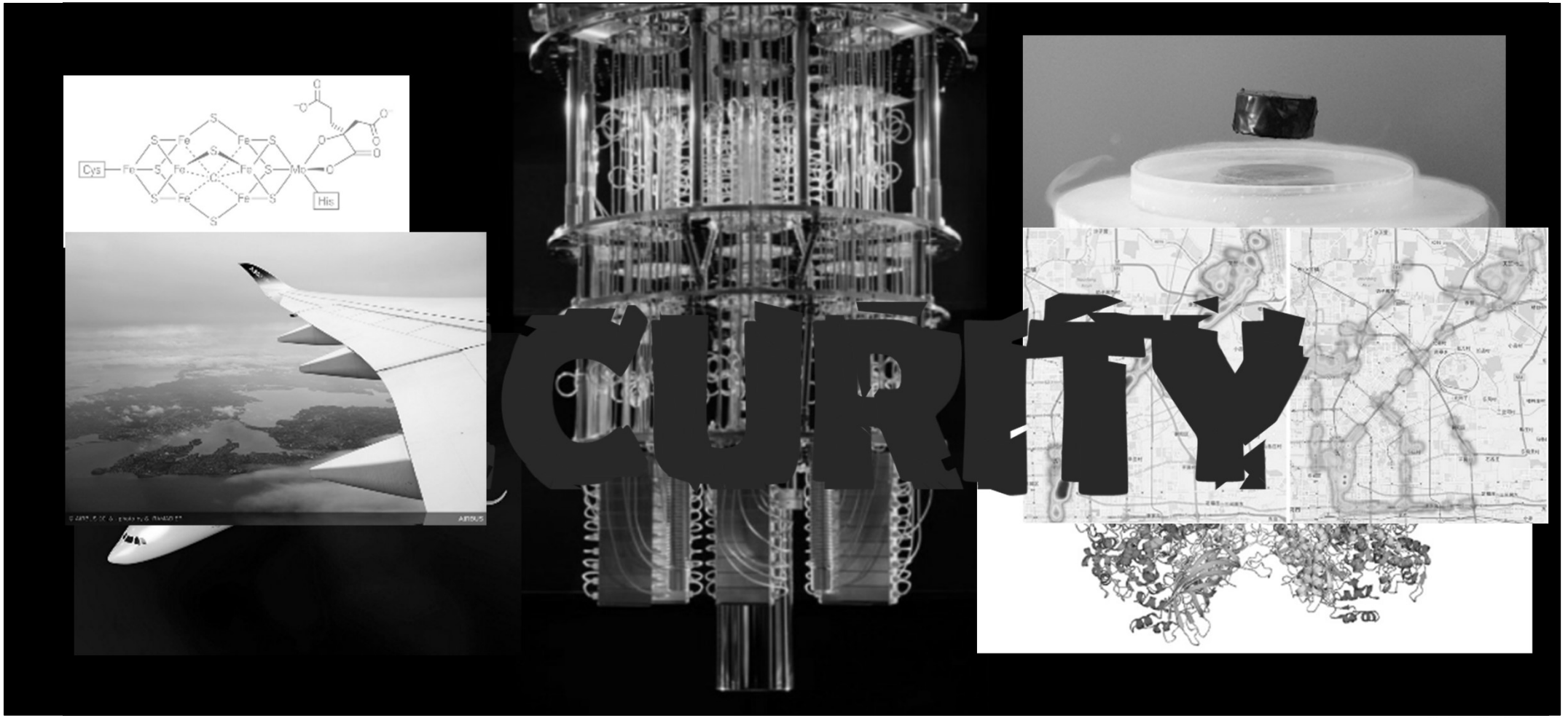
KEYNOTE: Quantum Secure Space Systems

DEFENCE AND SPACE

Johanna Sepúlveda, Ph.D.
Expert Post-Quantum Secure Communications
Chief Engineer Quantum Secure Communications

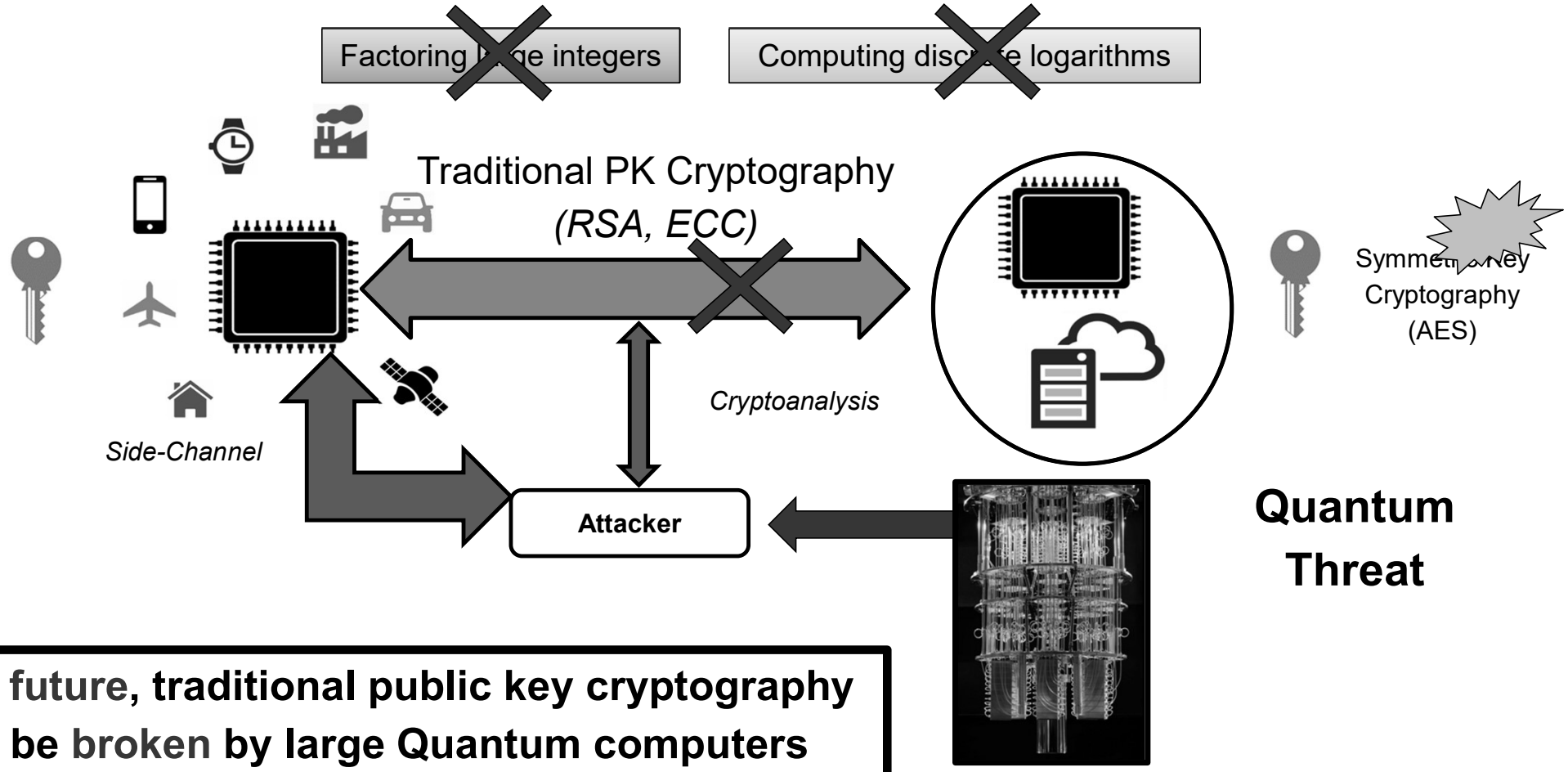
AIRBUS

Quantum Computer



AIRBUS

Traditional Security is under Threat



In the future, traditional public key cryptography will be broken by large Quantum computers

