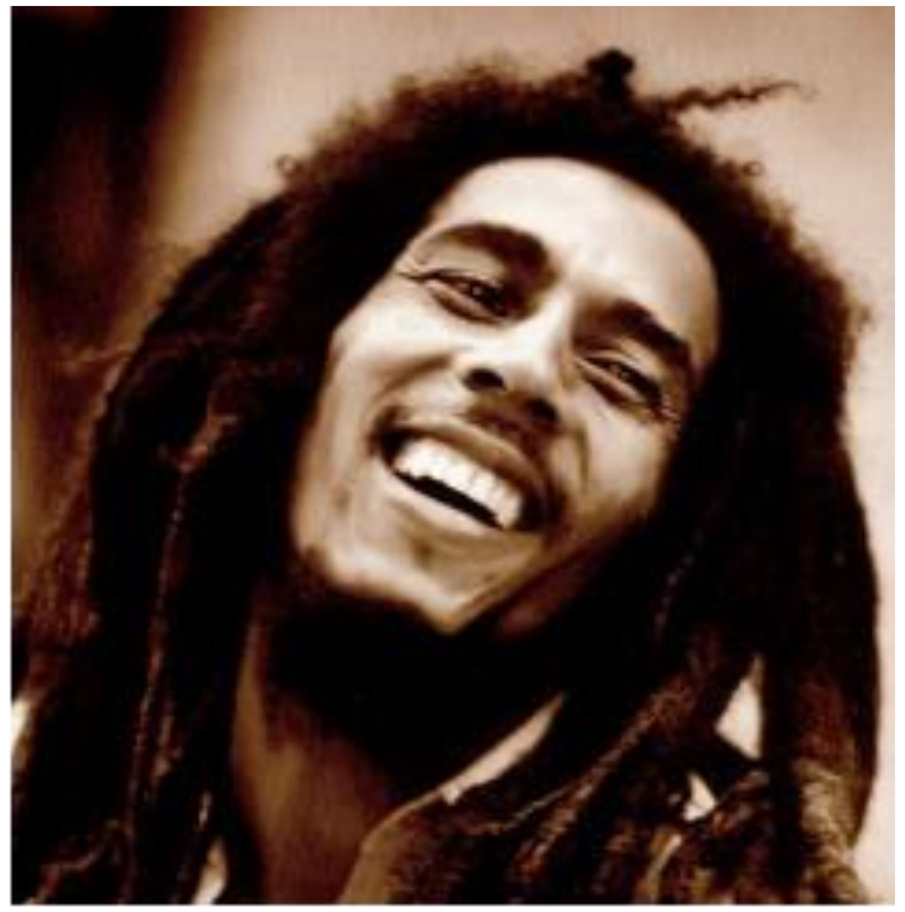
Quantum Communication and Quantum Cryptography

Guilherme Temporão
CETUC / PUC-Rio

Who Keeps the Dog?

Alice



Bob

How to share a random number between two untrusted parties?

Classical protocol: $P_{cheat} = 100\%$

Quantum protocol: $P_{cheat} = 75\%$

Quantum Coin Tossing

Quantum Communication Applications

Cryptography

- Quantum Key Distribution
- Byzantine Agreement
- Quantum Secret Sharing

Distributed Sensors

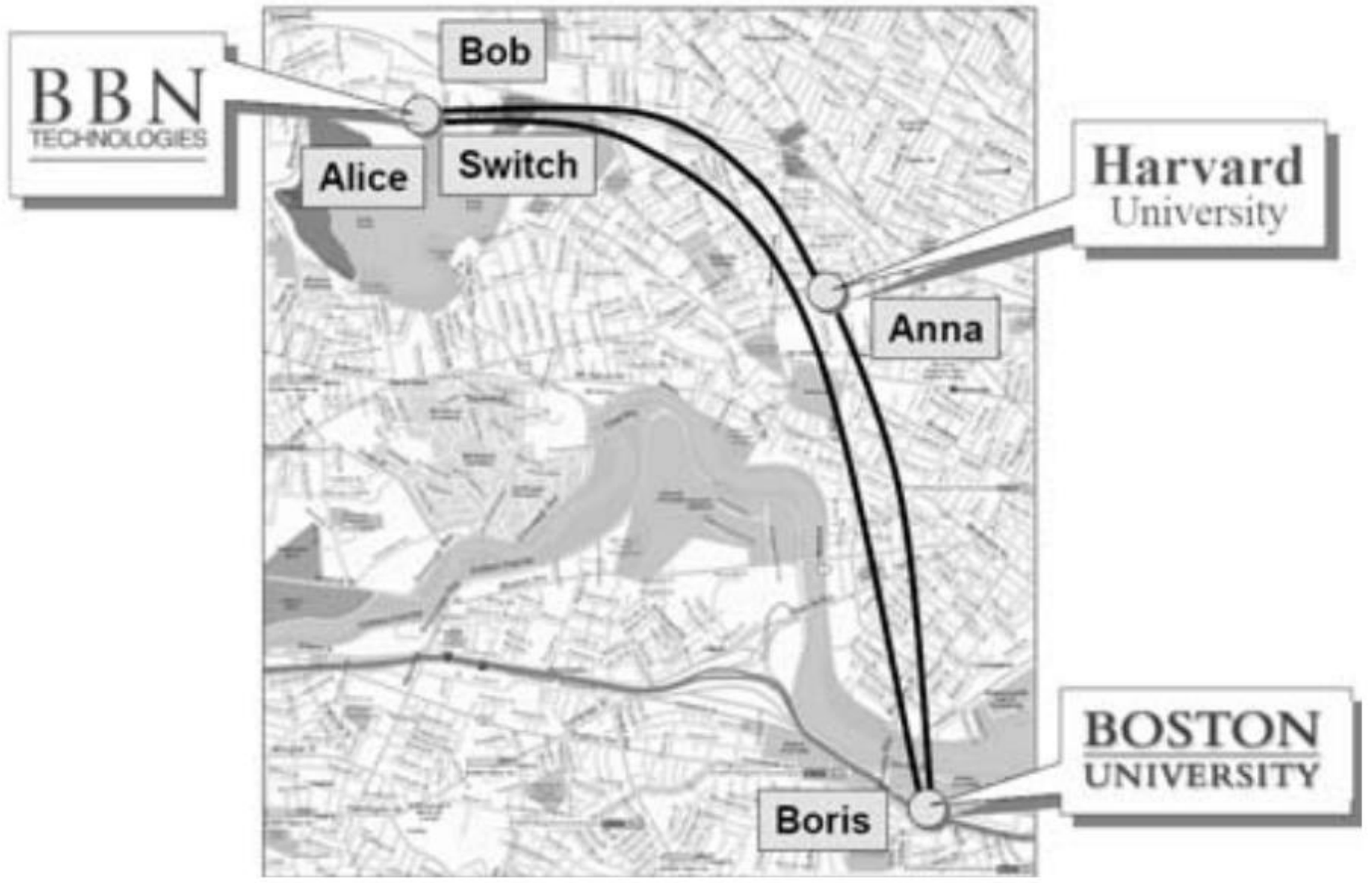
- Clock Synchronization
- Combining Telescopes
- Interferometry

