Practical Quantum Computing

Lecture 6
Quantum Key Distribution (QKD)

based on *Quantum Computing:Lecture Notes* by Ronald de Wolf https://homepages.cwi.nl/~rdewolf/qcnotesv2.pdf

Week	**Tuesday** (3h)			**Wednesday** (3h)			**Deadlines**	
1. The Basics	Introduction	Gates	Circuit Identities	Qiskit	Cirq/Qualtran	Q&A		
	Programming Assignment 1: The basics of a quantum circuit simulator			**Programming Assignment 1:** The building blocks of a quantum circuit simulator				
2. Entanglement and its Applications	Teleportation	Superdense Coding	Quantum Key Distribution	Qualtran/ Assignment2	Terminology of Projects	Q&A		
	Programming Assignment 2: The basics of a quantum circuit optimizer			**Programming Assignment 2:** The building blocks of a quantum circuit optimizer				
3. Computing	Phase Kickback and Toffoli	Distinguishing quantum states and The First Algorithms	Grover’s Algorithm	Invited TBA	PennyLane	Q&A		11 May 2024
4. Advanced Topics*	Arithmetic Circuits*	Fault-Tolerance*	QML*	Invited TBA	Crumble	Q&A	18 May 2024	

* not evaluated

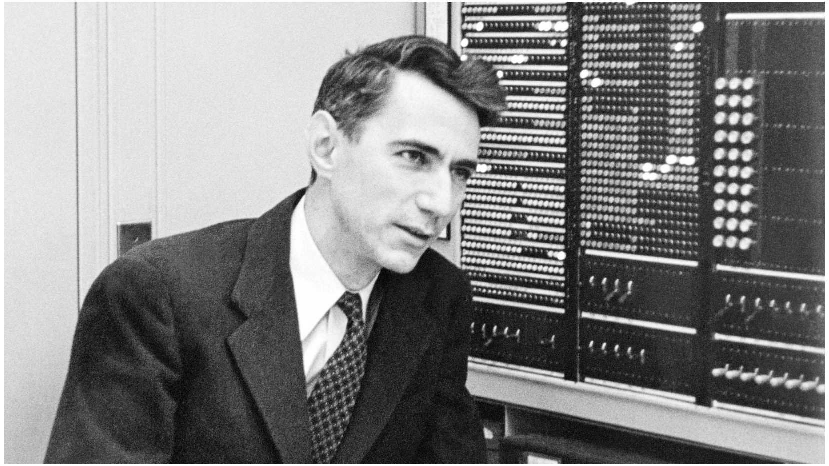
Learning goals - 06 Quantum Key Distribution (Entanglement)

1. What you have learned by now
   a. Quantum circuits: mathematics, diagrams and circuit identities
   b. Entanglement: teleportation, superdense coding, more powerful correlations and winning games by using entanglement
2. **Quantum Key Distribution**
   a. The One Time Pad for hiding classical information
   b. Using secret keys for hiding classical information
   c. Using quantum effects for building and sharing secret keys
   d. The first algorithms - BB84 and its functionality
3. **Quantum Key Distribution Networks**
   a. Architecture of such networks
   b. Quantum repeaters - building entanglement between very distant network nodes
   c. Examples: the Chinese QKD network and drones for QKD

In the exercise session and programming assignment of this week

- basics of quantum circuit optimization
- build our own quantum circuit optimizer
- benchmark your optimizer

One-Time Pad (OTP)

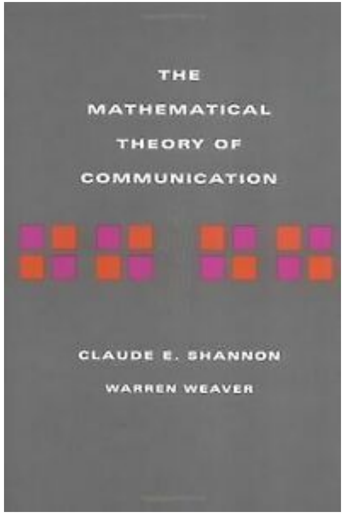


Encrypt a secret message with a *random key is as long as the message itself*

- cipher will not be crackable.
- communication partner must have the same key
- cannot use the same key twice

If Alice and Bob:

- share a secret key $K \in \{0,1\}^n$
- Alice can send $C = M \oplus K$ over the channel
- Bob learns M by adding K to what he received $C = (M \oplus K) \oplus K$
- if Eve didn't know anything about K then she learns nothing about M from tapping the message $M \oplus K$ that goes over the channel.



