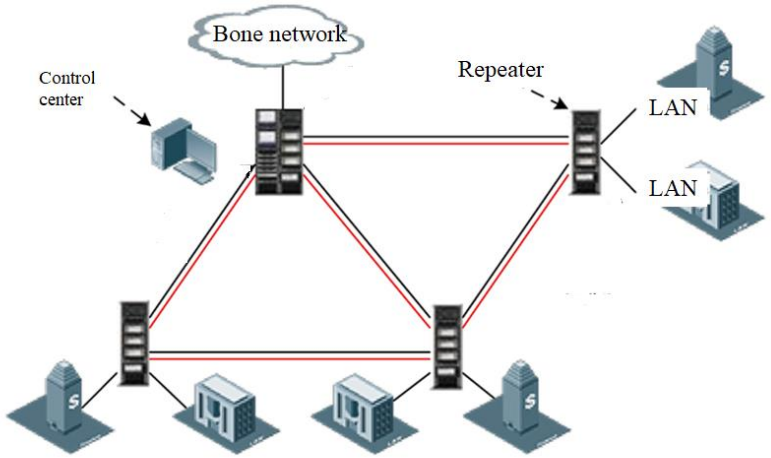
SECOQC QKD Network

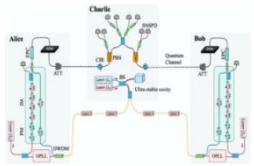
2008



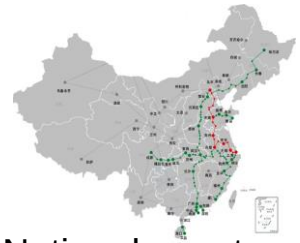
Tokyo QKD Network

2010





TF-QKD 1002 km



National quantum backbone network ~12000 km

2023

Inter-European Quantum Network

Cambridge quantum network

2019

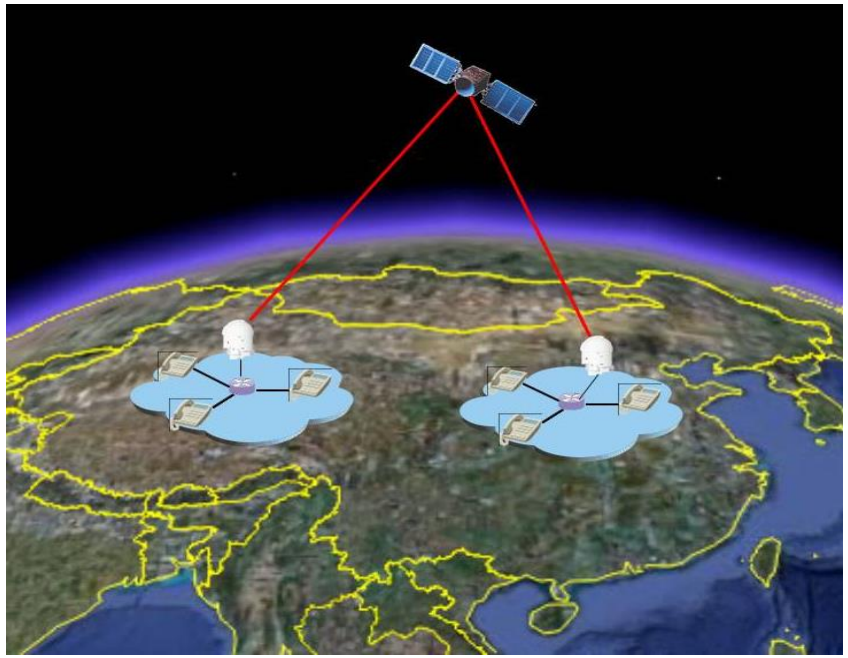
Beijing- Shanghai network ~2000 km

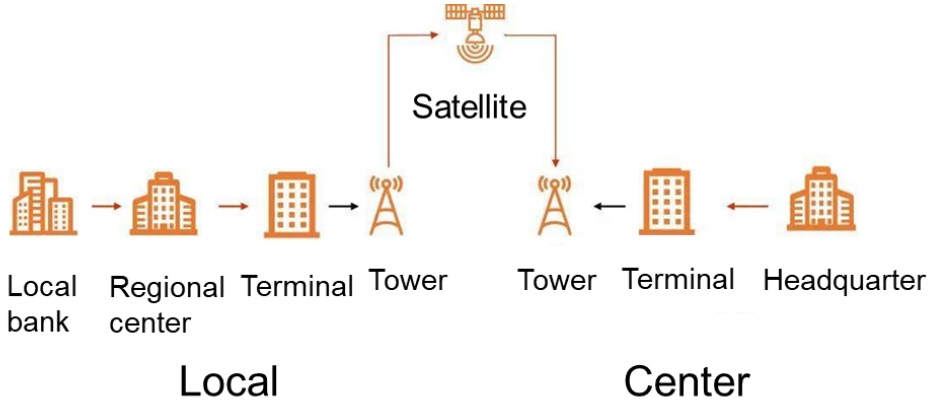
2017

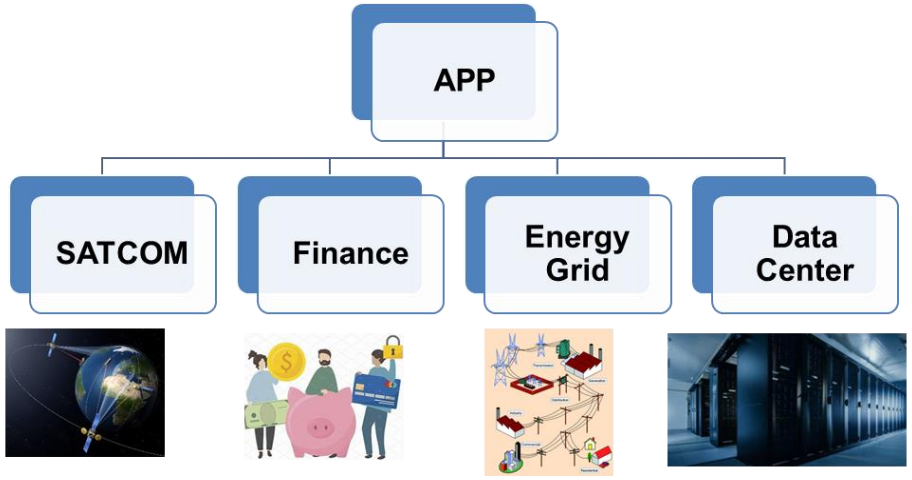
