quantum information

protocols and applications

radu ionicioiu

roqnet

outline

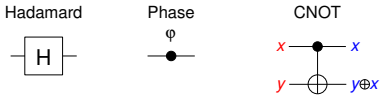
- I. the future is quantum
  overview of quantum technologies
- II. quantum information: foundations and entanglement
  qubit, quantum gates, entanglement
- III. quantum mechanics: protocols and applications
  teleportation, entanglement swapping, quantum cryptography

recap

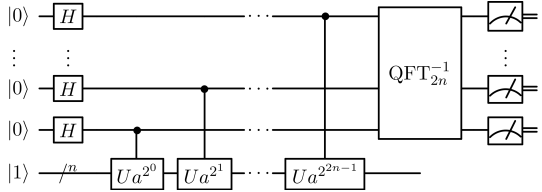
- **no-cloning**:
  an unknown q. state cannot be cloned

$$|\psi\rangle|0\rangle \xrightarrow{U} |\psi\rangle|\psi\rangle$$

- **universality**: $\{H, P_\varphi, CNOT\}$



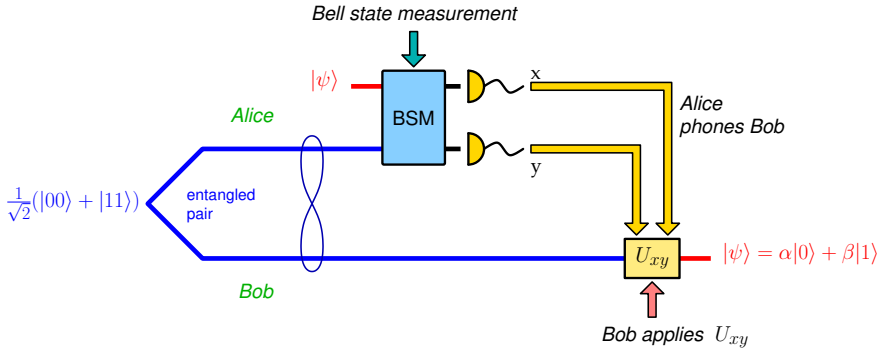
- **1- and 2-qubit gates**: building blocks to perform any q. algorithm



quantum protocols

teleportation

send an unknown state $|\psi\rangle$ over a quantum channel



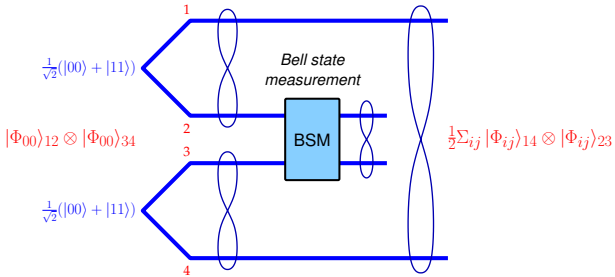
$$|\psi\rangle_1 \otimes |\Phi_{00}\rangle_{23} = \frac{1}{2}\{|\Phi_{00}\rangle_{12} \otimes |\psi\rangle_3 + |\Phi_{10}\rangle_{12} \otimes Z|\psi\rangle_3$$

$$+ |\Phi_{01}\rangle_{12} \otimes X|\psi\rangle_3 + |\Phi_{11}\rangle_{12} \otimes XZ|\psi\rangle_3\}$$