AIRBUS

Quantum-secure systems: Long Term Security

MIT Technology Review — February 3, 2016

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

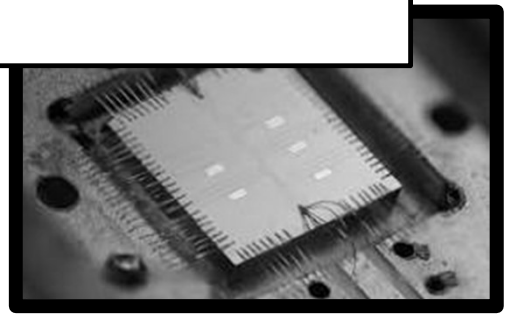
www.technologyreview.com

30

Life cycle of the product (Years)

Expose industry and products to attacks

Encrypted information can be stored today to be decrypted tomorrow



Risk and Opportunities

AIRBUS

Quantum-Secure Solutions

Post-Quantum Secure Communication Technologies

1. Quantum Key Distribution (QKD)

2. Post-Quantum Cryptography (PQC)

Quantum Key Distribution (QKD)

Still Immature (TRL5 2024)

AIRBUS

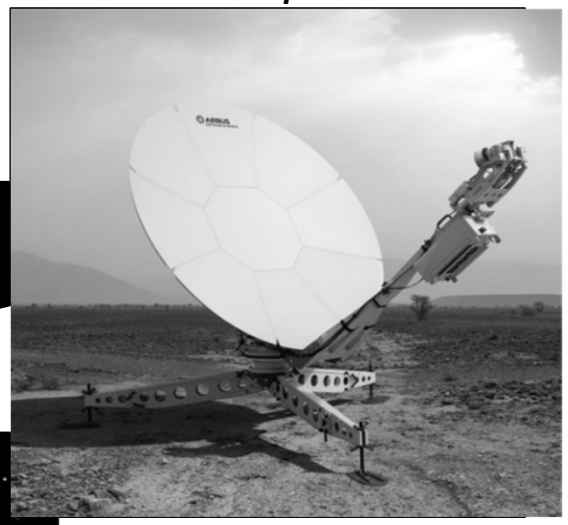
Quantum-Secure Technologies

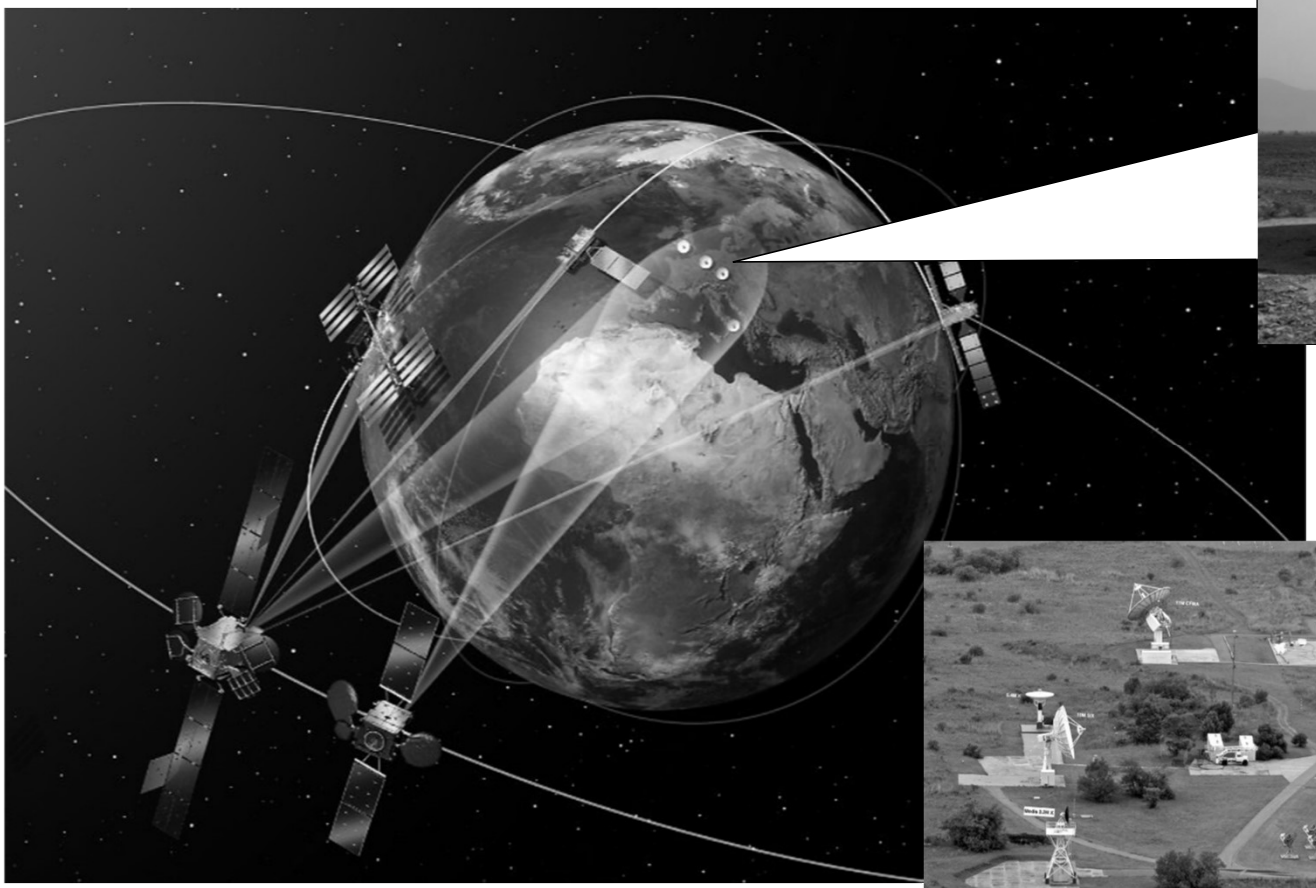
- **PQC** and **QKD are not competing**
- **PQC** and **QKD** can **work together**
- Two security technologies with different properties
- They can cover the security needs of a **wide variety of applications**

Transition: Layered approach (different layers of protection)