THE MATHEMATICAL THEORY OF COMMUNICATION

CLAUDE E. SHANNON

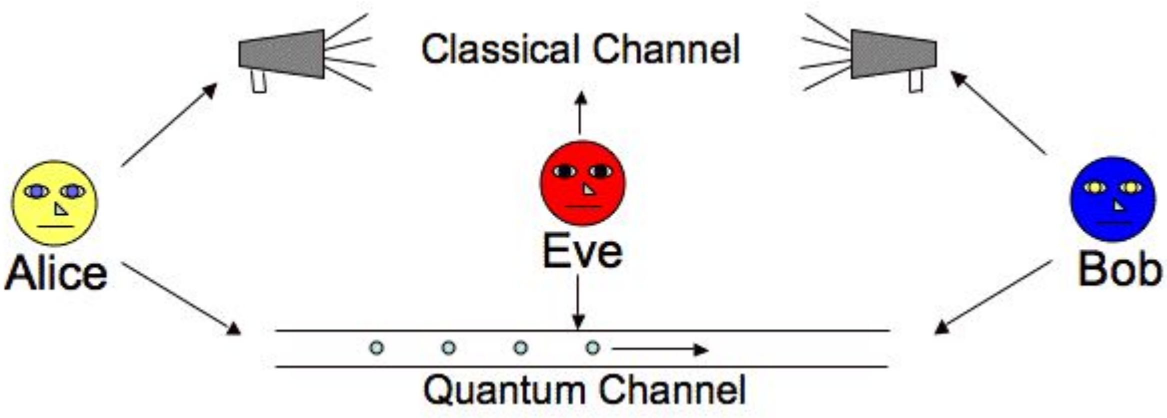
WARREN WEAVER

Quantum Key Distribution

How do you distribute a secret key without meeting in person?

The basic model for QKD protocols involves two parties

- wishing to exchange a key
- both with access to a classical public communication channel
- a quantum communication channel.

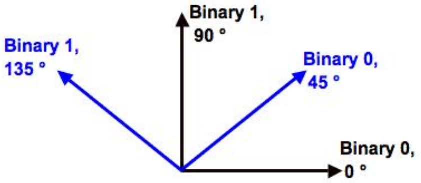


Fundamental: Eve cannot eavesdrop without affecting the qubit stream between Alice and Bob.

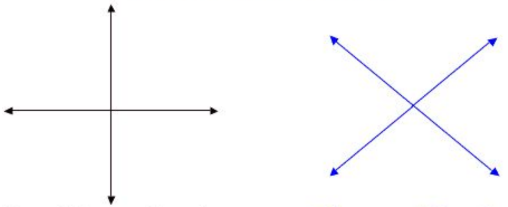
BB84: Bennett and Brassard 1984

The main property of quantum mechanics that we'll use:

- if a bit b is encoded in an unknown basis
- Eve cannot get information about b without disturbing the state
- the latter can be detected by Alice and Bob



Photon Polarization



Consider two possible bases:

- 0: Z basis is the computational basis |0〉,|1〉
- 1: X basis is the Hadamard basis |+〉,|−〉

BB84 protocol:

1. Alice chooses n random bits $a_1,...,a_n$ and n random bases $b_1,...,b_n$.
   a. She sends a_i to Bob in basis b_i over the public quantum channel
   b. For example, if $a_i = 0$ (value) and $b_i = 1$ (basis) then the ith qubit that she sends is in state |+〉
2. Bob chooses random bases $b'_1,...,b'_n$
   a. measures the qubits he received in those bases
   b. yielding bits $a'_1,...,a'_n$

BB84: Bennett and Brassard 1984

3. Bob sends Alice all b'_i, and Alice sends Bob all b_i

   a. For roughly n/2 of the i's, Alice and Bob used the same basis $b_i=b'_i$
   b. For those i's Bob should have $a'_i=a_i$
      i. if there was no noise
      ii. Eve didn't tamper with the i-th qubit on the channel
   c. Both Alice and Bob know for which i's this holds
   d. Let's call these roughly n/2 positions the **shared string**