entanglement swapping

teleportation of entanglement

entangle 2 systems which never met using a quantum channel

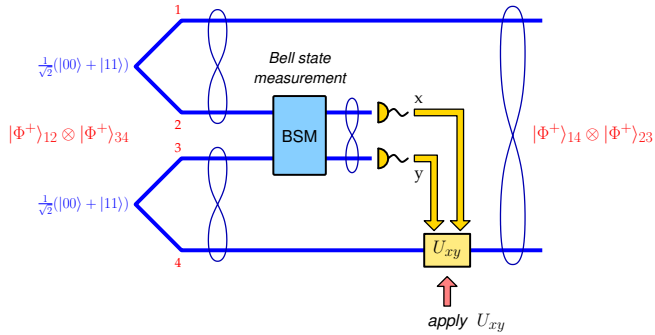


$$|\Phi_{00}\rangle_{12} \otimes |\Phi_{00}\rangle_{34} = \frac{1}{2} \sum_{ij} |\Phi_{ij}\rangle_{14} \otimes |\Phi_{ij}\rangle_{23}$$

entanglement swapping

teleportation of entanglement

entangle 2 systems which never met using a quantum channel



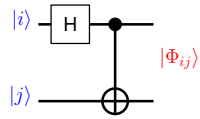
$$|\Phi_{00}\rangle_{12} \otimes |\Phi_{00}\rangle_{34} = \frac{1}{2} \sum_{ij} |\Phi_{ij}\rangle_{14} \otimes |\Phi_{ij}\rangle_{23}$$

summary

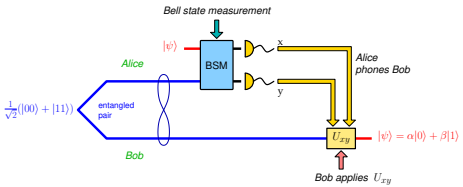
- "entanglement [...] *the characteristic trait of quantum mechanics*" (Schrödinger)
- both a mystery and a resource (... and much more)
- Bell states

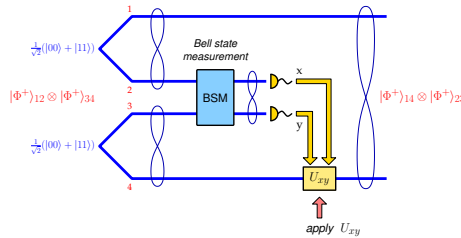
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$



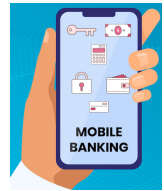
- teleportation, entaglement swapping





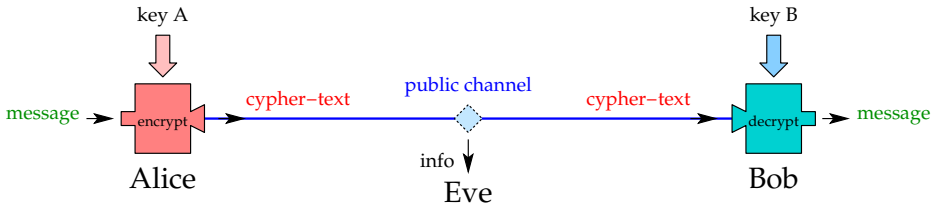
quantum communications

crypto: we use it every day



https://

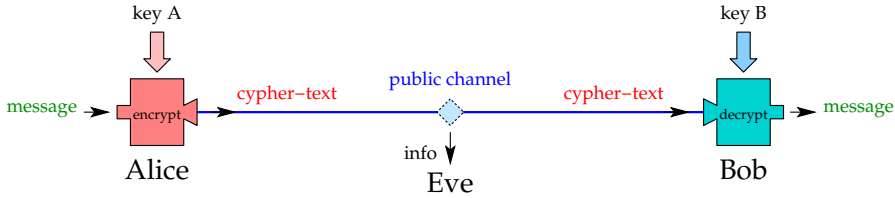
classical crypto



- symmetric: *key A = key B* — one-time pad (OTP), AES-256/512
- asymmetric: *key A ≠ key B* — public-key, RSA, DH
- authentication, digital signatures, privacy, security

public-key crypto

asymmetric crypto



key A ≠ *key B*

- encryption key: public (known by all)
- decryption key: secret (known only by the receiver)
- based on a hard problem: factoring (RSA), discrete log etc