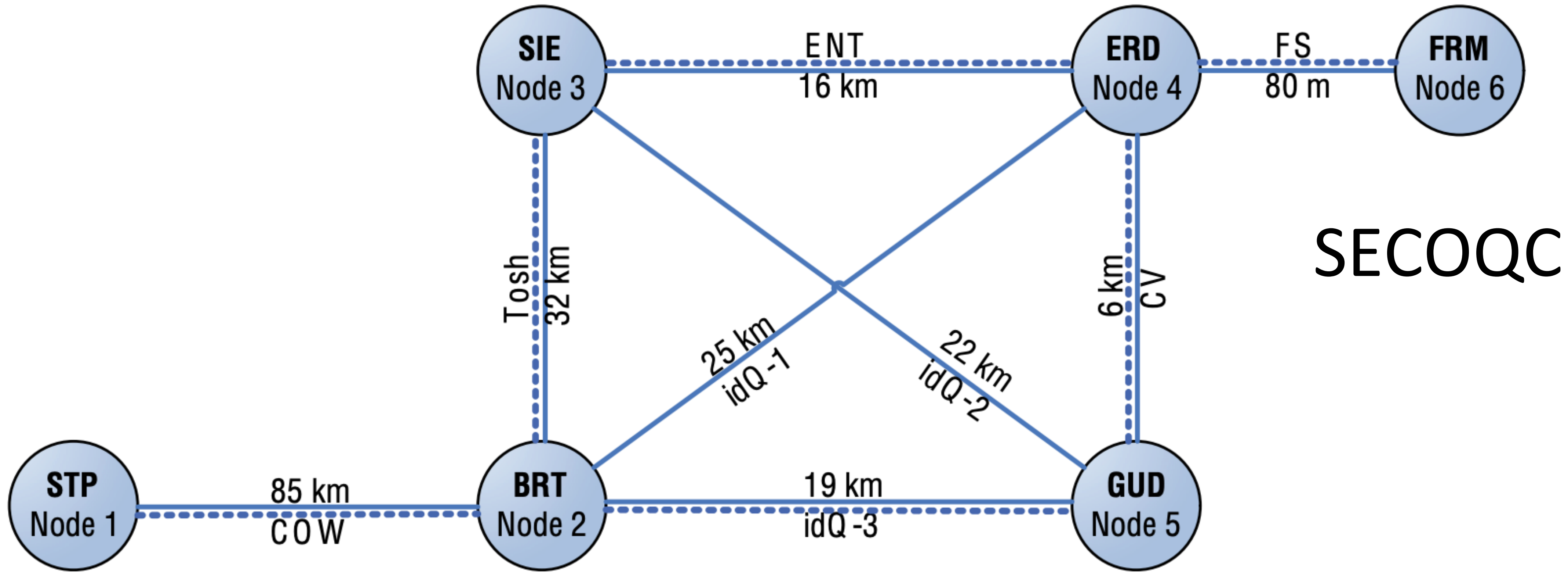
Distributed Computation

- Cloud Quantum Computing
- Blind Quantum Computing
- Nonlocal Quantum Computing

Quantum Communication Networks

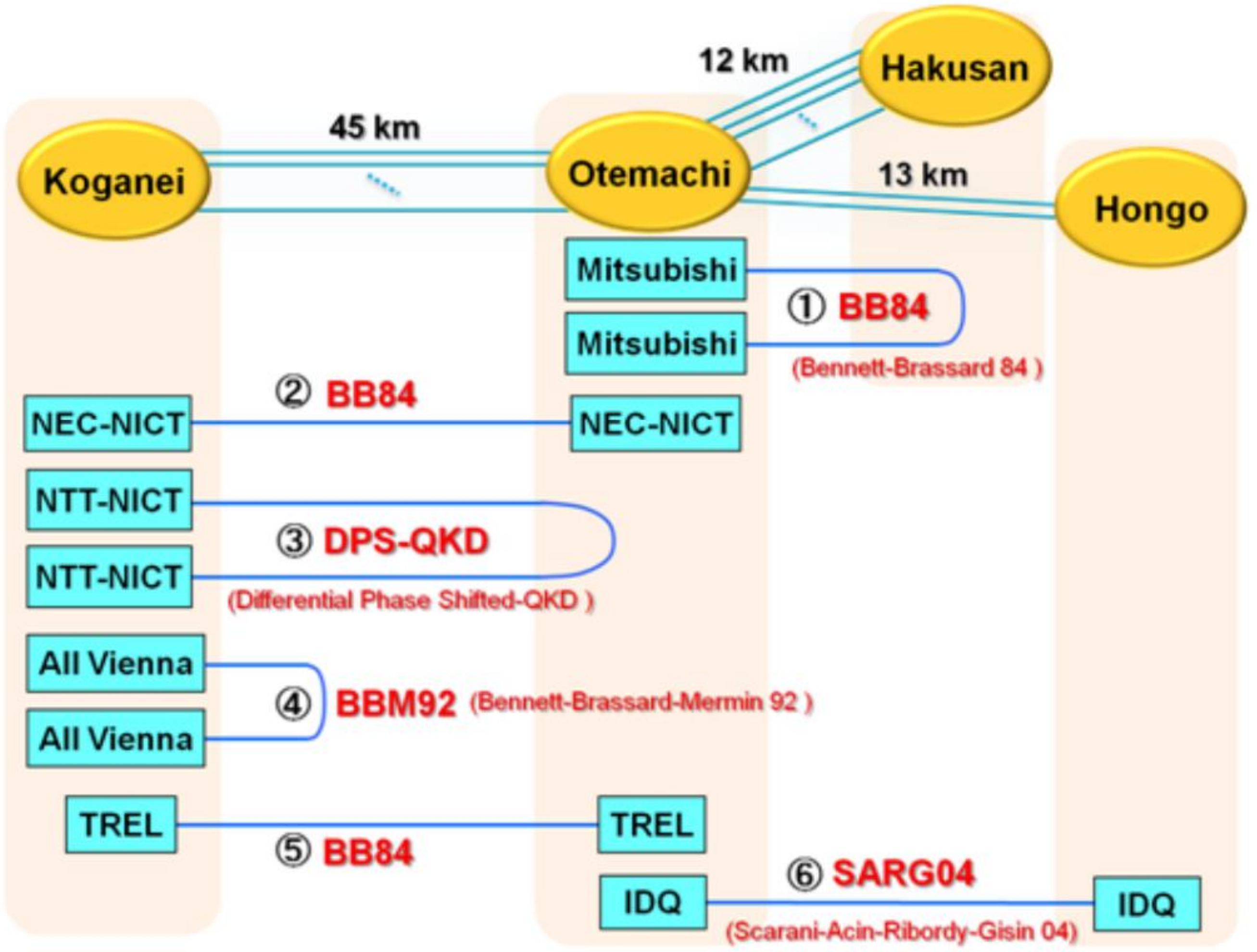
DARPA Network





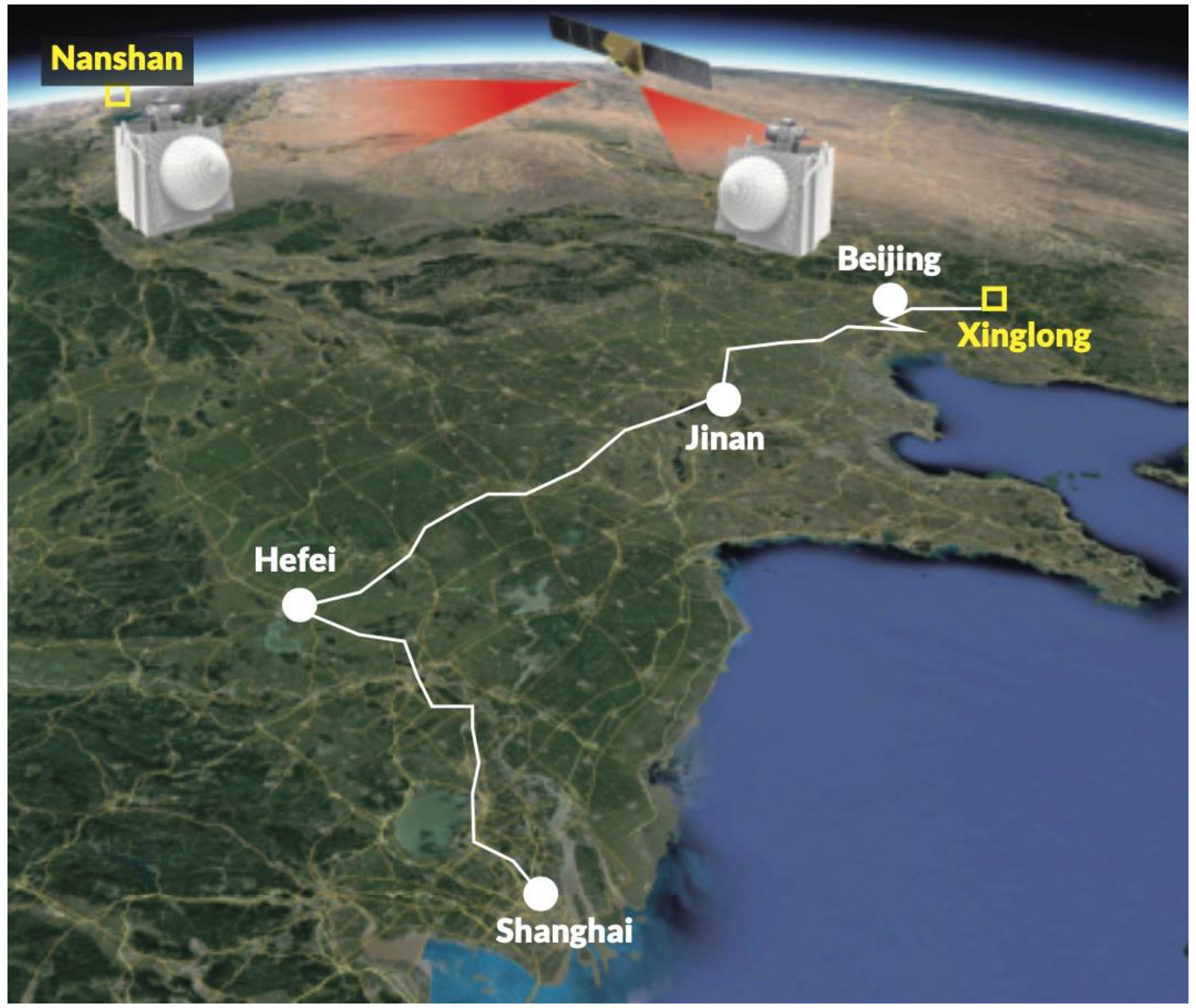
SECOQC Network

SwissQuantum Network



Tokyo Network

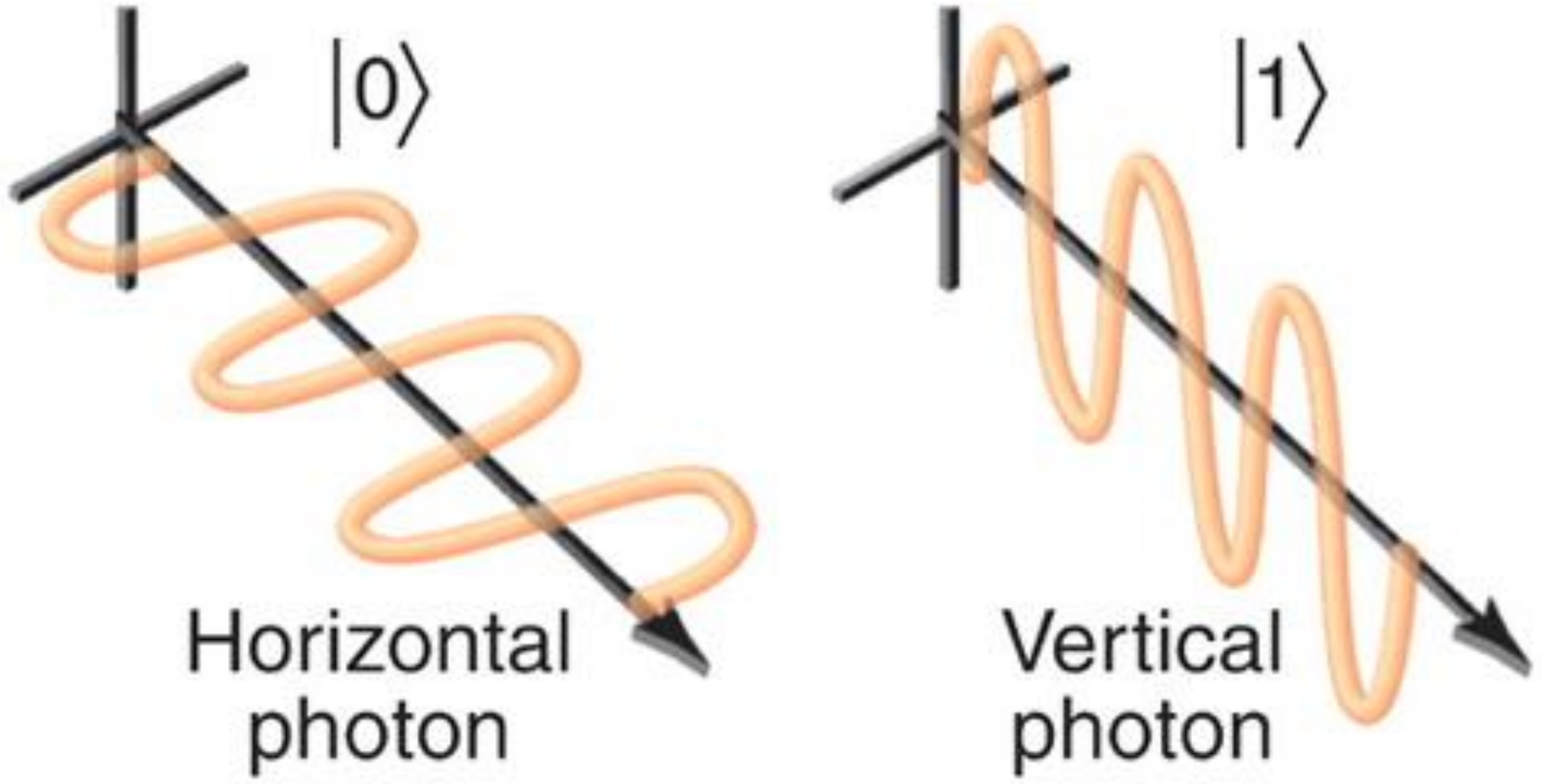