4. Alice randomly selects n/4 locations in the shared string, and sends Bob those locations as well as the value of a_i at those locations.

   a. Bob then checks whether they have the same bits in those positions
   b. If the fraction of errors is bigger than some number *p*, then they suspect some eavesdropper was messing with the channel, and they abort
   c. The number p can for instance be set to the natural error-rate that the quantum channel would have if there were no eavesdropper

Quantum Key Distribution

4. If the test is passed

    a. then they discard the n/4 test-bits,
    b. have roughly n/4 bits left in their shared string. This is called the **raw key**

5. Now they do some classical post processing on the raw key:

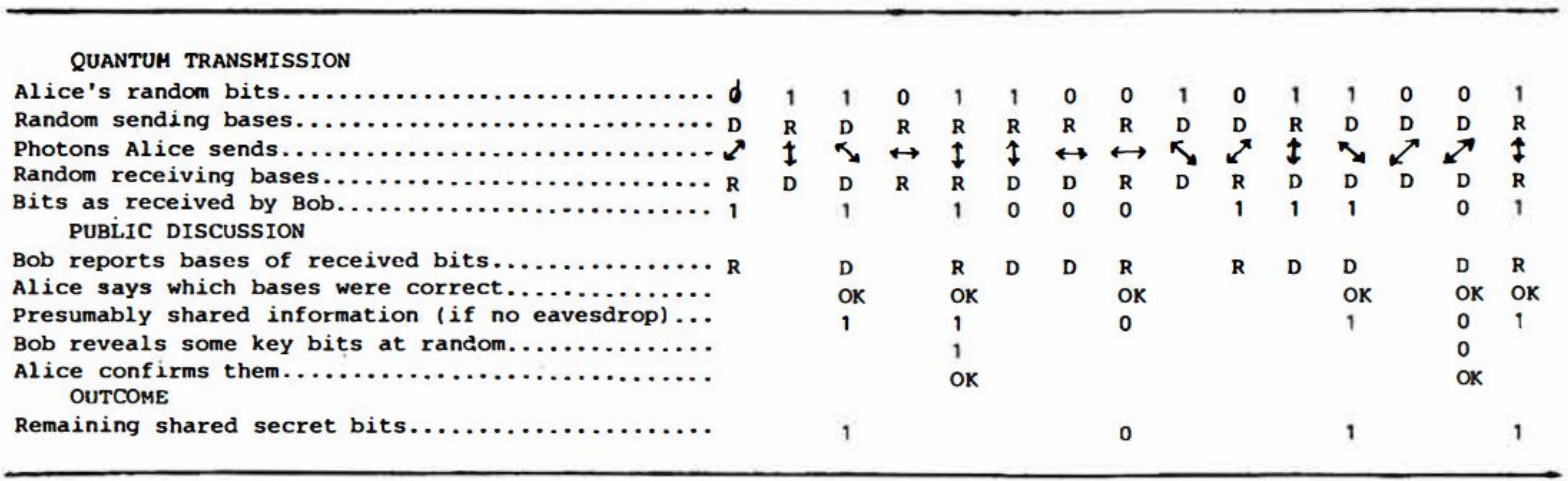
    a. “information reconciliation” to ensure they end up with exactly the same shared string
    b. “privacy amplification” to ensure that Eve has negligible information about that shared string

Might in fact better be called *quantum eavesdropper detection*

- Assume that the classical channel used in steps 3–5 is “authenticated”
    - Alice and Bob know they are talking to each other, and
    - Eve can listen but not change the bits sent over the classical channel
- In contrast to the qubits sent during step 1 of the protocol, which Eve is allowed to manipulate in any way she wants

https://homepages.cwi.nl/~rdewolf/qcnotesv2.pdf

BB84 - Example



QUANTUM TRANSMISSION															
Alice's random bits..................................	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases................................	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends...................................	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases..............................	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob..............................	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits..................	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct................			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)...			1		1			0				1		0	1
Bob reveals some key bits at random................					1									0	
Alice confirms them...................................					OK									OK	
OUTCOME															
Remaining shared secret bits........................			1					0				1			1

https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf

Learning goals - 06 Quantum Key Distribution (Entanglement)