the problem

quantum computers will break internet security

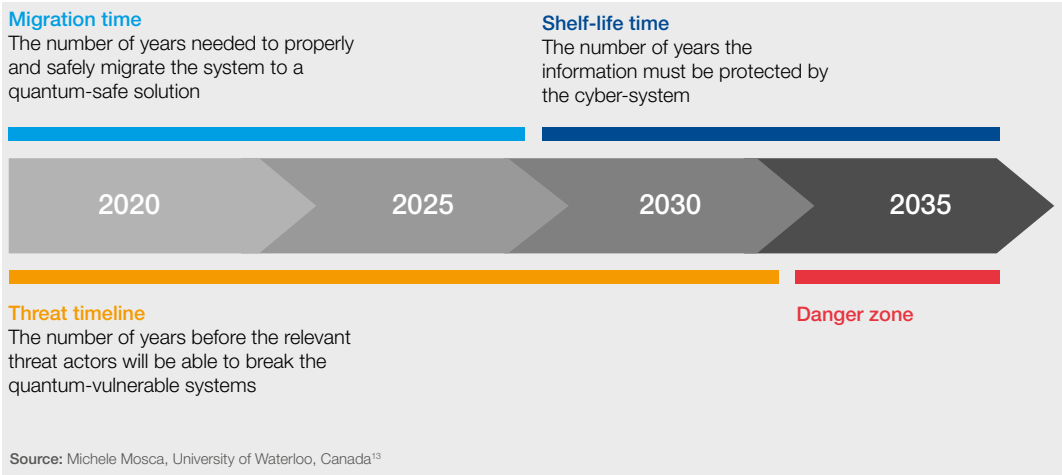
- secure communications
- digital signatures
- mobile networks
  5G, 6G, ...
- financial transactions
  mobile banking, POS, e-commerce
- authentication
- critical infrastructure
- blockchain
  bitcoin, ethereum, ...
- software updating
  cars, computers

$\Rightarrow$ *need to avoid the quantum apocalypse (Q-Day)*

how serious is the threat?

Mosca equation

"store now, decrypt later" (SNDL) attack

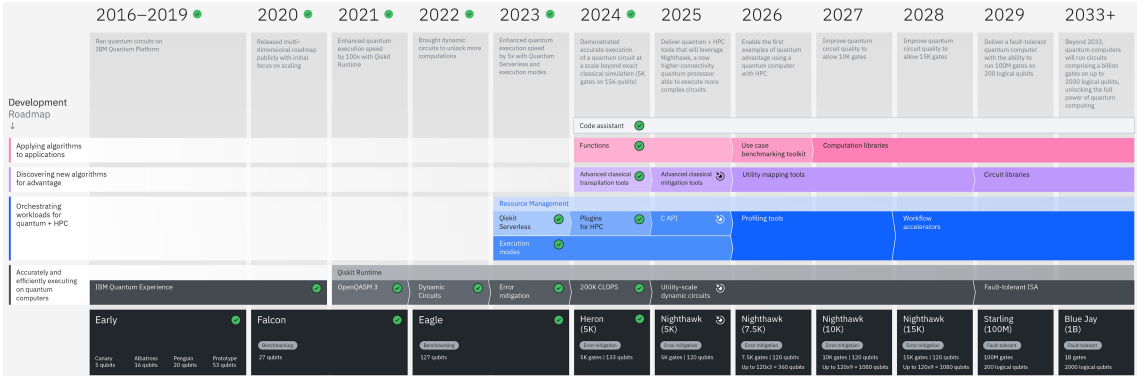


Source: Michele Mosca, University of Waterloo, Canada[13]

quantum computing

a $65 billion industry by 2030

IBM roadmap



... any solutions?