Satellite-based QKD

☑ Free-space channel

- Almost no attenuation in outer space
- ~10 km thickness of atmosphere

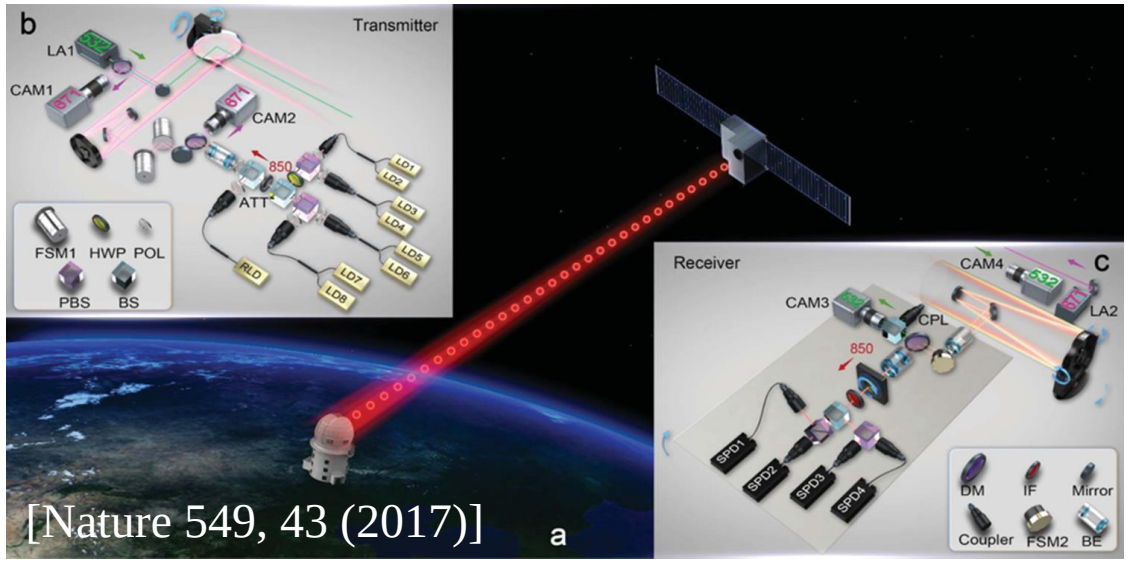






It is the most feasible way to build the global quantum network with satellited-based QKD

Development of satellite-based QKD technology

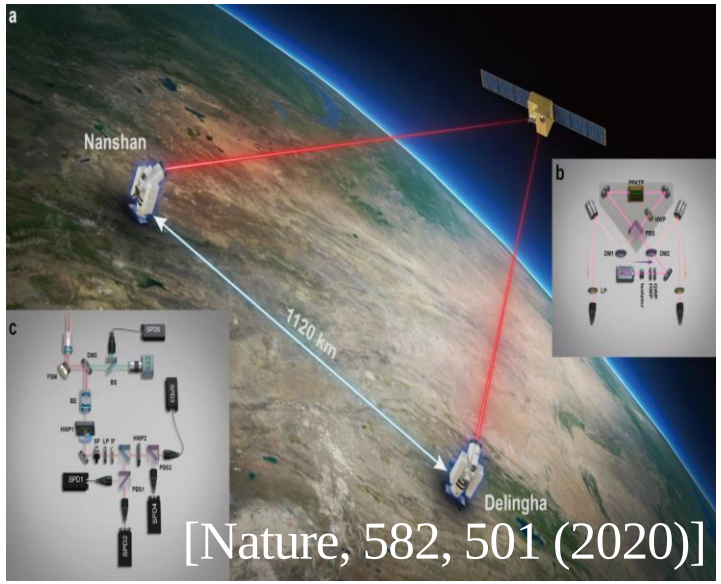


[Nature 549, 43 (2017)]

Satellite-to-ground QKD

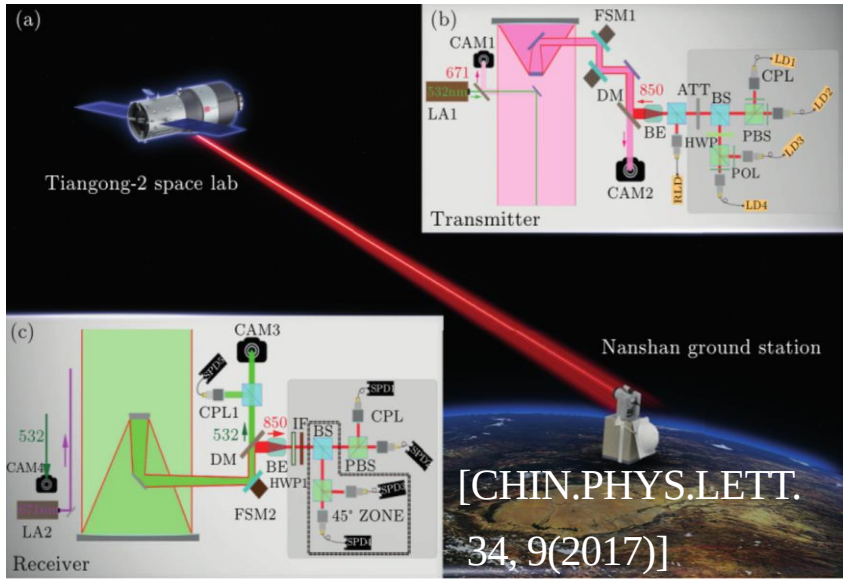
[PRL 120, 030501 (2018)]