Space System

Ground portable terminals





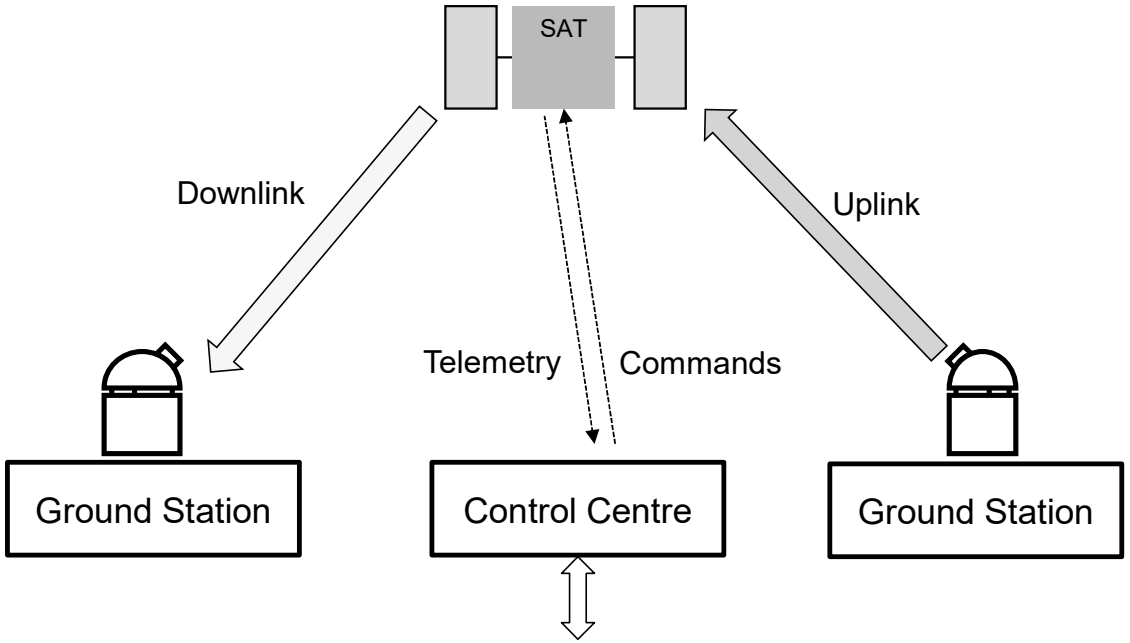
Ground segment

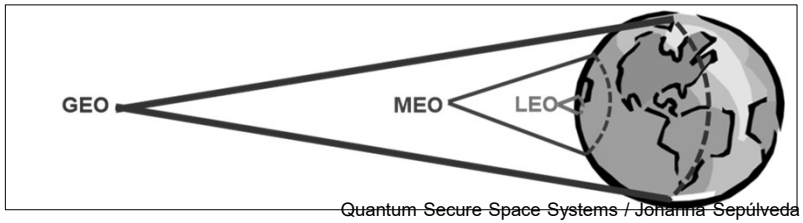
Antennas, Ground stations, Control/support centres (process, display, monitor) ..

AIRBUS

Security in Space Today

- **Exchange different type of data**
  Application data, commands and telemetry information
- **Different orbits**
  Impact on coverage and communication latency
- **Secure Channels**
  - Symmetric Cryptography
  - Pre-shared keys





Space Today: Improve life on Earth and beyond

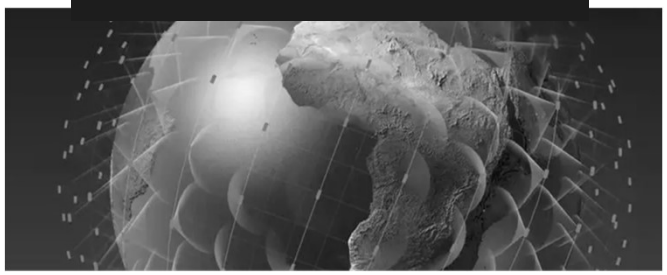
https://www.airbus.com/en/products-services/space

Earth Observation

Monitor land, sea and the atmosphere

Telecommunication

Reliable and high-performance relay satellites



Navigation

Position, Navigation and Timing (PNT) solutions for all applications

Performance

Memory footprint

Crypto-agility

Complexity

Reliability

Security

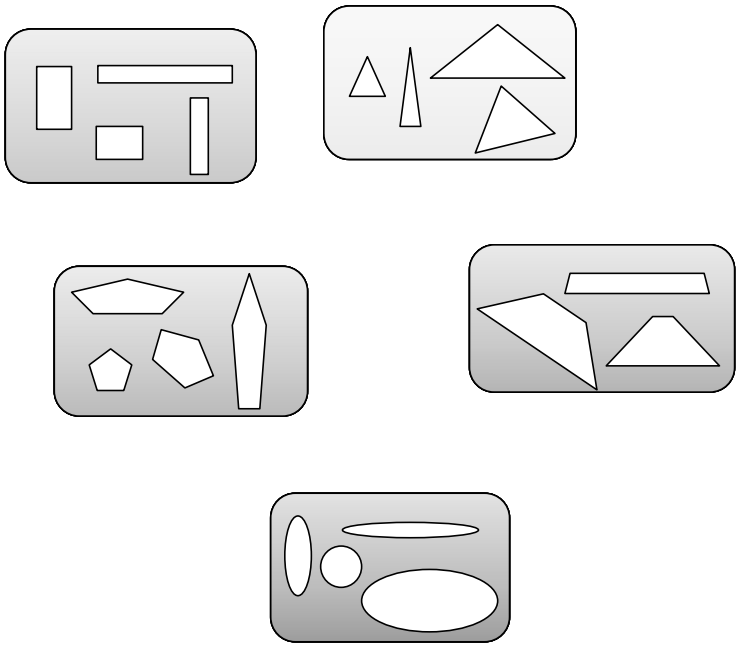
Power

AIRBUS

Post-Quantum Cryptography for Space

AIRBUS

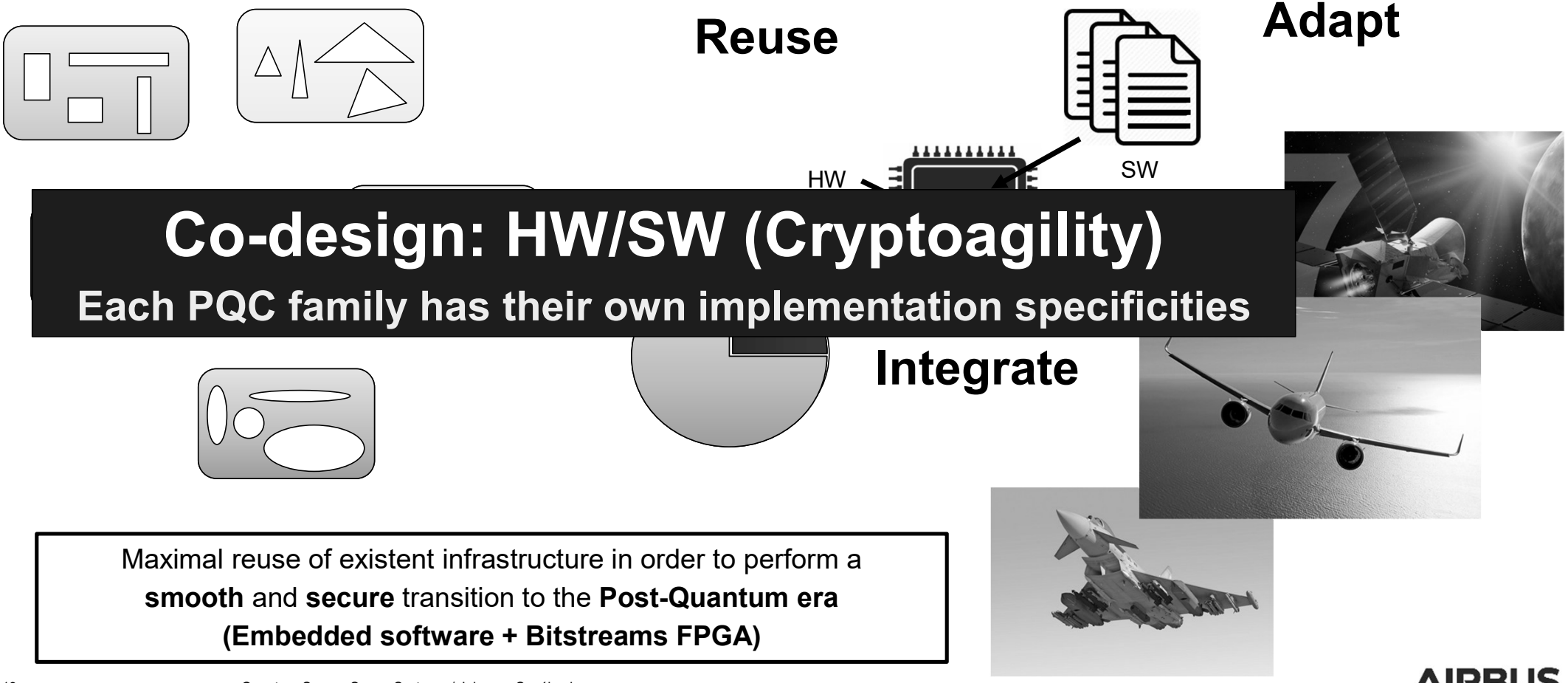
Challenge 1: **Algorithm Selection and Use Cases (Protocols)**