China's Quantum Network

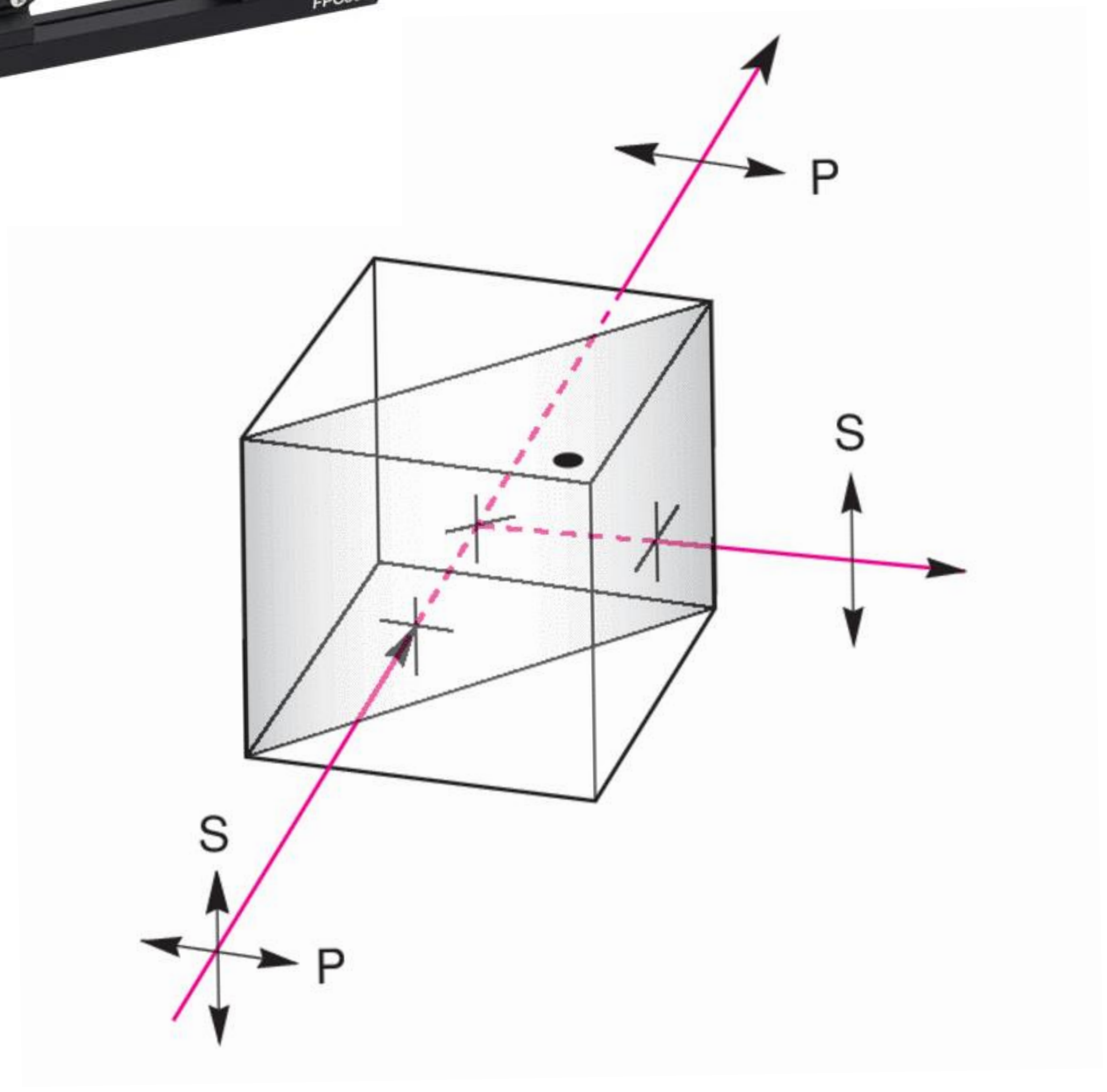


UERJ
2,3 Km
8,8 Km
FIOCRUZ
8,9 Km
CEFET
3,2 Km
Backbone
88,3 km
UFRJ
20,3 Km
MIX
20,3 Km
PUC
12,3 Km
CBPF
9,2 Km
SIX
POP RNP
dark fiber
free-space
ICARAÍ
UFF
~ 7km
CBPF
Rio de Janeiro
COPACABANA
29,5 km
IPANEMA
12,3 km
Cristo Redentor
UFRJ
55,8 km
Ilha do Fundão
PUC-Rio
101
TIJUCA