Intercontinental QKD



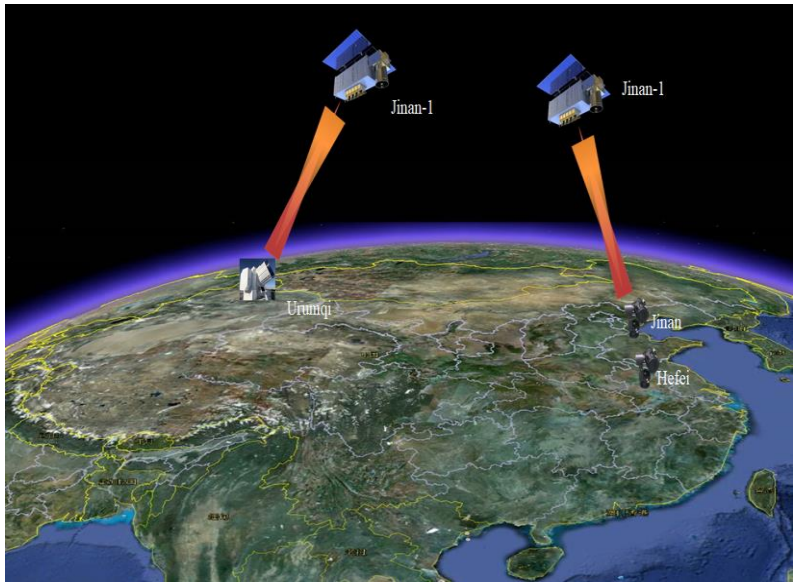
[Nature, 582, 501 (2020)]

Entanglement-based
secure quantum cryptography



[CHIN.PHYS.LETT. 34, 9(2017)]