Performance	Security	Complexity	
Memory footprint	Reliability		Power

AIRBUS

Challenge 2: **Efficient and Secure Update**



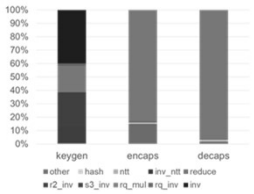
Co-design: HW/SW (Cryptoagility)

Each PQC family has their own implementation specificities

Maximal reuse of existent infrastructure in order to perform a **smooth** and **secure** transition to the **Post-Quantum era (Embedded software + Bitstreams FPGA)**

AIRBUS

NIST PQC Roadmap and Airbus Initiatives



Airbus: First PQC-codesign HW/SW (Crypto-agility)

Airbus: Contribution of Concept PQC-chip

Technical University of Munich

Airbus: Record implementation of advanced cryptoprimitives

April 2016: NISTIR 8105 report

December 2017: First-round candidates announced

July 2019: Second-round candidates announced

July 2020: Third-round schemes announced

Mid 2022: Third-round results; round four begins

2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Future

Dec 2016: Formal call for submissions

Nov 2017: Deadline for submissions

April 2018: First NIST PQC standardization workshop

August 2019: Second NIST PQC standardization workshop

June 2021: Third NIST PQC standardization workshop

2023–202 Draft standar available for schemes selecte after third round

Airbus: Ultraconstrained PQC solution

Airbus: First PQC-enhanced Wireless sensor network

Airbus: Record on PQC Implementation (performance, power, memory footprint)

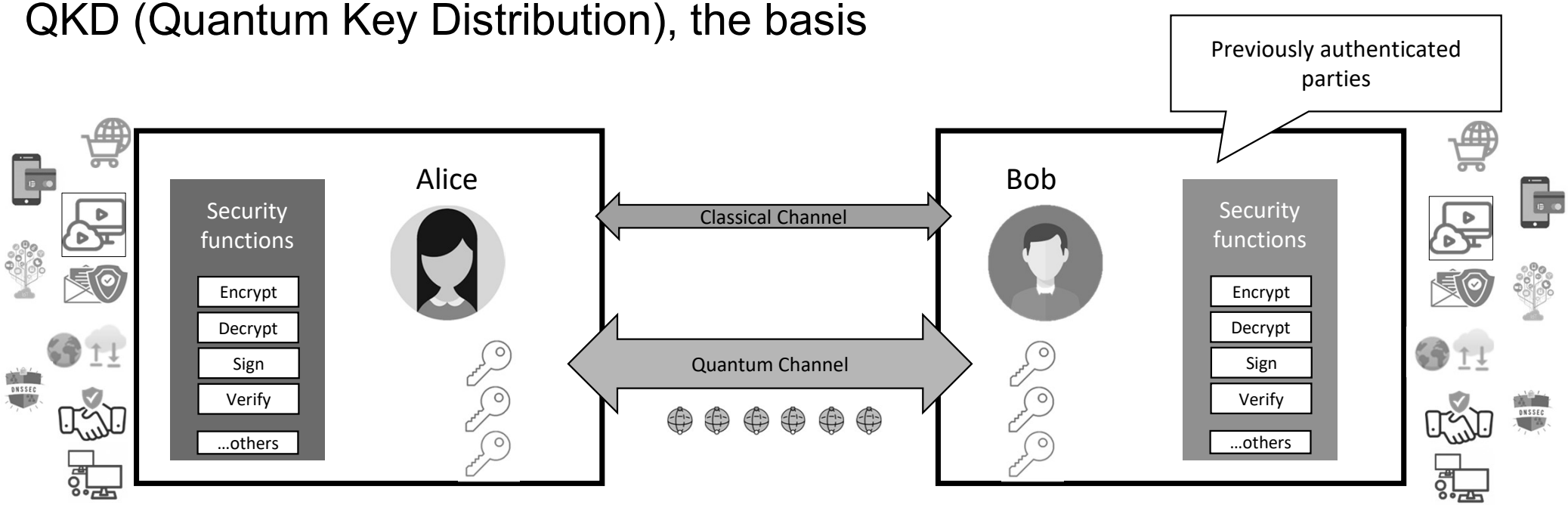
Airbus: Development of advanced PQC-enhanced systems Space, dynamic networks, blockchain

AIRBUS

Quantum Cryptography IN Space

AIRBUS

QKD (Quantum Key Distribution), the basis



The security depends on no computational assumptions

QKD allows to establish keys in a very secure way at both sites

- Information ways not copied
- Nobody spied the channel

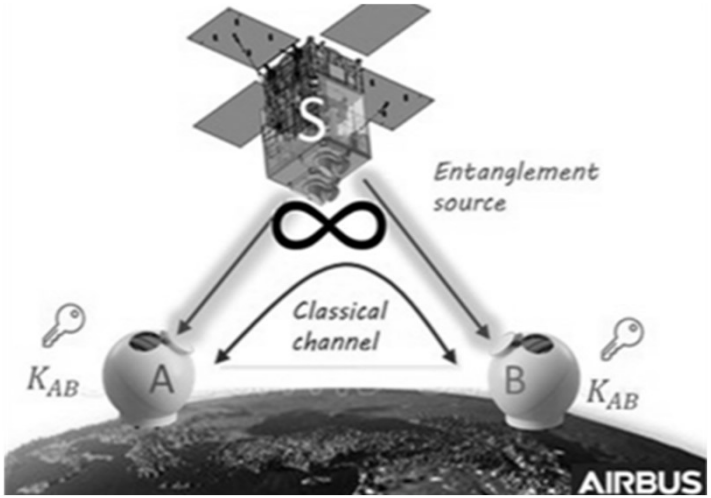
AIRBUS

QKD in Space

To deliver keys between different communication parties (identical, private)

- **Terrestrial**: Optical fibre or free-space ground-to-ground optical links
  Higher throughput, limited coverage *(maximum distance between consecutive nodes is 100km)*
- **Space**: free-space satellite links
  Low throughput but high coverage *(LEO)*