Q-Day

two ways out

1. the classical way: post-quantum crypto (PQC)

   find quantum-resistant, public-key classical algorithms $\Rightarrow$ *NIST PQC*

2. the hard way: quantum key distribution (QKD)

   use the power of quantum + symmetric crypto (AES, OTP)

PQC: status

NOT QUANTUM SAFE

RSA encryption

The hard problem:
Factoring large integers into prime numbers

Diffie-Hellman key exchange

Solving $g^a \bmod p = c$ for a, given g, p and c

Elliptic curve cryptography

Finding the relation between two points on an elliptic curve

QUANTUM SAFE

Lattice-based crypto

Finding the nearest point in a high-dimensional lattice

Code-based crypto

Decoding a certain kind of error-correcting code

Hash-based crypto

Inverting a function that maps an input of arbitrary length to a fixed-length sequence

QUANTUM SAFE?

Multivariate crypto

One scheme broken
February 2022
Solving systems of nonlinear equations in many variables

Isogeny-based cryptography

One scheme broken
July 2022
Finding a map that relates two elliptic curves

https://www.quantamagazine.org

NIST PQC

the finalists

- NIST: PQC selection 2017-2022

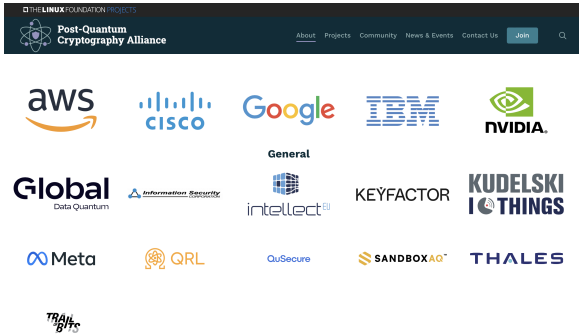
type	PKE/KEM	digital signature
lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
hash based		SPHINCS+
code based	HQC	

- standards: FIPS 203-205 (August 2024)
- HQC selected as backup KEM (March 2025)

what to do?

transition to quantum-resistant crypto

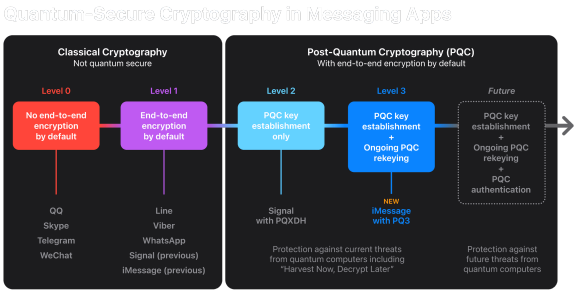
- replace public-key algorithms with quantum-resistant ones
- Bitdefender
- certSIGN

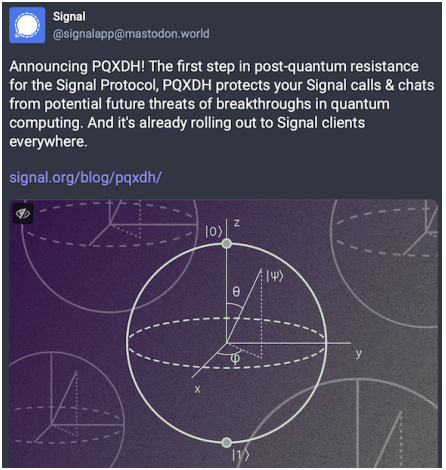


20 billion devices to be upgraded/replaced with PQC in the next 20 years

PQC: deployed

- signal protocol: enhanced by PQC
- : iMessages with PQ3





the quantum way: QKD

1. use quantum resources to securely distribute keys
2. use keys in symmetric crypto (OTP, AES etc)

quantum solves 2 problems:

- true (quantum) randomness
- secure key distribution
  eavesdropper detected

the quantum way: QKD

why does it work?

- no-cloning theorem $\Rightarrow$ Eve cannot clone an unknown quantum state
- measurement changes the state $\Rightarrow$ you listen, you leave a trace

Eve will be detected !