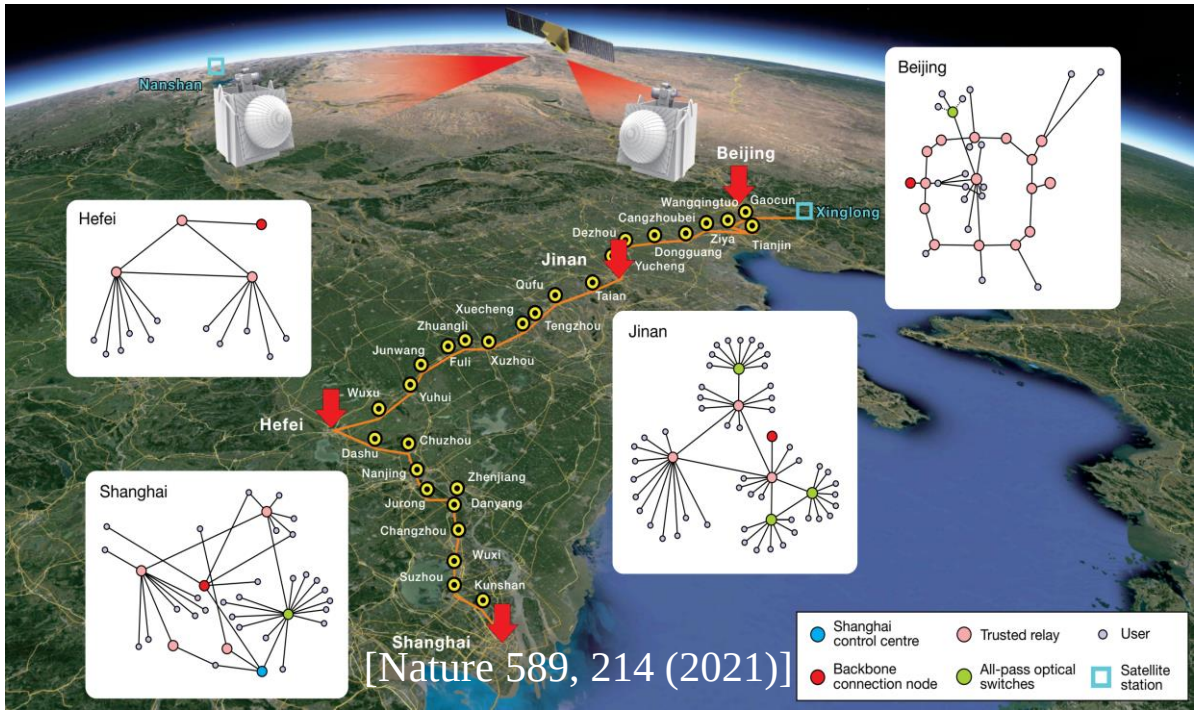
Space station-to-ground
QKD



Microsatellite -to-ground
real-time QKD

Development of satellite-based QKD technology

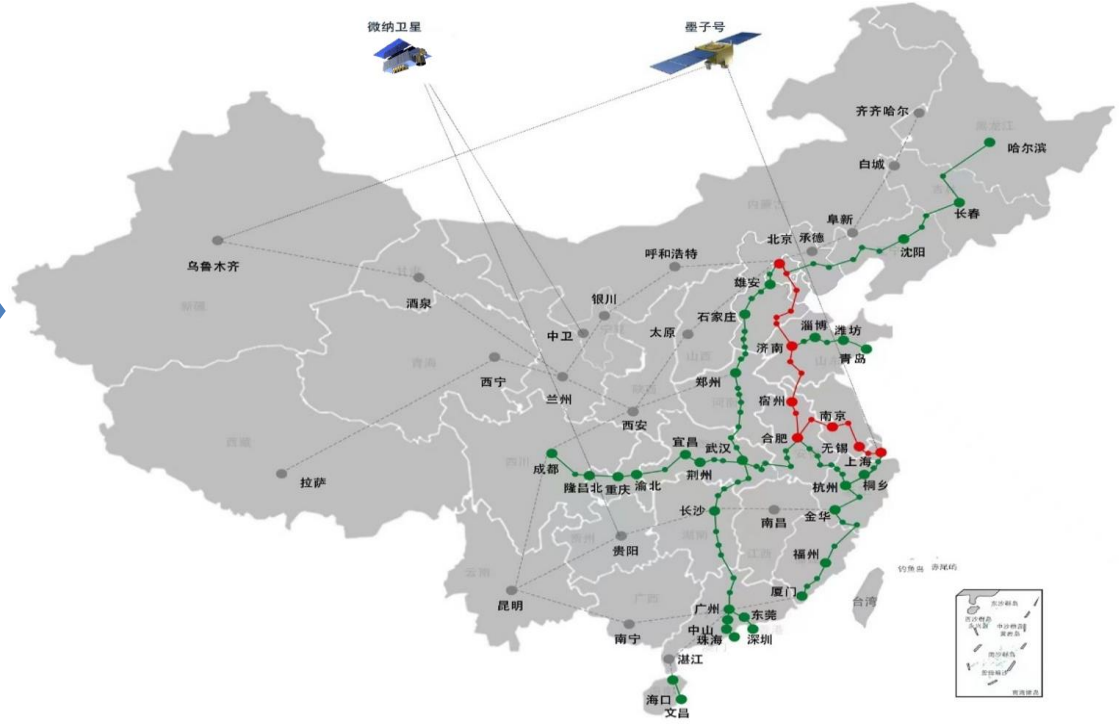
Space-ground integrated quantum network



[Nature 589, 214 (2021)]

~ 2000 km fiber
Micius satellite 2600 km free-space network
~150 users such as:
Banks: PBOC,ICBC
Power distribution companies: National Grid

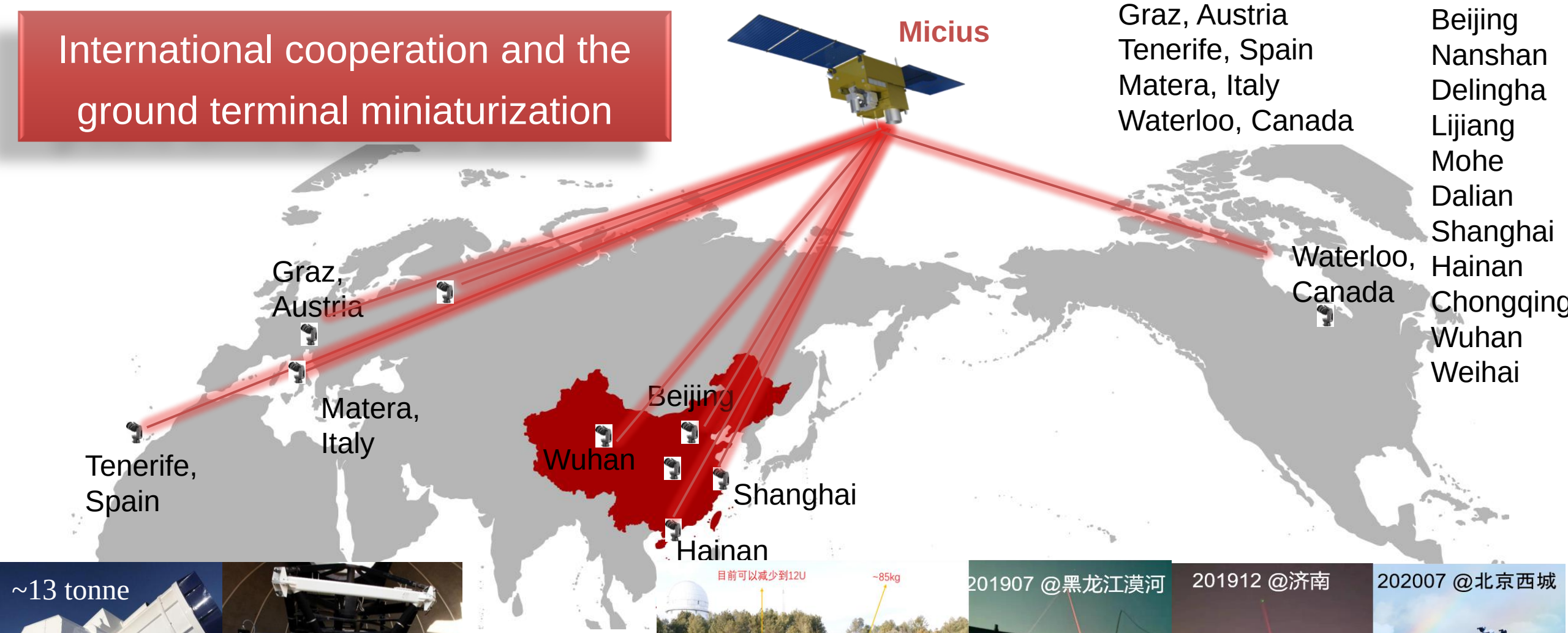
National quantum backbone network



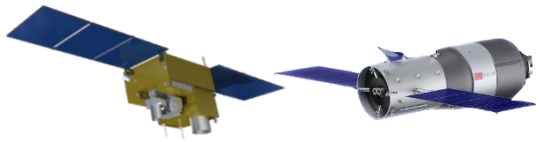
~12000 km fiber network
Jinan-1 satellite
Deliver service for more customers