Protocol 1: Prepare and Measure

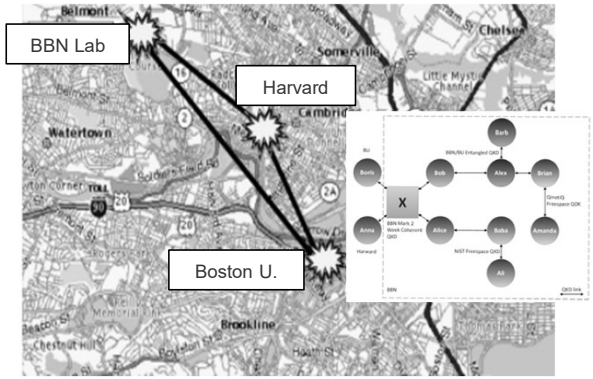


Protocol 2: Entanglement

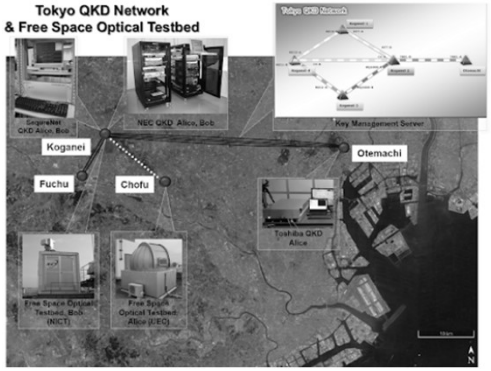
AIRBUS

Worldwide Demonstrations (terrestrial)

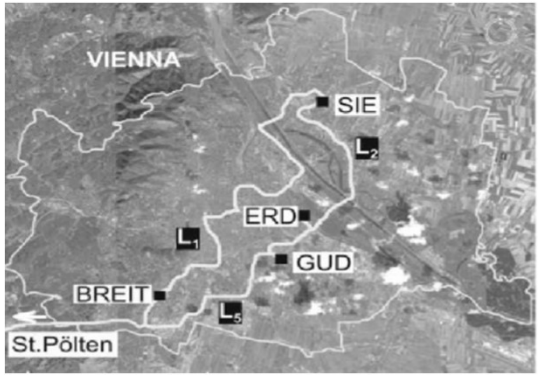
DARPA (2002)



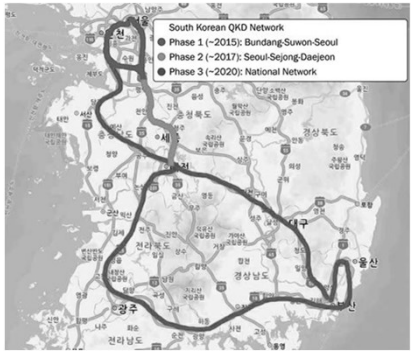
TOKYO (2009)



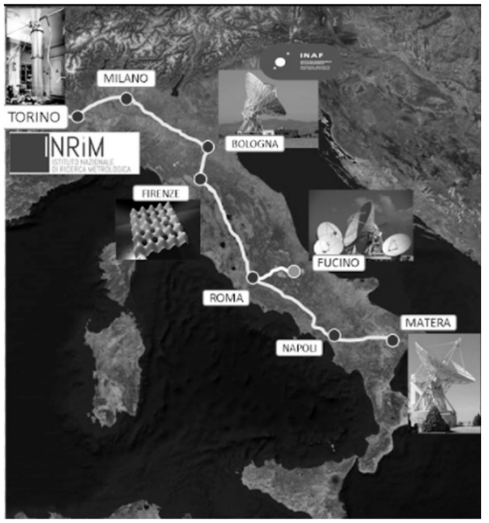
CAMBRIDGE (2019)



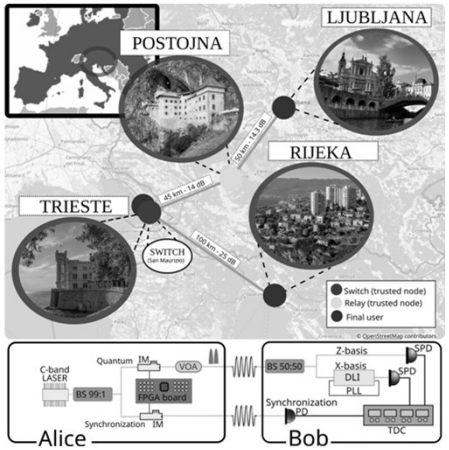
SECOQC (2008)



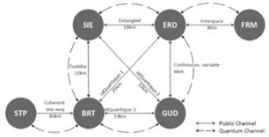
SOUTH KOREA (2015, 2017, 2020)



ITALY-IQB INRIM CNR (2018)

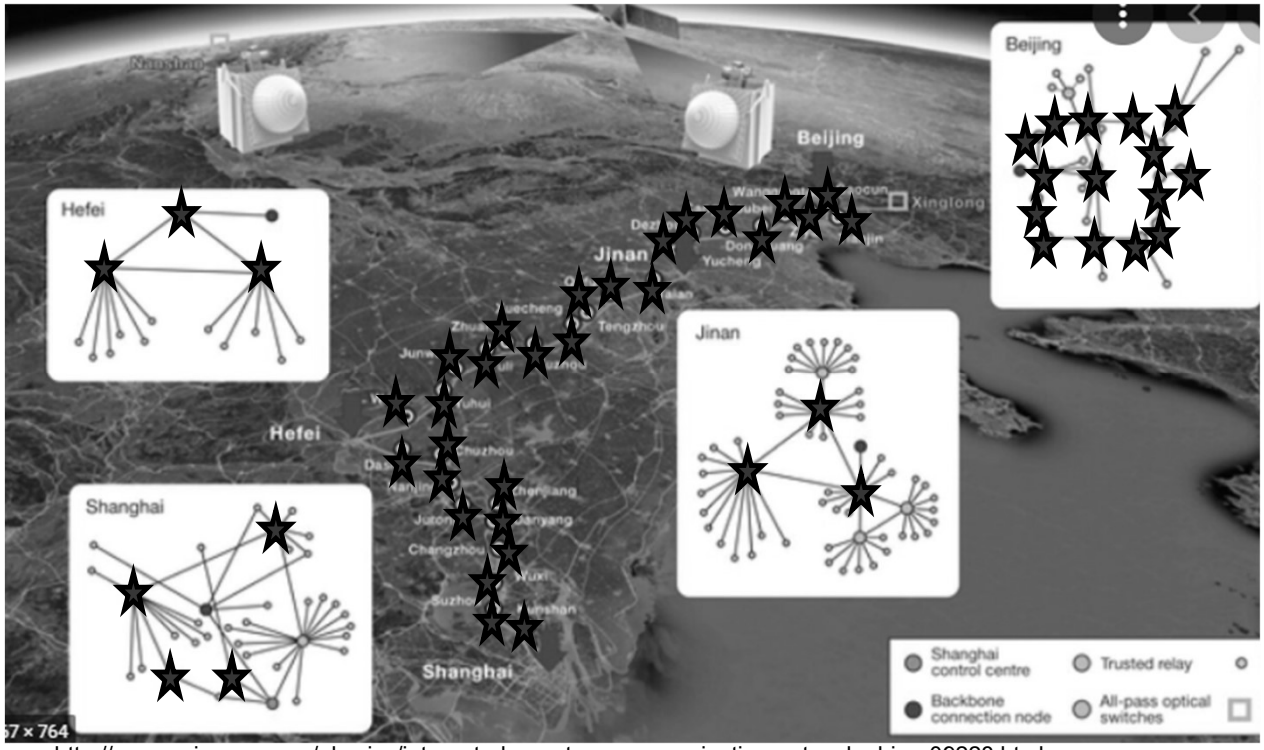


ITALY-SLOVENIA-CROATIA (2021)