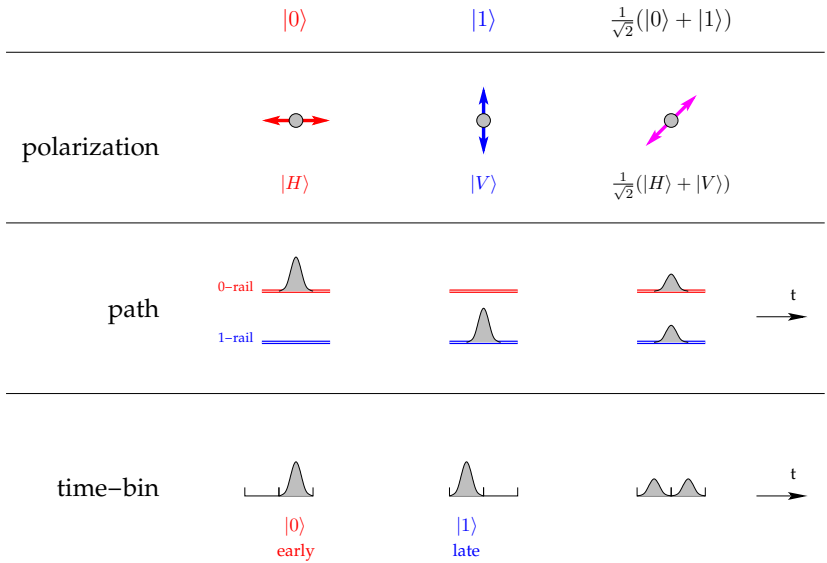
classically impossible

QKD protocols

classification

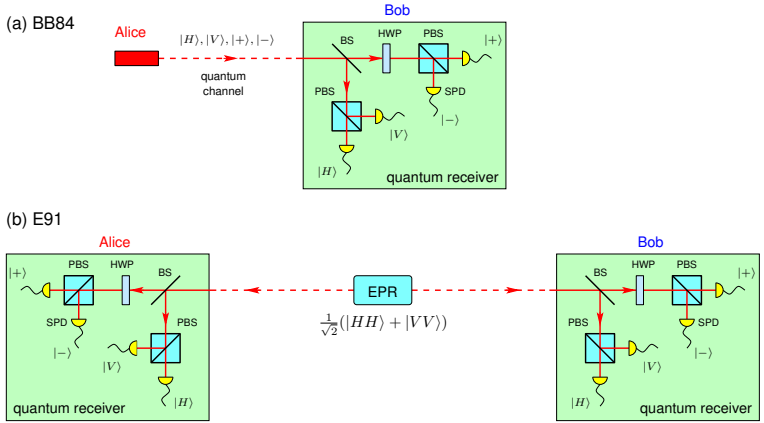
- qubit type: DV (discrete variables) vs. CV (continuous variables)
- protocol type: prepare & measure vs. entanglement-based
- qubit encoding: polarization, time-bin, OAM etc
- propagation medium: optical fibers, free-space, underwater
  EuroQCI will use the first two
- other: device-independent (DI-QKD), twin-field (TF-QKD) etc

encoding



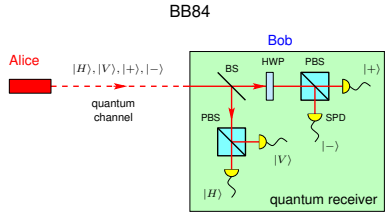
prepare & measure *vs.* entanglement-based

overview



prepare & measure: BB84

Bennett-Brassard 1984



- step 1: Alice prepares & sends to Bob single-photon states $\{|H\rangle, |V\rangle, |+\rangle, |-\rangle\}$
- step 2: Bob randomly measures in either H/V or $\pm$ basis
- step 3 (post-processing): Alice & Bob discuss on a authenticated public (= non-secured) classical channel in order to extract a common secure key