Development of satellite-based QKD technology

International cooperation and the ground terminal miniaturization

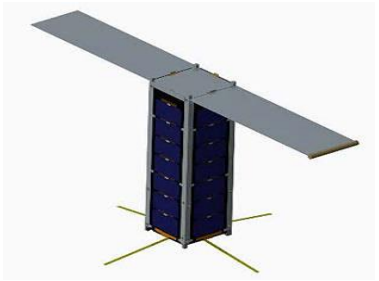


Development of satellite-based QKD technology

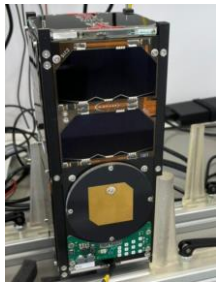


China:
Micius
2016.8

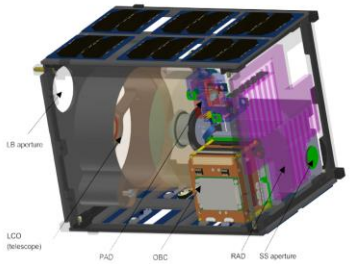
China:
Tiangong-2
2016.9



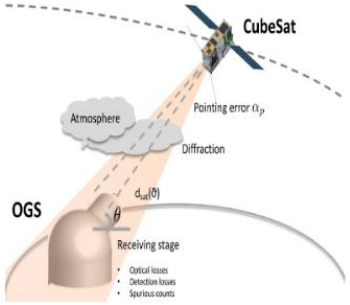
USA: CAPsat
2021.10



Israel: TAU-SAT3
2023.1

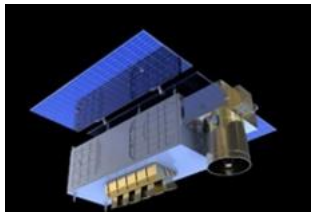


Austria and France:
NanoBob
Planning 2024



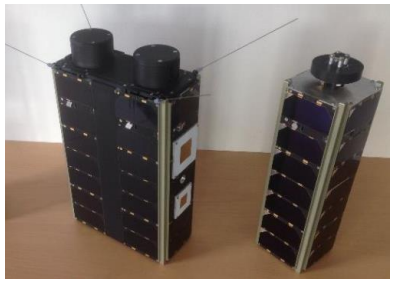
UK: QUARC
Planning 2025

Singapore: SpooQy-1
2019.6



China: Jinan-1
2022.7

USA: SEAQUE
Planning 2024



Germany:
QUBE-II and QUBE-I
Planning 2024

EU: Eagle-1
Planning 2025

Content

What is QKD and satellited-based QKD

Standardization and Certification

Future plan

Development of QKD standard

- ISO/IEC 23837 part 1 and 2 published in 2023
- JTC3 established in start of 2024

Quantum network research group established from 2018

QKD network and security standardization starts from 2018

Development of ISO/IEC 23837 starts from 2017

Software-defined quantum communication，SDQC，established in 2016

ISG-QKD established in 2008，16 standards for QKD published，including user case，security proof……

2008 2016 2018 2023

Existing standards of QKD

Quantum Key Distribution

ITU

FG QIT4N

- The impact of quantum technology on ICT networks
- 8 deliverables published

SG11

QKDN protocol and signaling

SG13

QKDN architecture and function

SG17

QKDN and QRNG security

36 standards published

ETSI

World Class Standards

ISG-QKD

Industry Specification Group on Quantum Key Distribution

12 specifications published:

QKD use cases;
Components and internal interfaces;
Vocabulary;
Application interface;
Security Proofs;
etc.