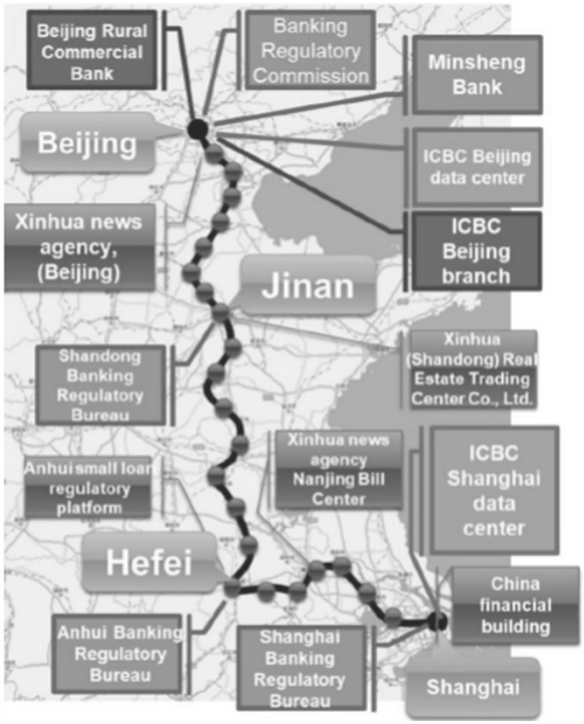


AIRBUS

Chinese QKD Network: Terrestrial And Space QKD



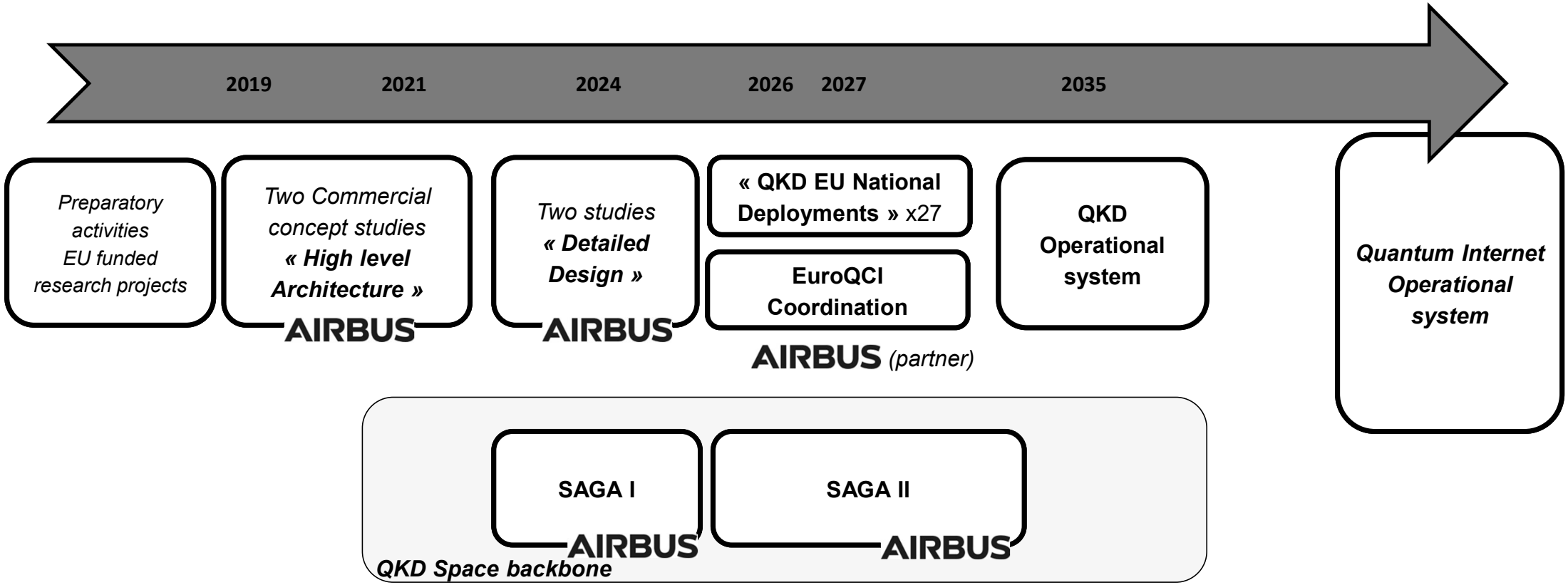
http://www.sci-news.com/physics/integrated-quantum-communication-network-china-09228.html



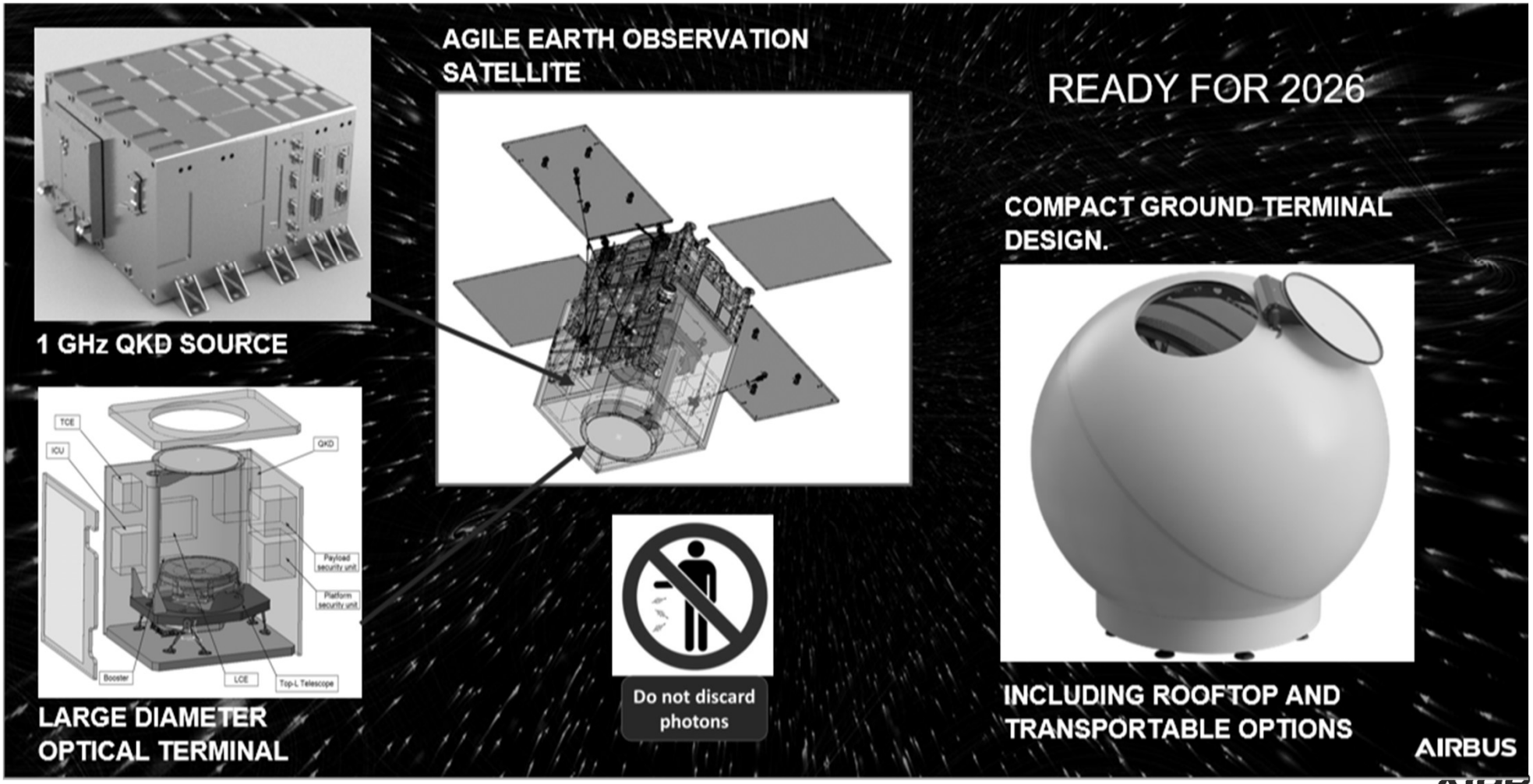
- Spanning Beijing to Shanghai (2000 km)
- Extended to 4600 km by use of free space QKD links
- Fibre losses limit distance between nodes to ~100 km
- Dedicated fibre network with **more than 30 trusted** nodes and 700 fibres