The Photonic Qubit

Polarization encoding



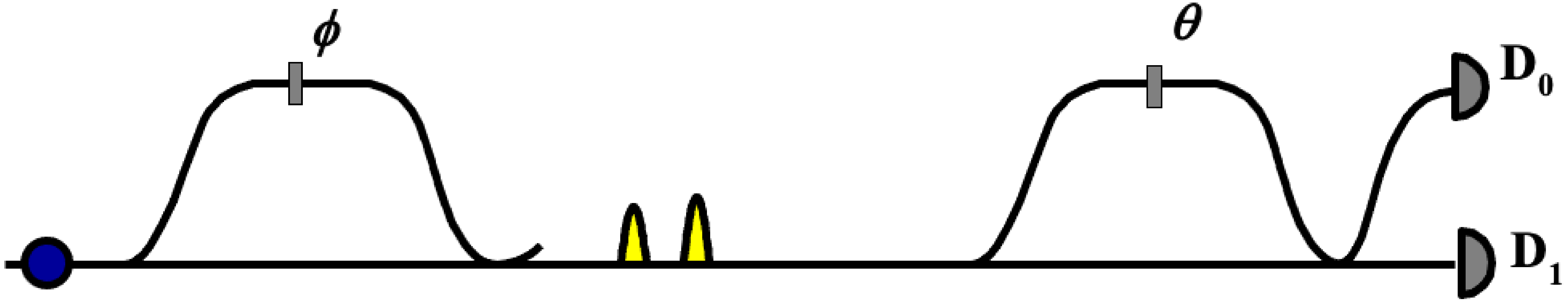


$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

The Photonic Qubit

Time-bin encoding

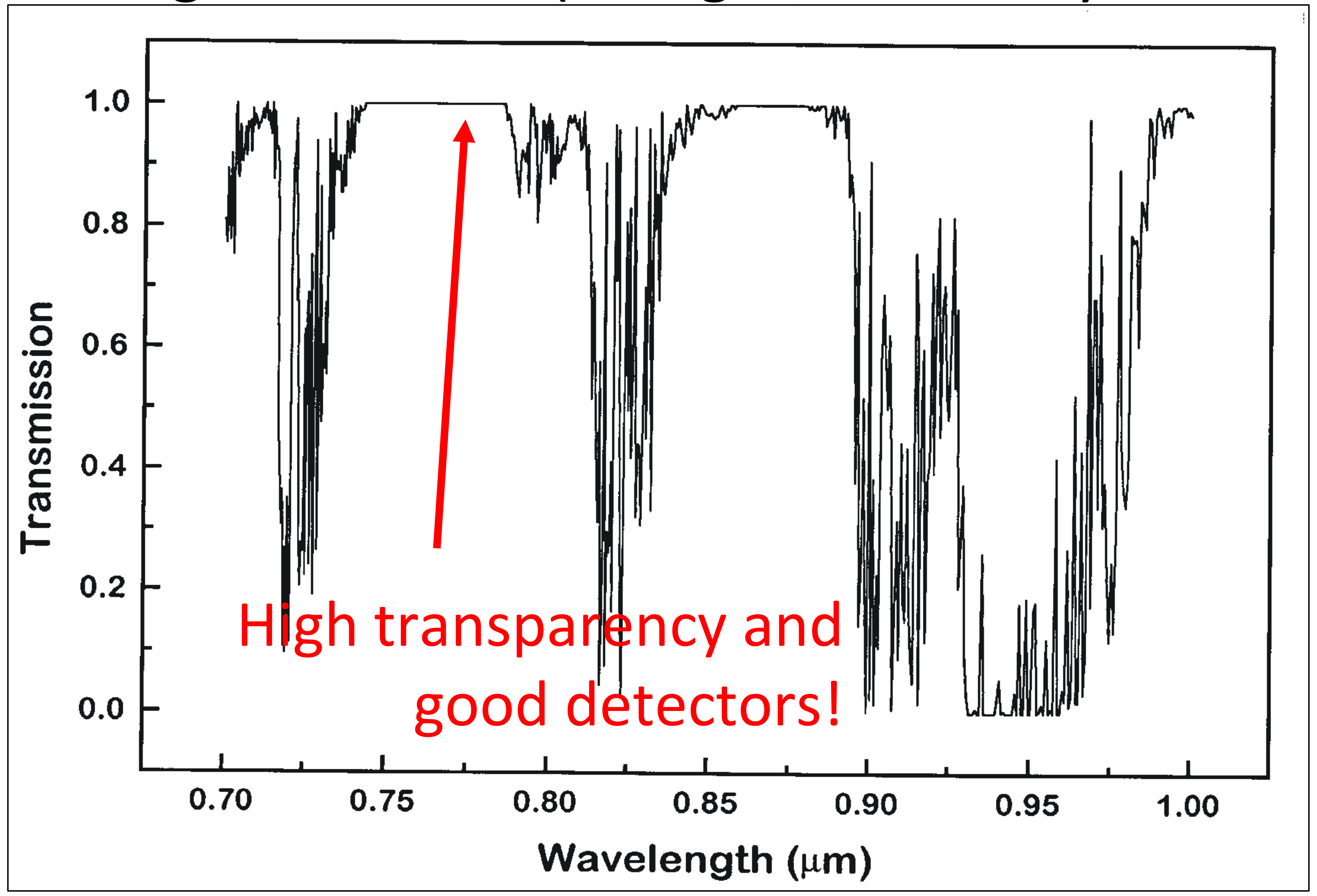
$$|\psi\rangle = \sqrt{t}\,|0\rangle + \sqrt{1-t}e^{i\phi}\,|1\rangle$$



Quantum Channels

Free Space (atmosphere)

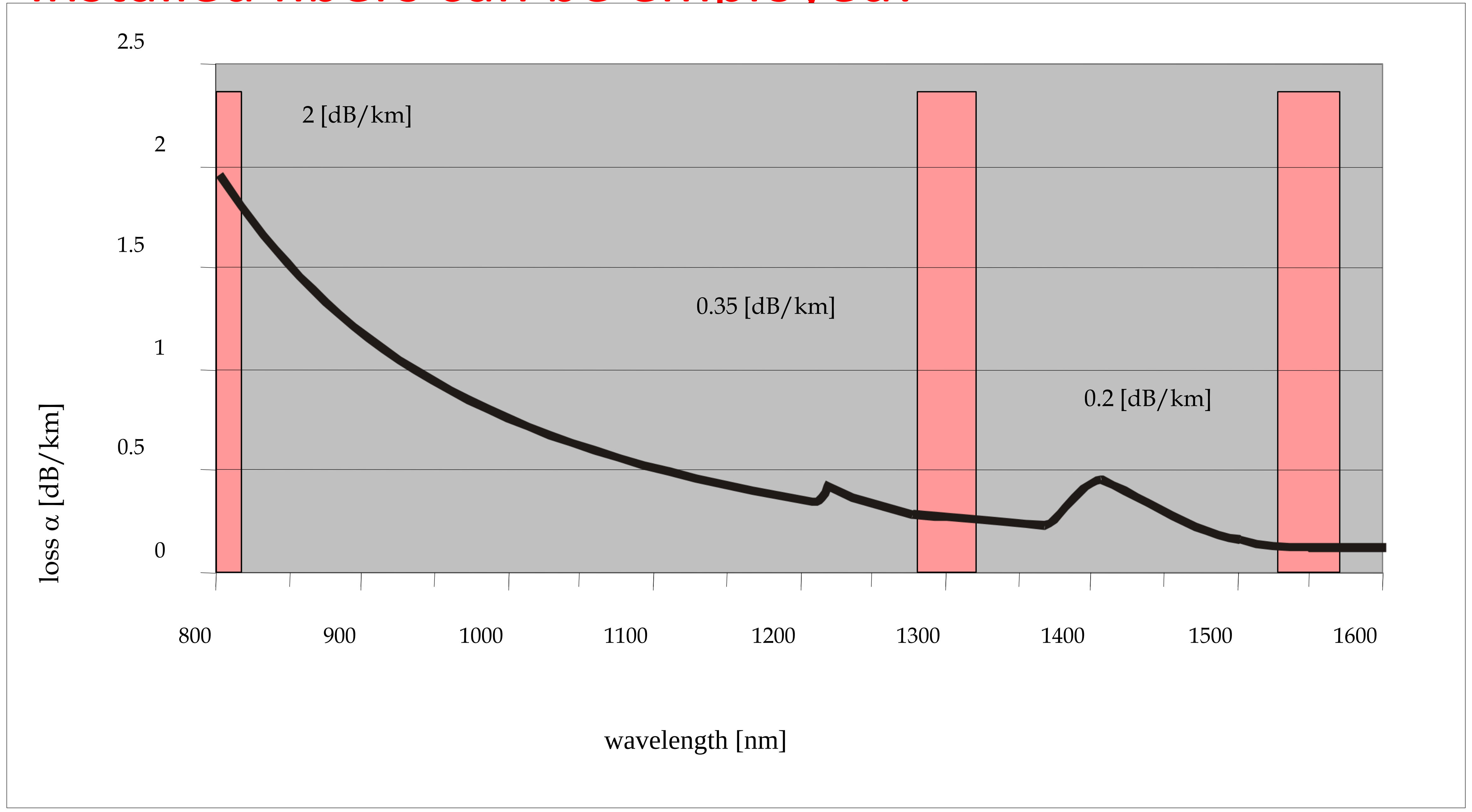
- Transmission
  - absorption (obstacles, weather conditions)
  - diffraction
  - atmospheric turbulence
- Background noise (sunlight, blackbody radiation)