ISO/IEC JTC1

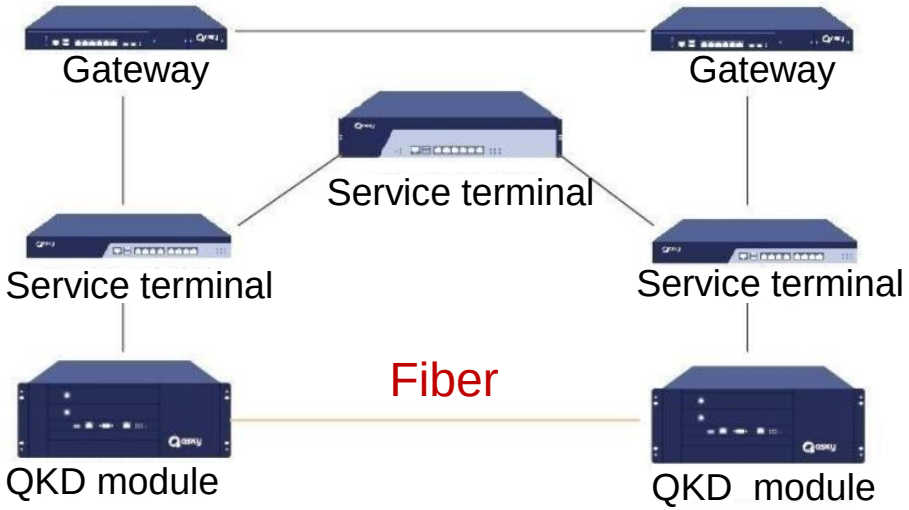
INFORMATION TECHNOLOGY STANDARDS

ISO/IEC JTC1 SC27

Information security, cybersecurity and privacy protection

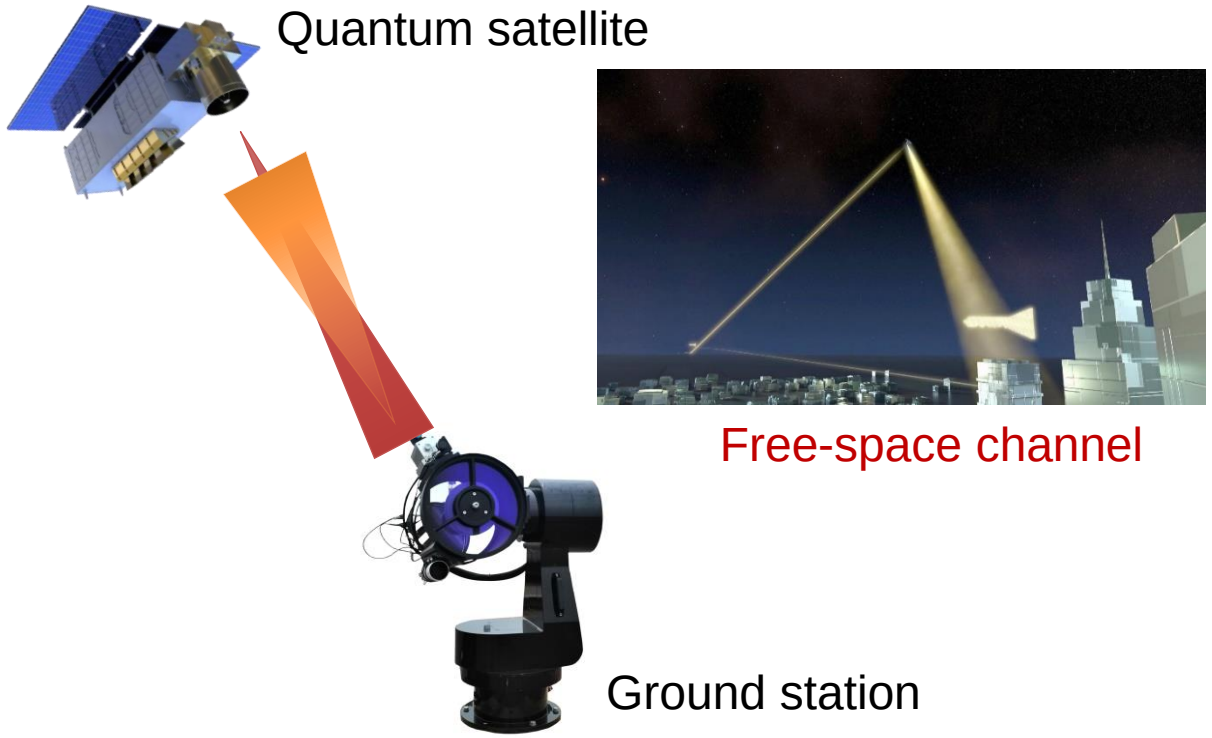
Security requirements, test and evaluation methods for quantum key distribution:
Part 1 Requirements & Part 2 Evaluation and testing methods

Different objects of standardization



QKD system based on fiber:

- Connected by fiber or network
- Set in manageable cabinets



QKD system based on free space:

- Connected by telescope system
- Transport in free-space channel
- Satellite set in outer space
- Ground station set outdoors, both in harsh environments