1. What you have learned by now
   a. Quantum circuits: mathematics, diagrams and circuit identities
   b. Entanglement: teleportation, superdense coding, more powerful correlations and winning games by using entanglement
2. **Quantum Key Distribution**
   a. The One Time Pad for hiding classical information
   b. Using secret keys for hiding classical information
   c. Using quantum effects for building and sharing secret keys
   d. The first algorithms - BB84 and its functionality
3. **Quantum Key Distribution Networks**
   a. Architecture of such networks
   b. Quantum repeaters - building entanglement between very distant network nodes
   c. Examples: the Chinese QKD network and drones for QKD

In the exercise session and programming assignment of this week

- basics of quantum circuit optimization
- build our own quantum circuit optimizer
- benchmark your optimizer

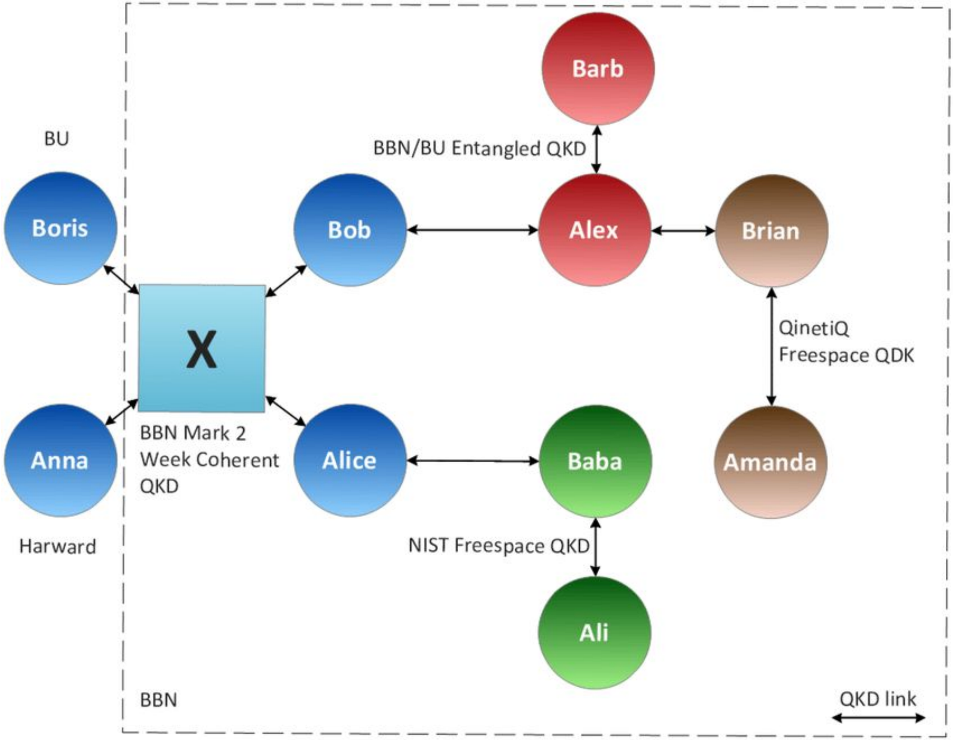
QKD Networks

DARPA QKD Network

- The world's first QKD network
- presented in December 2002 by BBN Technologies and Harvard and Boston Universities
- laid the foundation for the further development of trusted repeater QKD networks
- demonstrated practically the disadvantages of a *switched* QKD network type

The network consisted of:

- a weak-coherent BB84 transmitter pair (Anna and Alice)
- a pair of compatible receivers (Boris and Bob)
- one 2×2 optical switch to connect any sender to any receiver



https://dl.acm.org/doi/fullHtml/10.1145/3402192

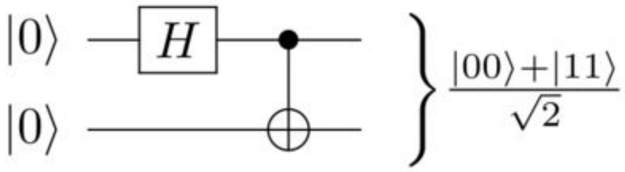
Entanglement Swapping

A ---- B   C ---- D   A and D can be arbitrarily distant, B and C next to each other