Optical Fibers

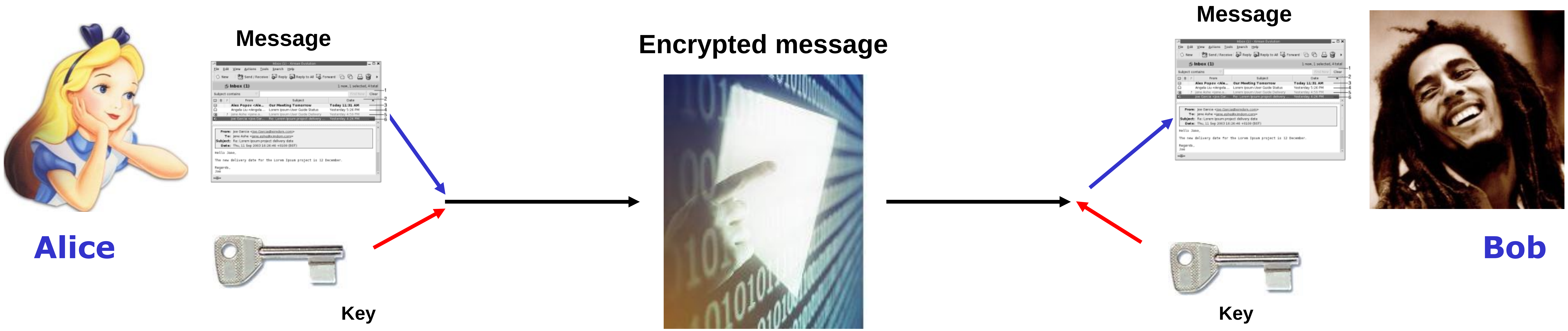
- Transmission (absorption)
- Dispersion
- Random birefringence - depolarization

Installed fibers can be employed!



Why Quantum Cryptography?

Gilbert Vernam (1917): "One-Time Pad" – **provably secure**



Alice								
message (M)	0	1	1	0	1	0	0	1
key (K)	1	0	0	1	1	0	1	0
M ⊕ K = C (cipher text)	1	1	1	1	0	0	1	1

transmission ↓

Bob								
cipher text (C)	1	1	1	1	0	0	1	1
key (K)	1	0	0	1	1	0	1	0
C ⊕ K = M ⊕ K ⊕ K = M (message)	0	1	1	0	1	0	0	1

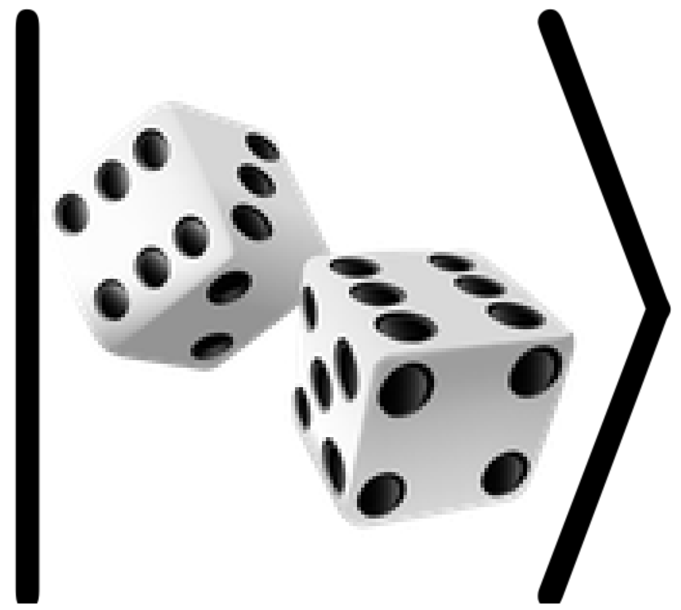
Why Quantum Cryptography?

The one-time pad is secure if it is:

- √**of the same size of the message**
- √**never reutilized**
- √**random**
- √**known only by Alice and Bob**

Randomness:

Not a problem!



"Quantum Random Number Generator"

(commercially available)

Problems: randomness, key distribution

Practical solutions for key distribution:

- Cryptography based on "security by obscurity"
- Cryptography based on **comptational complexity**

Classical solution to the key distribution problem

Symmetric cyphers (private key)
AES (Advanced Encryption Standard, 2001)
256 bit key
Attack: search for one among 2^{256} keys

Grover's algorithm

Asymmetric cyphers (public key)
RSA (Rivest, Shamir, Adleman, 1977)
Different keys for encoding and decoding
Attack: factorization of large numbers

Shor's algorithm

Systems vulnerable to ...

Theoretical progress

Systems based on unproved mathematical assumptions.
Can become insecure overnight with theoretical advances

More computational power

Sufficient computational power can break cryptographic codes

Example: RSA

Quantum Computing

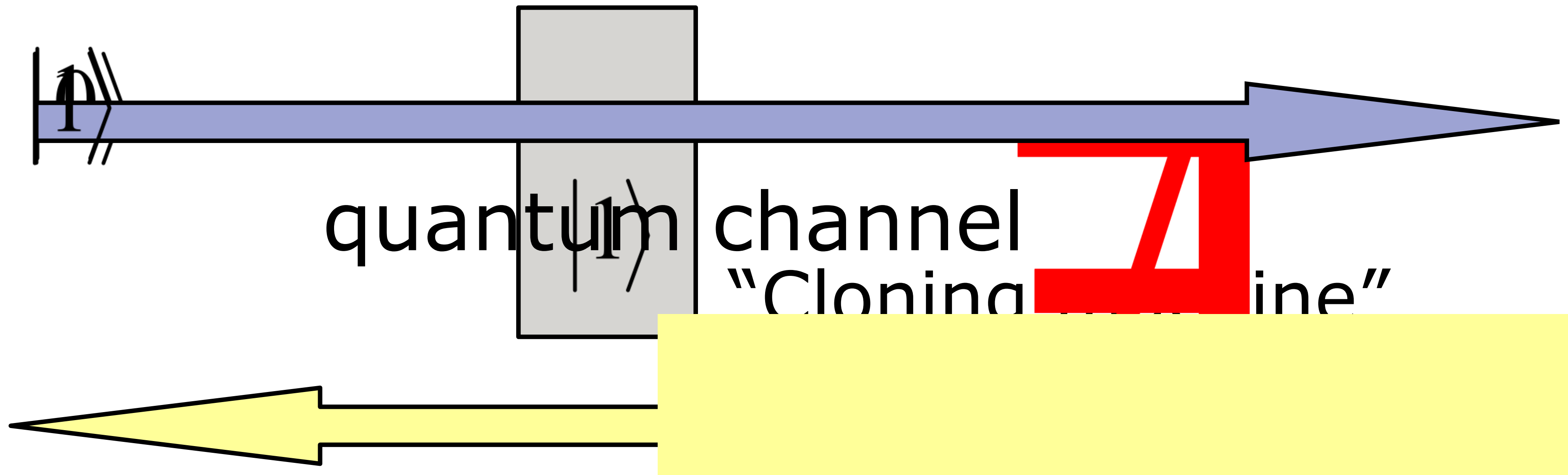
Quantum computers are already being developed by research centers and industry