BB84

analysis

		Bob measures: Z-basis		X-basis	
		p_H	p_V	p_+	p_-
Alice sends	$\|H\rangle$	1	0	0.5	0.5
	$\|V\rangle$	0	1	0.5	0.5
	$\|+\rangle$	0.5	0.5	1	0
	$\|-\rangle$	0.5	0.5	0	1

- when is the state sent by Alice = state measured by Bob?
- if $basis_{Alice} = basis_{Bob} \Rightarrow |\psi_{Alice}\rangle = |\psi_{Bob}\rangle$
- need basis reconciliation

BB84

analysis

Alice sends	:	H	V	$-$	$-$	$-$	H	V	$+$	...
Bob measures	:	H	$+$	H	$+$	$-$	$+$	V	V	...
sifted key	:	0	X	X	0	1	X	1	X	...

post-processing (on authenticated public channel)

- basis reconciliation: keep only the bits when $basis_{Alice} = basis_{Bob}$ ($\sim$50% of bits discarded) $\Rightarrow$ sifted key
- compute QBER (quantum bit error rate)
- error correction, privacy amplification

BB84

analysis

why does it work?

- no-cloning theorem $\Rightarrow$ Eve cannot clone an unknown state
- two MUBs (mutually unbiased bases): $|b_i\rangle \in \{|H\rangle, |V\rangle\}$ and $|f_j\rangle \in \{|+\rangle, |-\rangle\}$

$$|\langle b_i | f_j \rangle|^2 = \frac{1}{2}$$

- measurement changes the state $\Rightarrow$ higher QBER, detectable

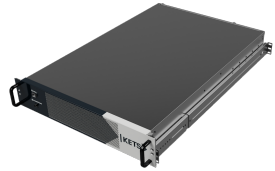
Eve can be detected !

classically this is impossible

QKD

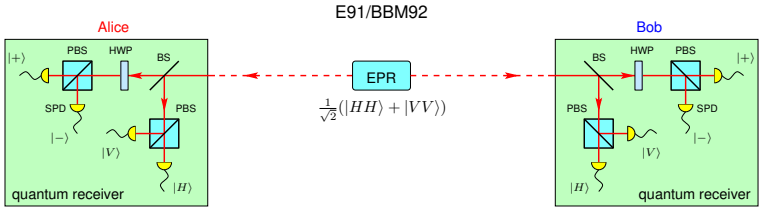
commercial

- EU27: idQuantique (IDQ), ThinkQuantum, QTI, KeeQuant, Quantum Optics Jena, LuxQuanta ...
  non-EU: Toshiba, Kets Quantum, Quintessence Labs, Qubitekk, QuantumCTek ...
- € 150-300 k/pair



entanglement-based QKD

E91, BBM92



- Alice & Bob both measure 1 photon (from the entangled pair)
- quantum receiver: same as in BB84
- postprocessing: basis reconciliation, error correction, privacy amplification
- violation of Bell inequality $\Rightarrow$ secure communication

E91/BBM92

analysis

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \frac{1}{2}(|H+\rangle + |H-\rangle + |V+\rangle - |V-\rangle)$$

		Bob measures			
		Z-basis		X-basis	
		p_H	p_V	p_+	p_-
Alice measures	$\|H\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
	$\|V\rangle$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
	$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
	$\|-\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$

- if $basis_{Alice} = basis_{Bob} \Rightarrow |\psi_{Alice}\rangle = |\psi_{Bob}\rangle$
- need basis reconciliation