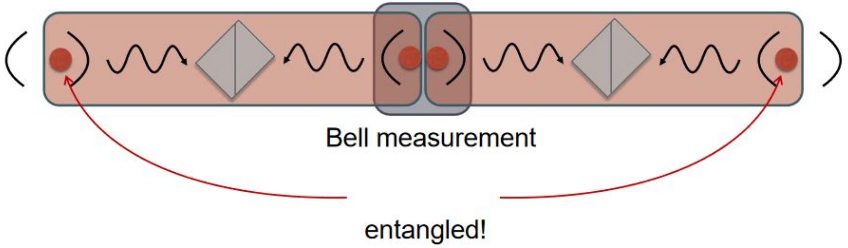
A ----------------D   After performing an operation on B and C -> A and D are entangled

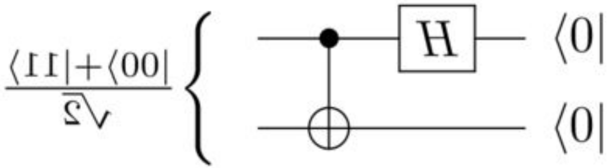
Quantum repeater networks

- make end-to-end entanglement
- entanglement is a consumable resource



Create Bell pair state

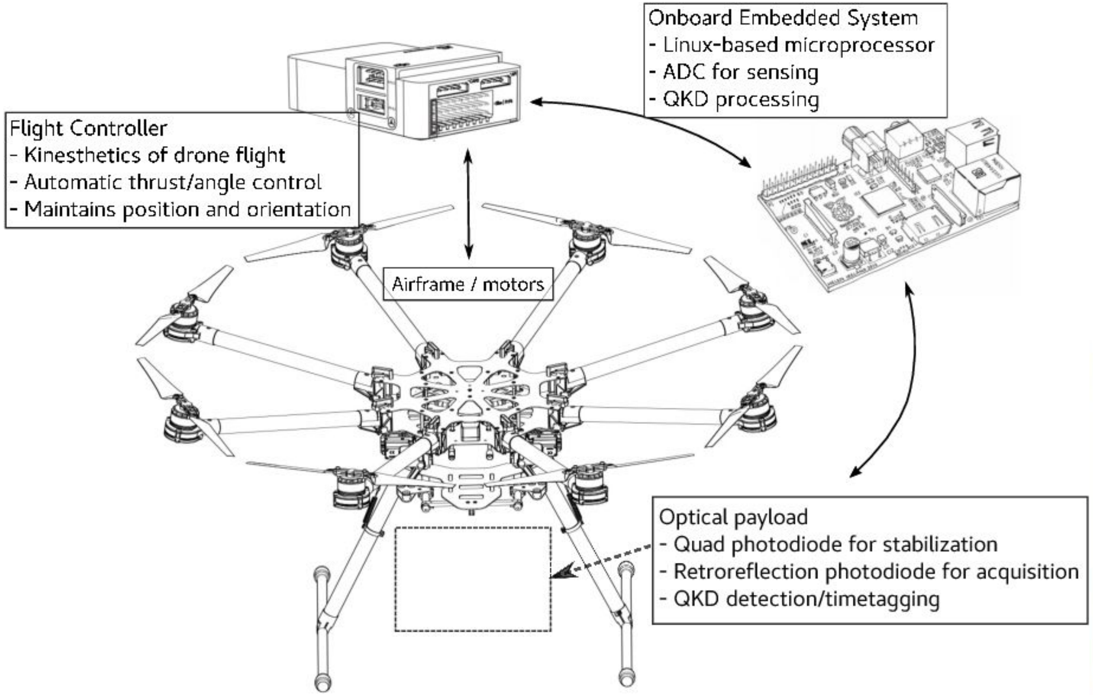




Inverse operation: Bell measurement

[vanMeter] https://datatracker.ietf.org/meeting/104/materials/slides-104-qirg-sessa-tutorial-on-quantum-repeaters-pdf-00