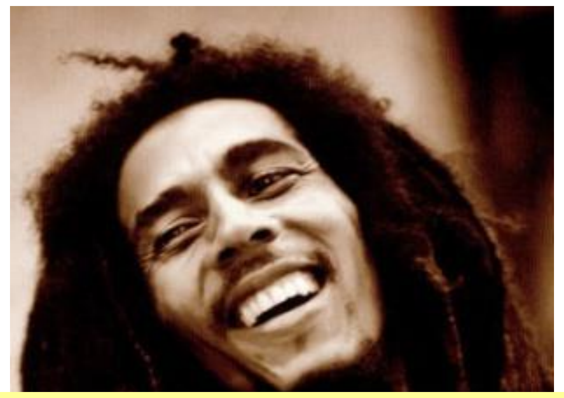
D:WAVE The Quantum Computing Company™
rigetti
IBM
intel
XANADU
Honeywell
Google
PsiQuantum

QKD: main idea

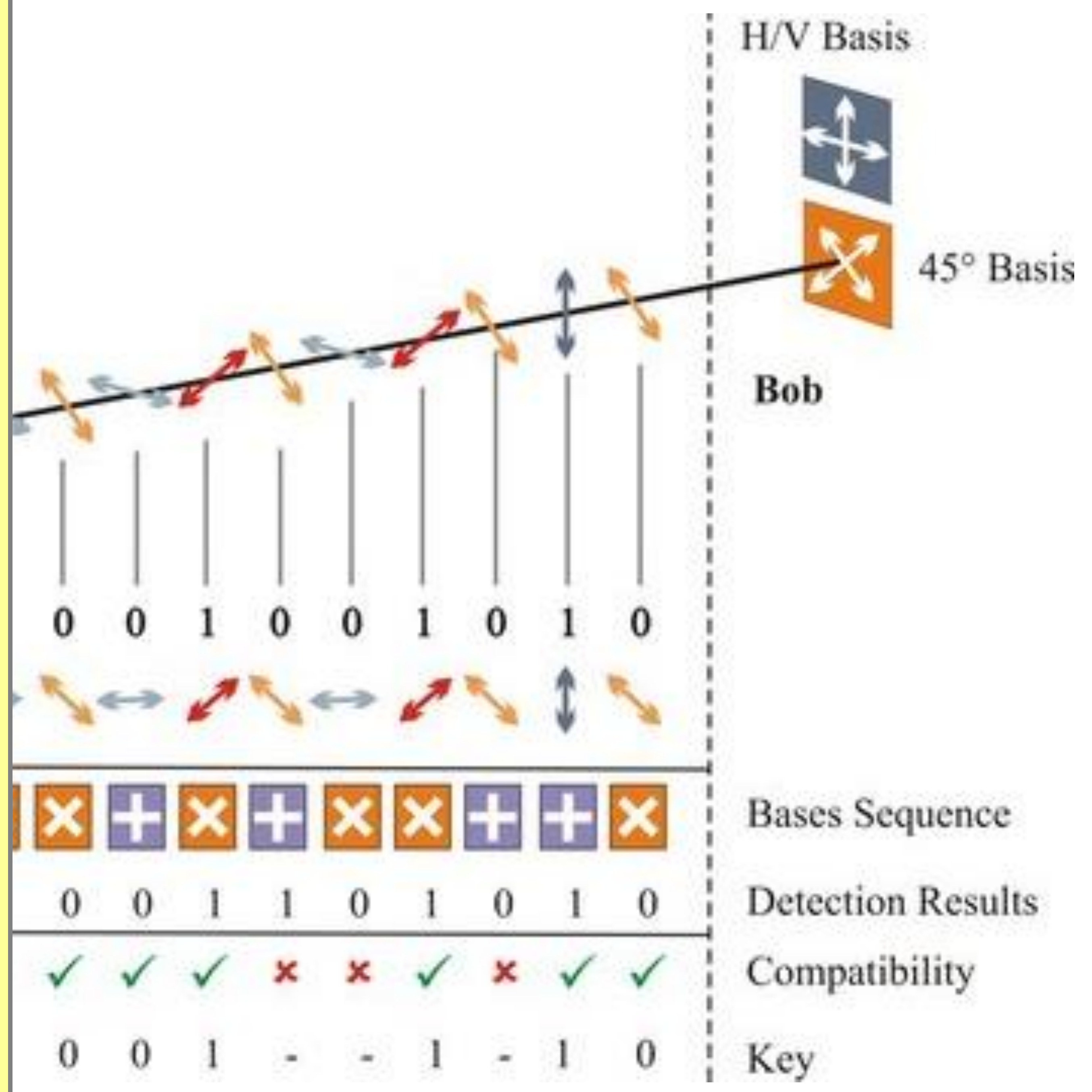
Used for sharing a key (random bit sequence) between two users, Alice and Bob.

Alice





BB84 Protocol
(Bennett, Brassard 1984)

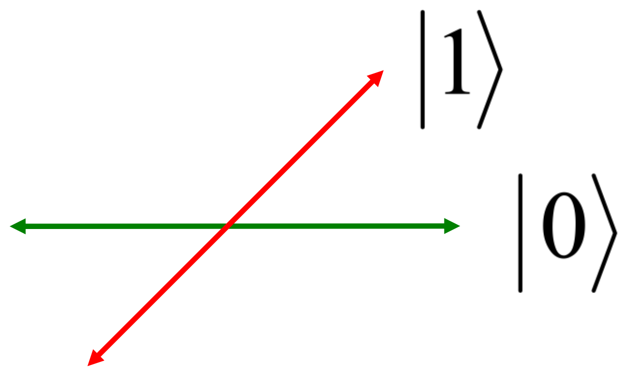


However, we have assumed:

- Ideal single-photon sources
- Ideal single-photon detectors
- No side-channel leakage

What happens in practice?

Ideia: code bits in non-orthogonal states



Measurements → disturbances (errors) → **eavesdropper detected** naturenews

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quan… cryptographers

Lasers crack commercial encryp…

Zeeya Merali

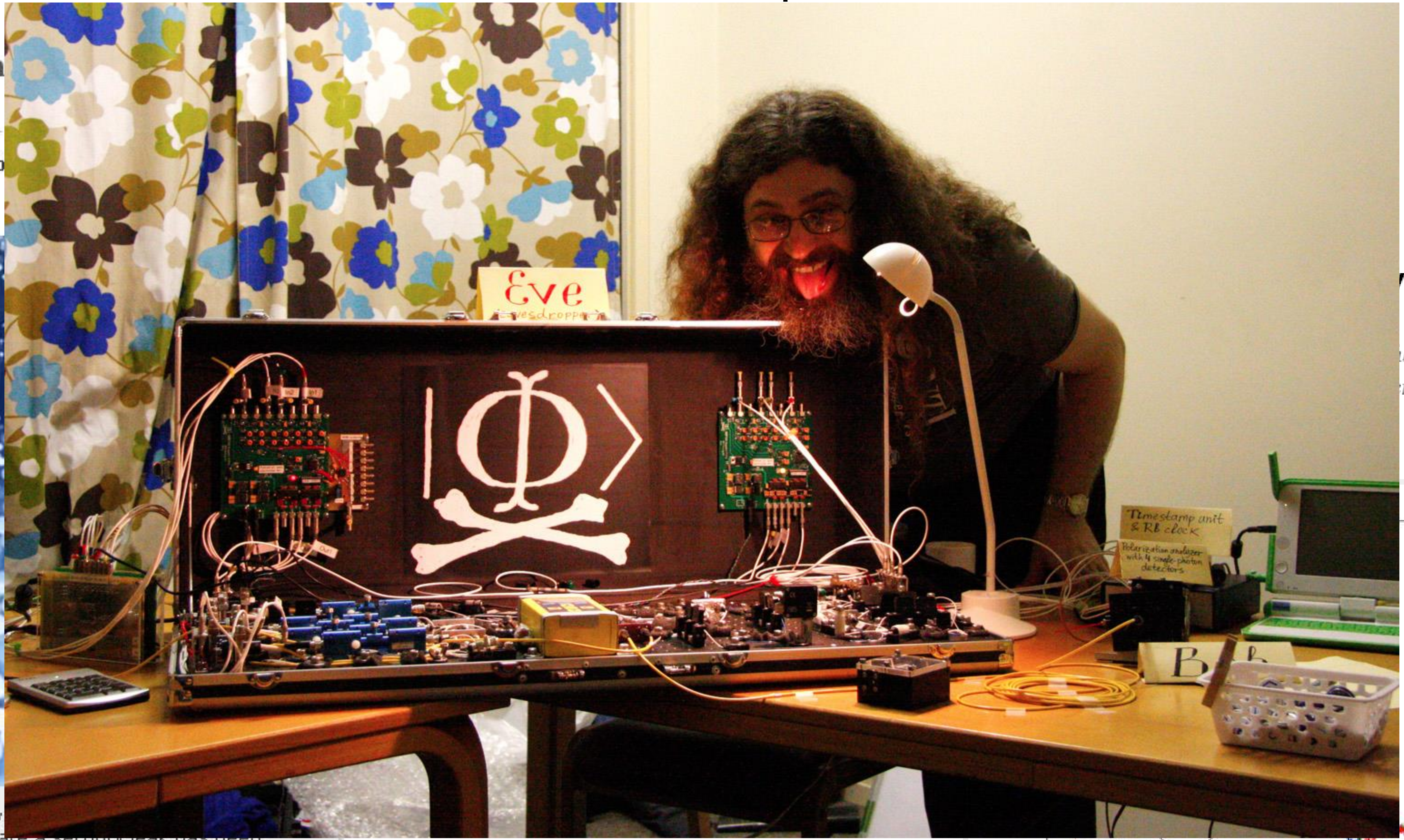
Quantum hackers have performed the first 'invisible' attack on two commercial quantum cryptographic systems. By using lasers on the systems — which use quantum states of light to encrypt information for transmission — they have fully cracked their encryption keys, yet left no trace of the hack.