AIRBUS

Quantum-crypto at **AIRBUS: EuroQCI (EC) and SAGA (ESA)**



AIRBUS HIGH CAPACITY QKD SATELLITE - QUBISAT

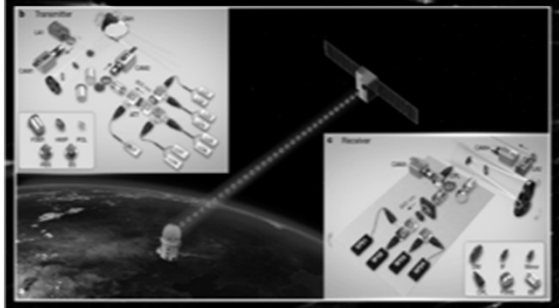


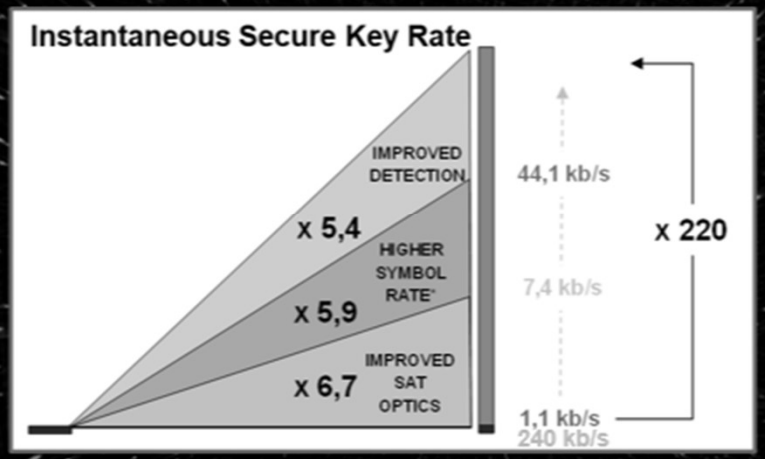
AIRBUS

AIRBUS HIGH CAPACITY QKD SATELLITE - QUBISAT

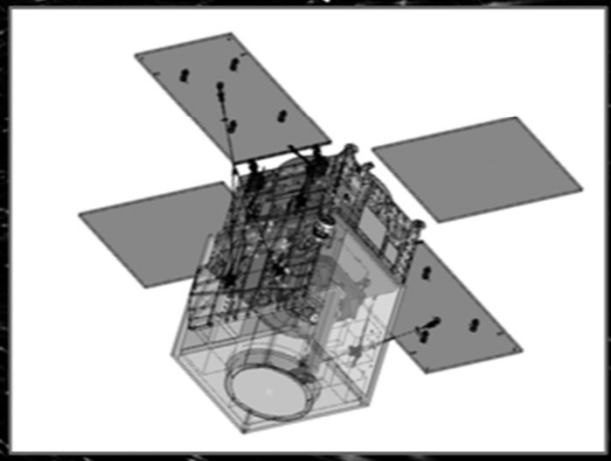
Comparison with State of the Art

SCIENTIFIC MISSION
MICIUS





OPERATIONAL SYSTEM
AIRBUS QUBISAT

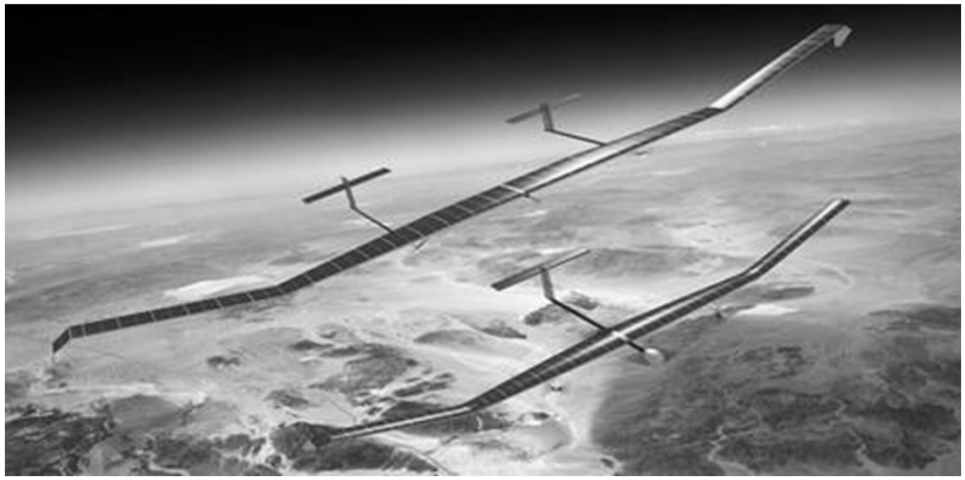


X220 performance improvement at link level
X700 performance improvement at system level (with realistic key demands and satellite scheduling included)

AIRBUS

AIRBUS

Looking to the future: Extended Space/Airborne QKD (HAPS and Drones)



Thank you

johanna.sepulveda@airbus.com

Post-Quantum Cryptography (PQC) Types

Code-based

(e.g. McEliece, Rollo)

Pros:

- Well studied error correcting codes
- Multipurpose
- Fast

Cons:

- Very large key sizes

Hash-based

(e.g. Merkle Hash-trees)

Pros:

- Security relies on hash functions
- Very efficient

Cons:

- No encryption schemes
- Track of signed messages

Multivariate

(e.g. Rainbow, LUOV)

Pros:

- Multipurpose
- Very efficient for signature schemes

Cons:

- Most public key schemes are broken

Isogeny

(e.g. SIKE)

Pros:

- Elliptic-based
- Smallest key sizes

Cons:

- Low efficiency
- Difficult to construct

Lattice-based

(e.g. NTRU, LWE, RLWE)

Pros:

- Efficient
- Public key, digital signatures, FHE, IBE

Cons:

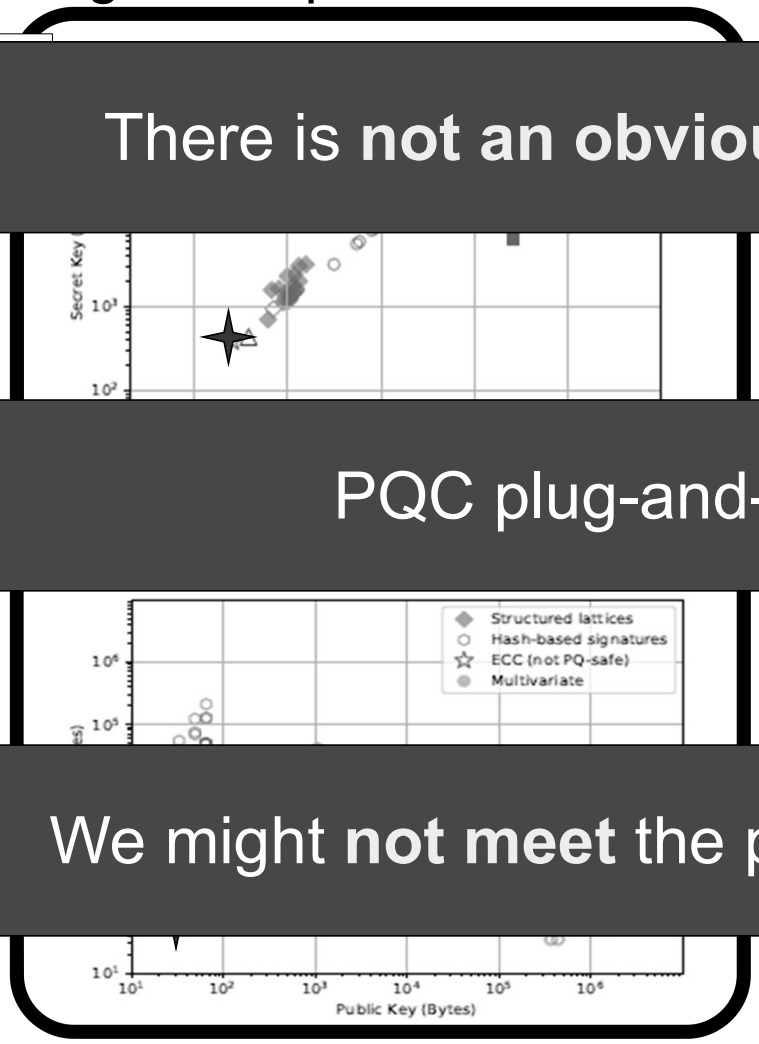
- Key sizes when compared to classical crypto

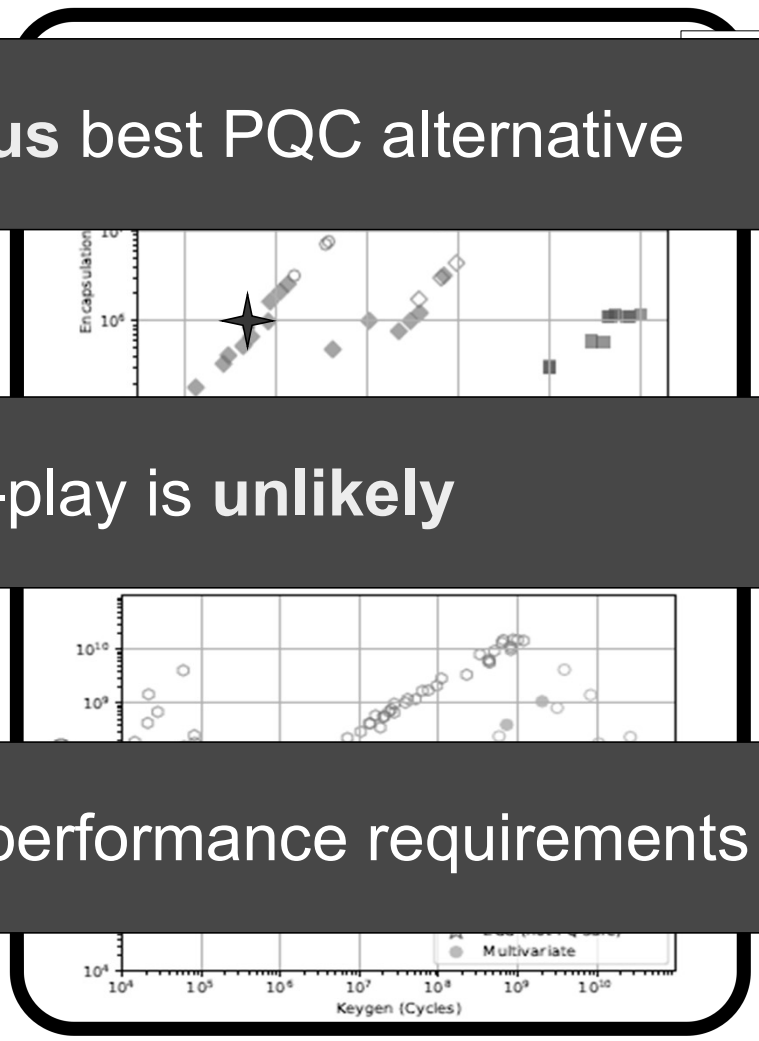
Benchmarking “Example”

There is **not an obvious** best PQC alternative

PQC plug-and-play is **unlikely**

We might **not meet** the performance requirements

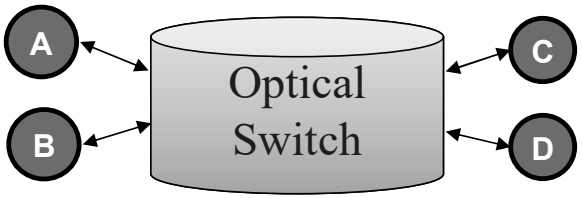




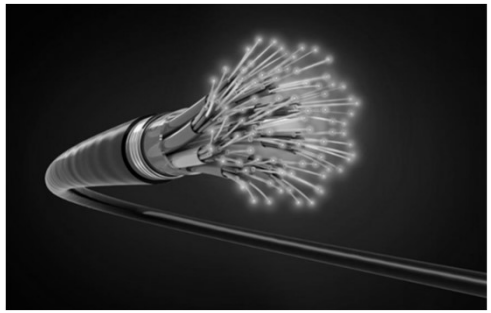
QCI: Towards extending the communication range

Short Range

Switched



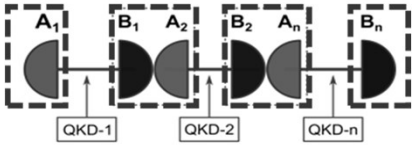
Optical Fibre



Up to 100Km

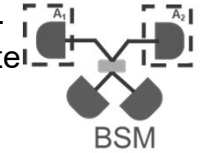
Medium Range

Trusted Nodes: QKD node (quantum receiver/transmitter) hosted in a **secure boundary**



Trusted-less Nodes:

MDI: Includes two transmitters and a receiver (which can be untrusted). The receiver performs the Bell State Measurement



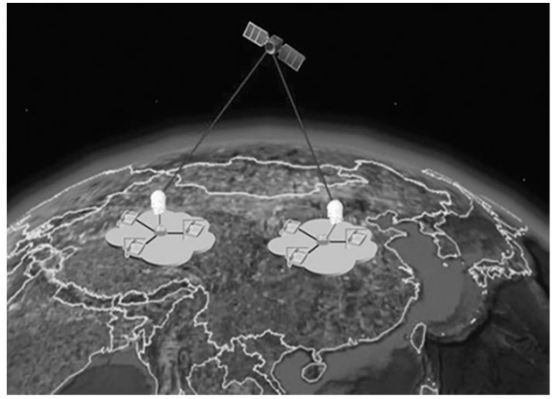
Entanglement Guarantees that the system is secure against loopholes in the source.

Quantum Repeaters: In development by research institutions

Up to 600Km

Long Range

Satellite



Used to cover high distances: > 2000 Km