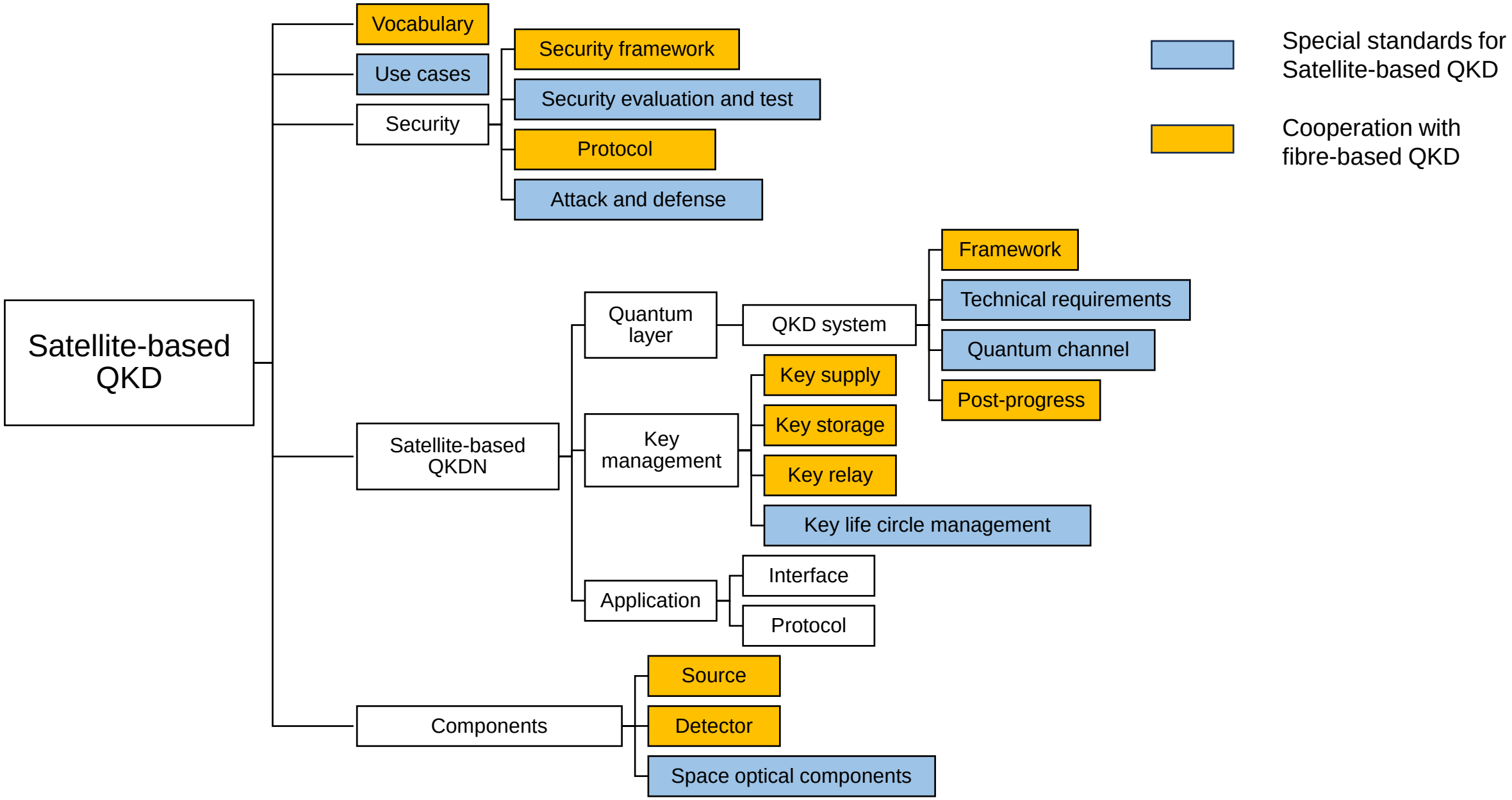
The Gap

Gap analysis from CENELEC (European Committee for Electrotechnical Standardization), not too much information for QKD using free space or satellite is known to us

QKD standard categories			Type of standards								
			Basic standard	Terminology standard	Testing standard	Product standard	Process standard	Service standard	Interface standard	Standard on data to be provided	Informative
	SG	**Security evaluation: generic standards**	X		X	X					
	SM	**Security evaluation: evaluation methodology and testing standards**	X		X	X					
	SB	**Security evaluation: background documents**	X		X	X	X	X	X	X	
	ME	Metrology standards (Testing, calibration, characterization, stability, attacks, countermeasures)		X	X				X		X
	KM	Key management and key delivery Interface standards					X		X		
	QN	QKD Network standards	X					X	X		X
	SA	Satellite modules and networks	X	X	X	X	X	X	X	X	X
	WP	White papers, technical reports and supporting documentation									X
	VC	Vocabulary and general standards	X	X	X						X
	OT	Other standards									X

https://www.cencenelec.eu/news-and-events/news/2023/brief-news/2023-03-22-standardization-for-quantum-technologies/

Standardization consideration of satellite-based QKD



Standard projects

Satellite-based Quantum Key Distribution

SG13

Y Suppl.80:
Quantum key distribution networks use cases

Y.TR-SQKDN:
Standardization consideration of Satellite-based QKDN

Started from 2024-3-15

Technical Group: SES

Satellite Earth Stations & Systems

Technical specification (TS):
Satellite-Quantum Key Distribution (S-QKD) Satellite Systems & Associated Optical Earth Stations (OES)

Started from 2023-5-22

ISO/IEC JTC1 SC27

Information security, cybersecurity and privacy protection

PWI: Investigation of the effect of transmission media on QKD security evaluation and possible modifications to ISO/IEC 23837

Started from 2023-10-16

Test and certification

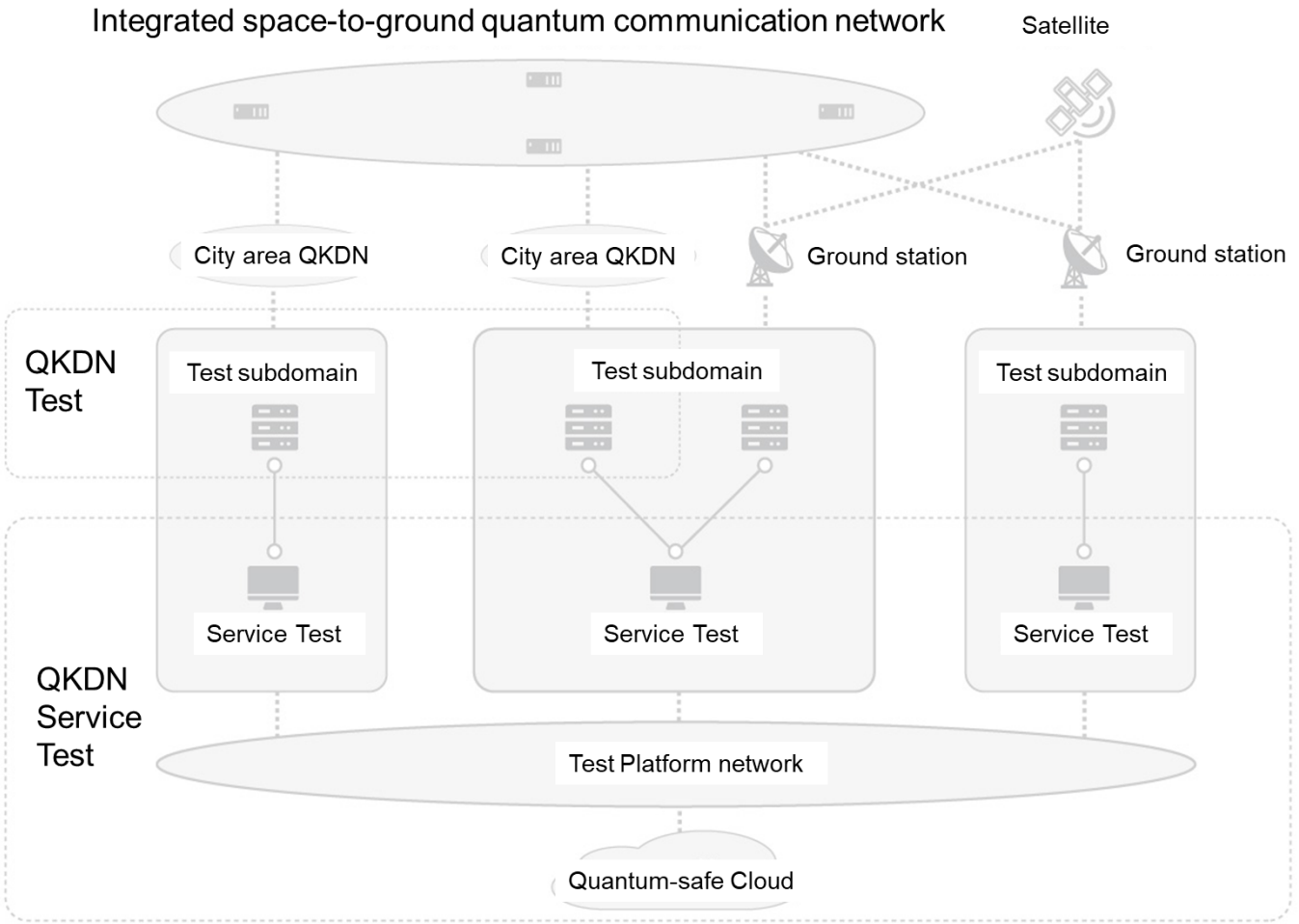
Test platform for an integrated space-to-ground quantum communication network