QKD attacks

- intercept-resend: Eve measures & resends a photon
  ⇒ increased QBER → Eve detected
- photon-number splitting: Eve uses a BS, takes a photon
  ⇒ use decoy states or single photon source
- Trojan horse: Eve sends bright light, measures the phase
  ⇒ monitor light, use circulators/isolators
- man-in-the-middle: Eve impersonates Alice & Bob
  ⇒ use authenticated classical channel → need inital shared secret
- denial of service: Eve blocks/cuts the channel
  ⇒ develop QKD networks

quantum networks

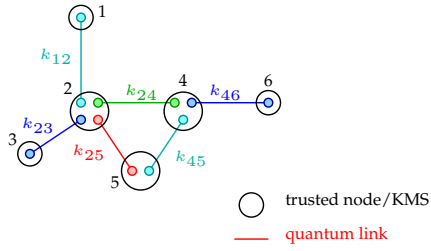
QKD systems: point-to-point $\Rightarrow$ need quantum communication networks

- 1st generation: trusted nodes
  - available now
  - low functionality: key distribution
- 2nd generation: quantum repeaters
  - challenging
  - advanced functionality: entanglement distribution, quantum internet, blind QC

1st generation quantum networks

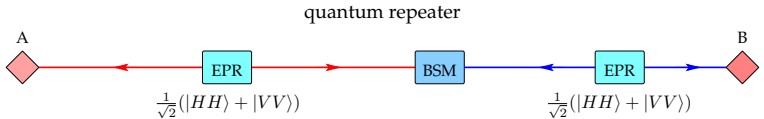
trusted nodes

- information: quantum (between nodes), classical (at nodes)
  $\Rightarrow$ *nodes need to be trusted*
- KMS: shares keys between non-connected nodes
  (key management system)
- KMS: classical key transport software
- example: generate and share a key k_{16} between nodes 1 and 6



2nd generation quantum networks

quantum repeaters



- *entanglement swapping*: distribute entanglement between distant nodes
- no need to trust intermediary nodes
- extended functionality
  - quantum internet
  - distributed quantum sensing
  - blind quantum computing

quantum: worldwide

QKD networks

Vienna (2009)

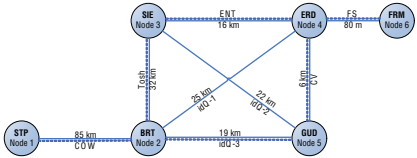
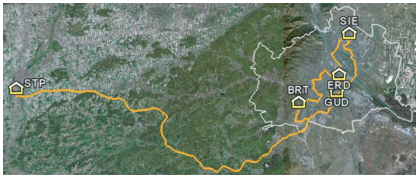
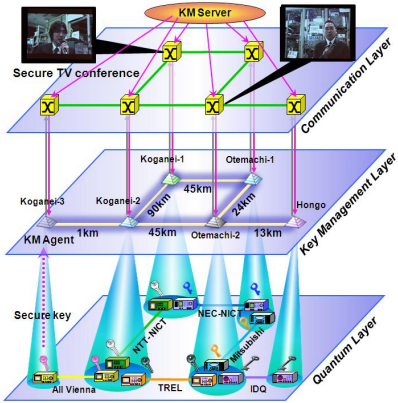


Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.



Peev *et al.*, New J. Phys. **11**, 075001 (2009)

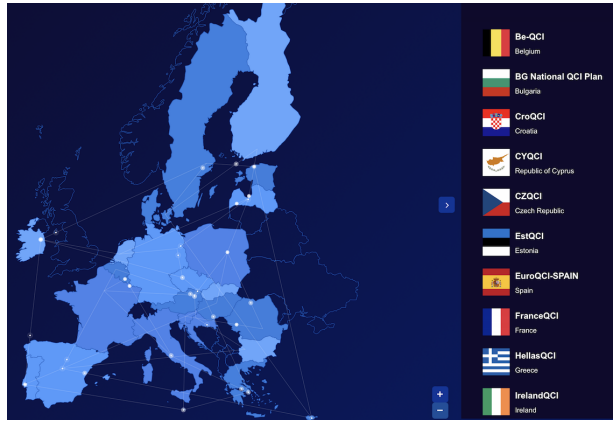
Tokyo (2011)



Sasaki *et al.*, Opt.Exp. **19**, 10387 (2011)