Quantum cryptography is often touted as being perfectly secure. It is based on the principle that you cannot make measurements of a quantum system without disturbing it. So, in theory, it is impossible for an eavesdropper to intercept a quantum encryption key

A w… create a security leak has been discovered.

NewScientist

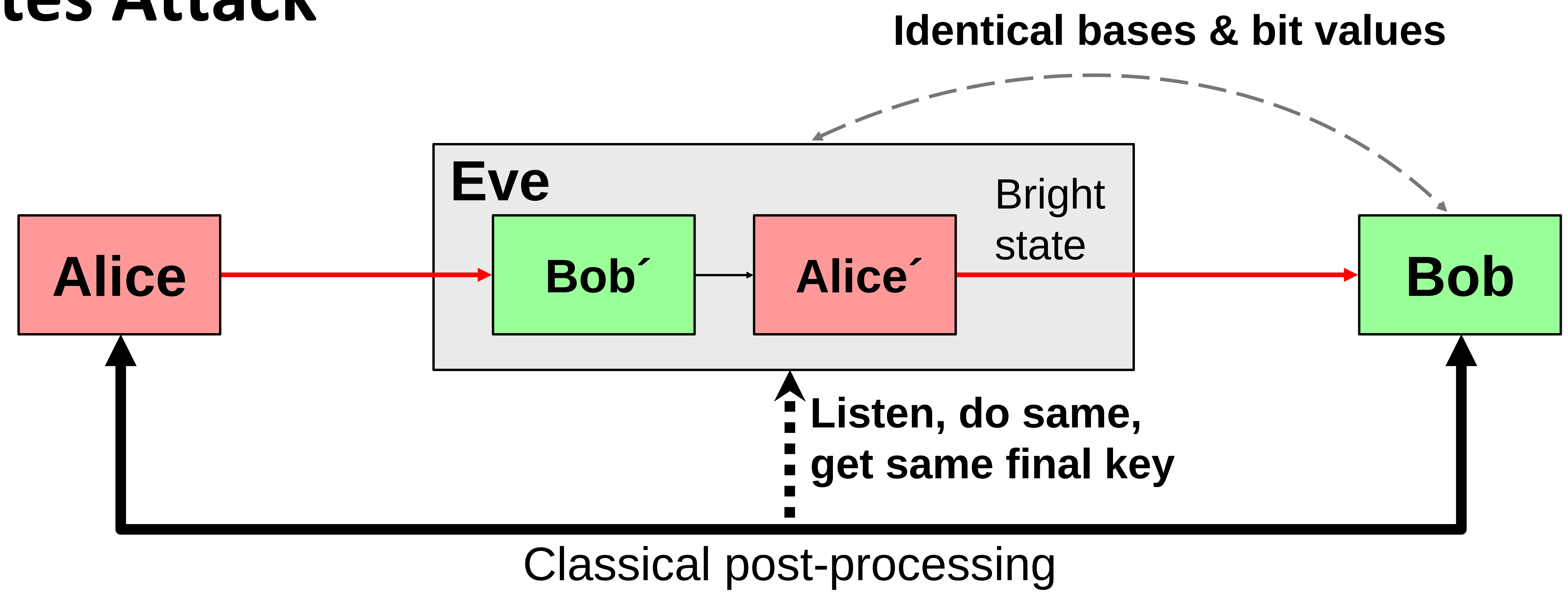
Laser cracks 'unbreakable' quantum communications

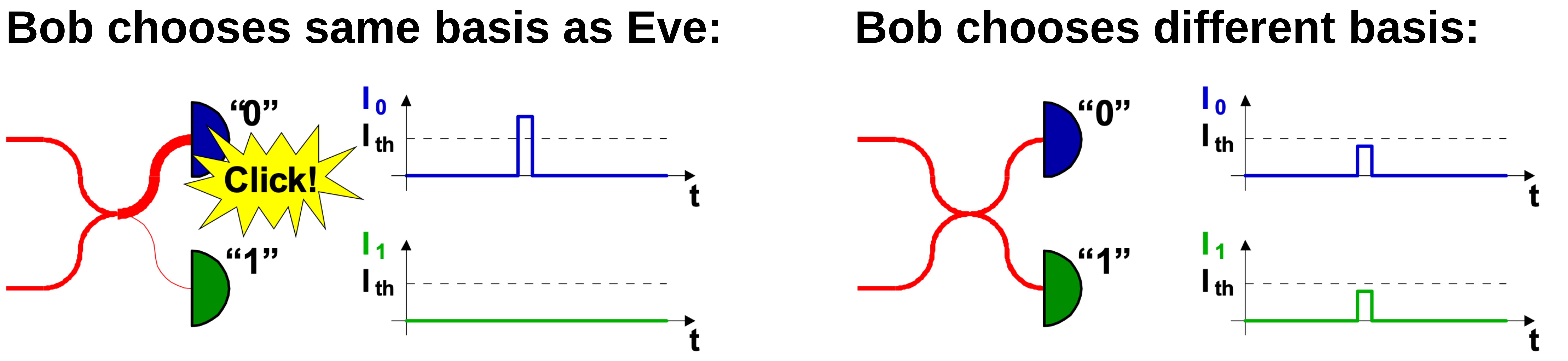


…yptography System

…ul attack of its kind on a …m.

Faked States Attack

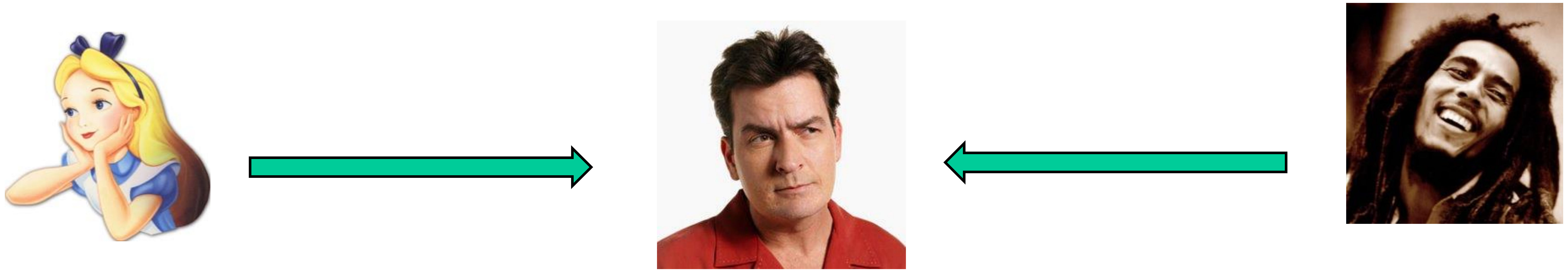




L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Nat. Photonics **4**, 686 (2010)

Measurement Device Independent QKD

Alice and Bob communicate with a mid-way station Charlie, which projects the received two-photon state onto the Bell basis (**Bell State Measurement**). Charlie then publicly announces the BSM result.