Drone-to-Drone QKD



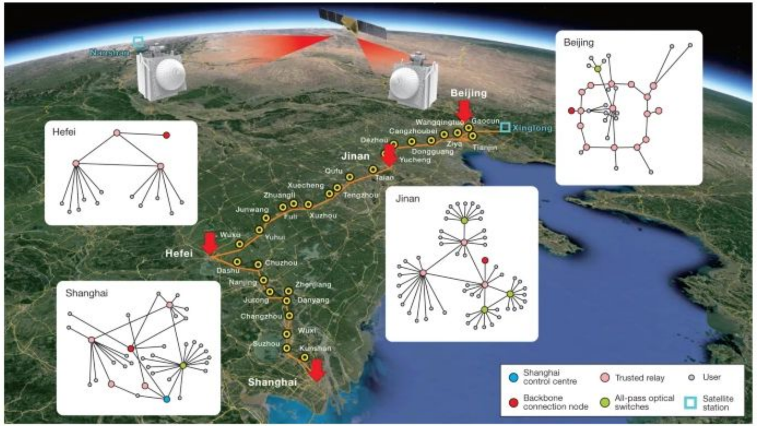
Onboard Embedded System
- Linux-based microprocessor
- ADC for sensing
- QKD processing

Flight Controller
- Kinesthetics of drone flight
- Automatic thrust/angle control
- Maintains position and orientation

Airframe / motors

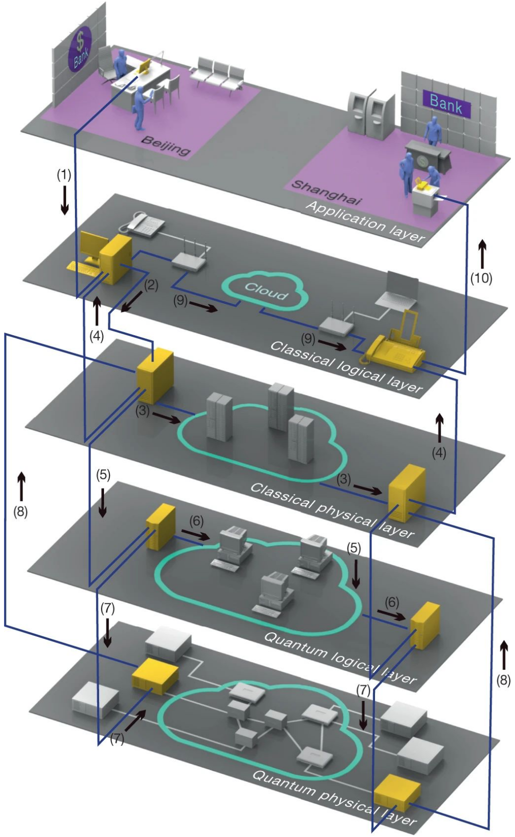
Optical payload
- Quad photodiode for stabilization
- Retroreflection photodiode for acquisition
- QKD detection/timetagging

An integrated space-to-ground quantum communication network over 4,600 kilometres



The network consists of four QMANs (in Beijing, Jinan, Shanghai and Heifei; red arrows), a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. There are three types of node in the network: user nodes (purple circles), all-pass optical switches (green circles) and trusted relays (pink circles). Each QMAN consists of all three node types (see insets). The backbone is connected by trusted relays (shown as yellow and black circles in the main image and red circles in the insets). A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre. In Beijing, the Beijing control-centre node is located at the same location as the backbone connection node (indicated by the red circle). Map data: Google, Data SIO, NOAA, US Navy, NGA, GEBCO, Landsat/Copernicus; copyright ZENRIN.

The network consists of five layers: the application layer, the classical logical layer, the classical physical layer, the quantum logical layer and the quantum physical layer. As an example, we consider how a secure transmission from Beijing to Shanghai works. The message transmission order is sent from the user in Beijing to the computer (1). The computer sends an order to the key management system to ask for the key (2) and to the router to find the classical route for classical information transfer (3). The key management system checks whether the key is sufficient. If it is, it sends the key to the computer (4); otherwise, it sends an order to the quantum system server to generate more keys (5). The quantum system server sends the order to the quantum control system (6), which finds the optimal key generation route and sends the order to generate keys (7). The keys are generated in the quantum physical layer and stored in the key management system (8). After encoding or decoding the message with the key (9), the information can be transferred securely to the user in Shanghai (10).


Bank
Bank
Beijing
Shanghai
Application layer
(1)
(2)
(9)
Cloud
(9)
(10)
(4)
Classical logical layer
(3)
(3)
(4)
(8)
Classical physical layer
(5)
(6)
(5)
(6)
Quantum logical layer
(7)
(7)
(7)
(8)
Quantum physical layer