Test item

- Access test
- Security evaluation
- Space-to-ground key generation test

Function

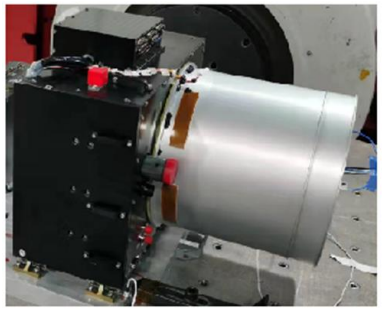
- Test management
- Test environment monitoring
- Check the key generation of every nodes in real time

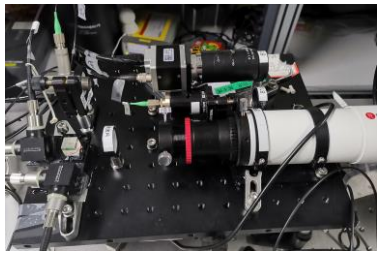


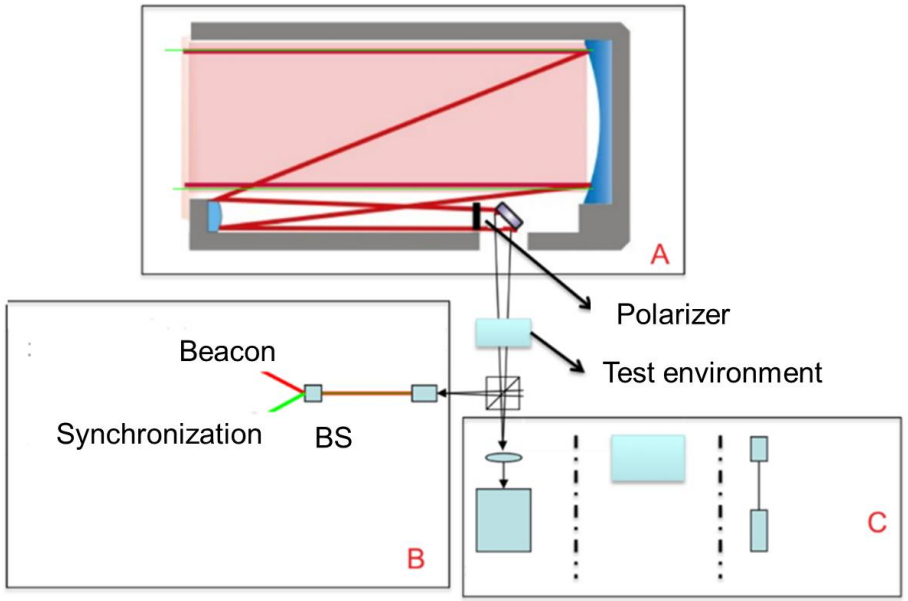
Test and certification

Testbench for space optical module

- Telescope system
- Beacon module
- ATP (Acquisition, pointing and tracking) module
- Functional test & Performance test

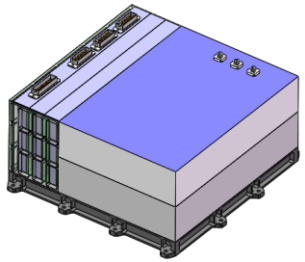


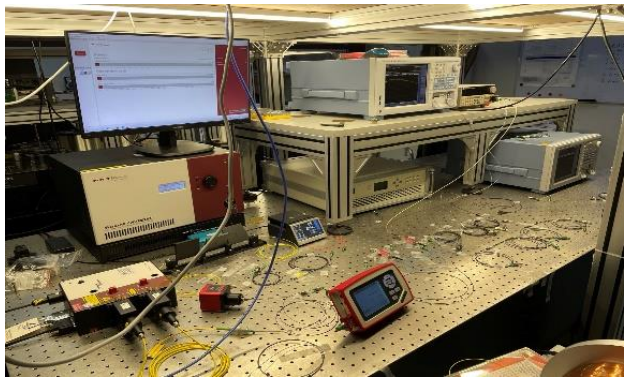




Testbench for quantum module

- Source
- Encoder
- Decoder
- Detector
- Attack & Defense
- Space-like environments





Content

What is QKD and satellited-based QKD

Standardization and Certification

Future plan

Future plan

01 Research

Initiate TR or standard outlook to pave the way to standardization of satellite-based QKD.

02 Standardization

Carry out standard projects targeted on satellite-based QKD

03 Certification

Discuss on certification and test method

Thank you for your attention