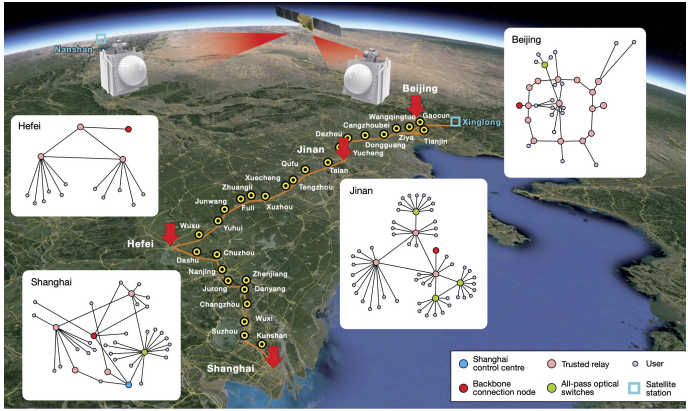
Petrus: building EuroQCI

- network of 27 national QCIs
- fiber + free-space links
- cross-border links



China

Beijing-Shanghai quantum backbone, 2000 km (≃ Bucharest-Brussels)



- Hefei: 46 nodes intra-city quantum network

(4th gen. crypto machine)

China

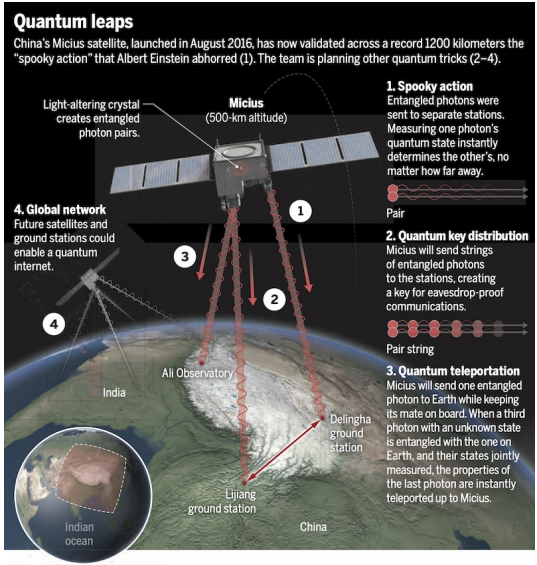
space

2016: Mozi/Micius satellite

- 635 kg, $100 Mil.
- QKD
- entanglement distribution
- teleportation

2022: Jinan-1 satellite

- < 100 kg
- key rate 10^2-$10^3\times$ Mozi



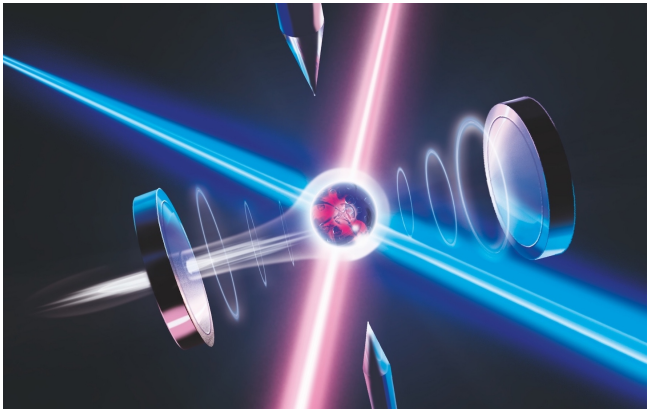
Science (16 June 2017)

quantum, next?

take home message

- whatever you do, a *quantum app* can do it better/faster/more secure
- quantum is ~~coming~~ here: not *if*, but *when*
- transition to quantum economy
- we need:
  - quantum-ready workforce $\Rightarrow$ invest in research & education
  - quantum-secure economy $\Rightarrow$ invest in infrastructure & industry

are YOU ready?



Thank you!