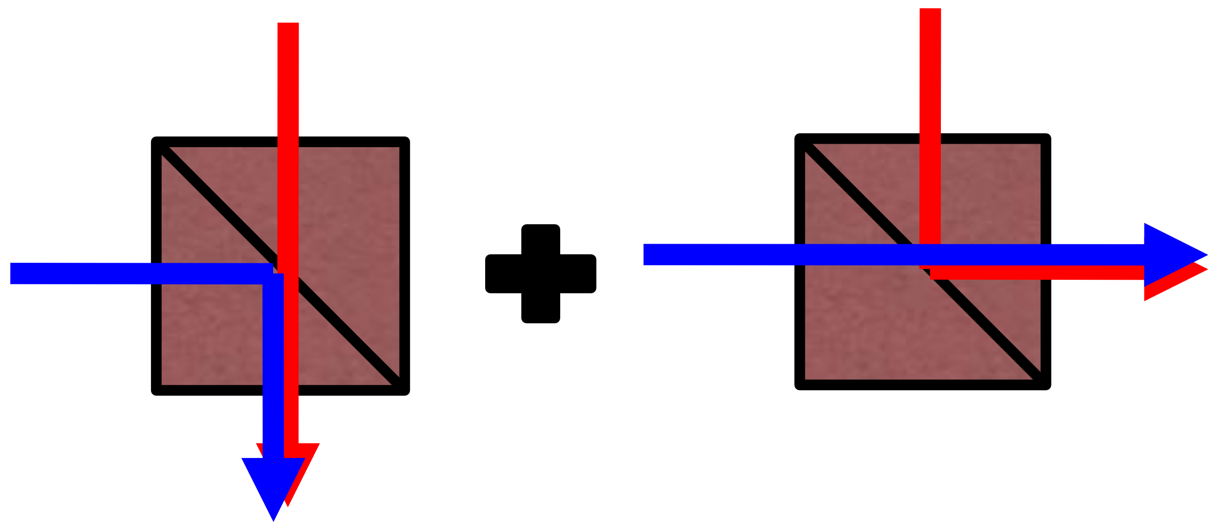


BELL STATE MEASUREMENT

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Photon Bunching



$$|1,1\rangle \rightarrow |2,0\rangle + |0,2\rangle$$

Hoi-Kwong Lo, Marcus Curty, Bing Qi, Physical Review Letters 108, 130503 (2012)

Maximum distance of QKD

P_{in} $\alpha = 0.2\text{dB/km}$ P_{out}

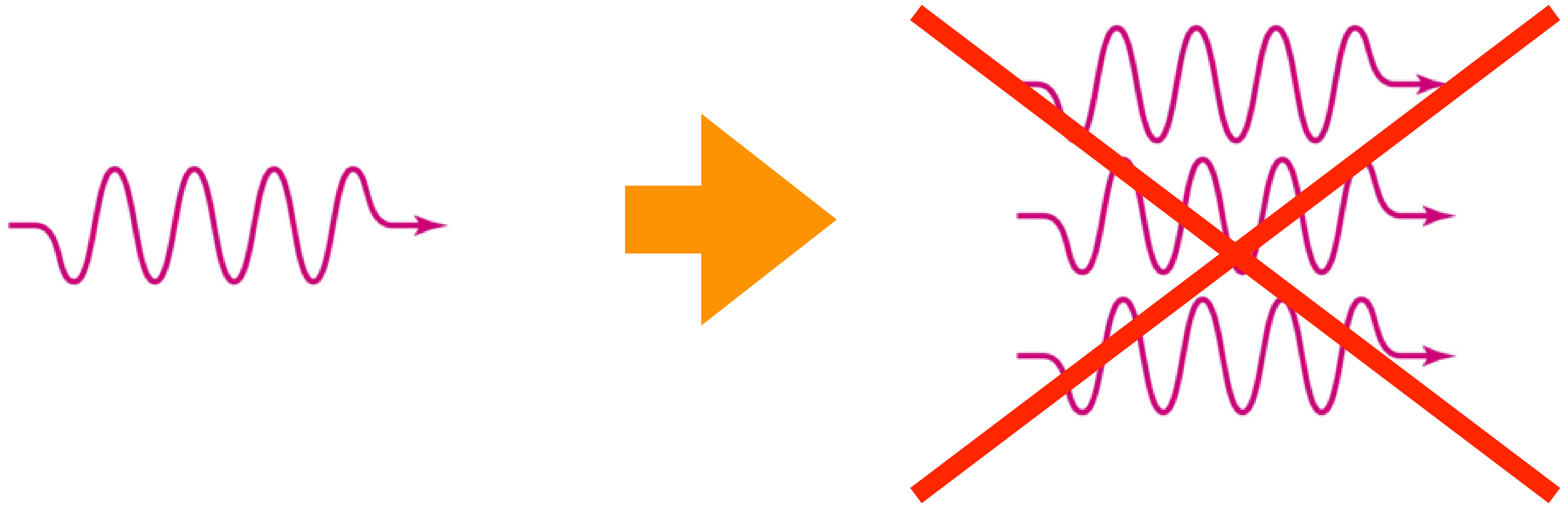
$L = 100\text{km} \implies P_{\text{out}} = P_{\text{in}} - 20\text{dB}$ (99% photon loss)

$L = 500\text{km} \implies P_{\text{out}} = P_{\text{in}} - 100\text{dB}$ (99.99999999% photon loss)

Solution: Repeaters / Regenerators

The Amplification / Regeneration Problem

1) What do we mean by “photon amplification”?



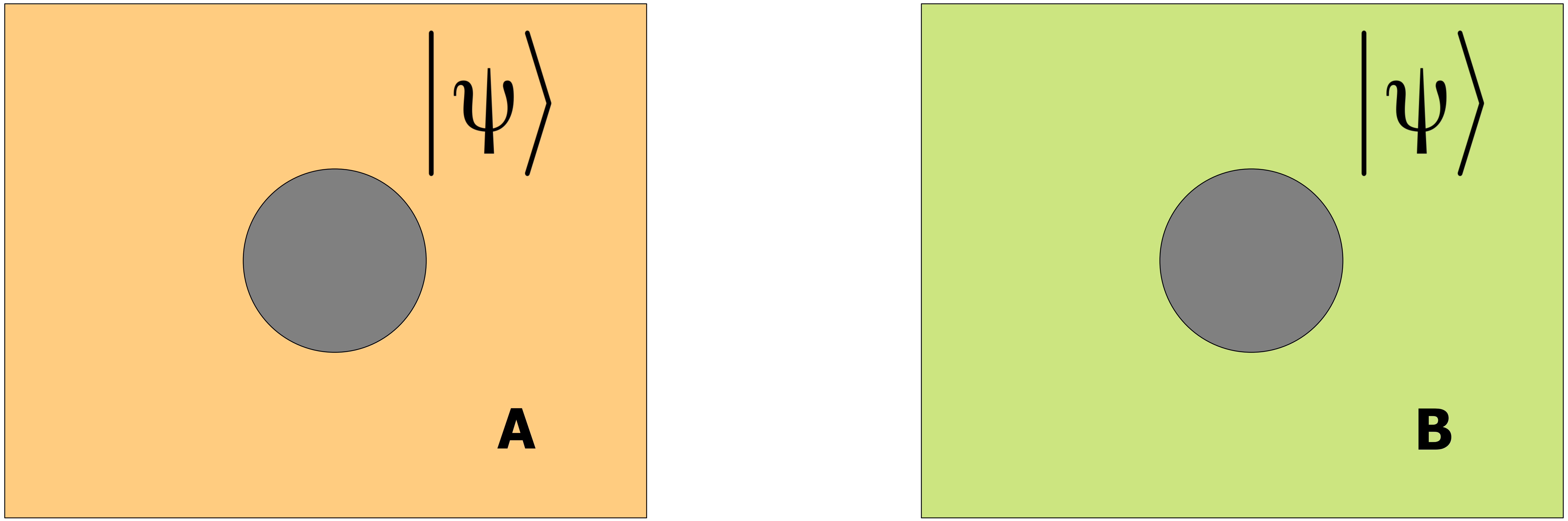
No-Cloning Theorem!

2) How could we “regenerate a photon”?

By making measurements - which destroy the original quantum state!

Classical solutions do not apply!

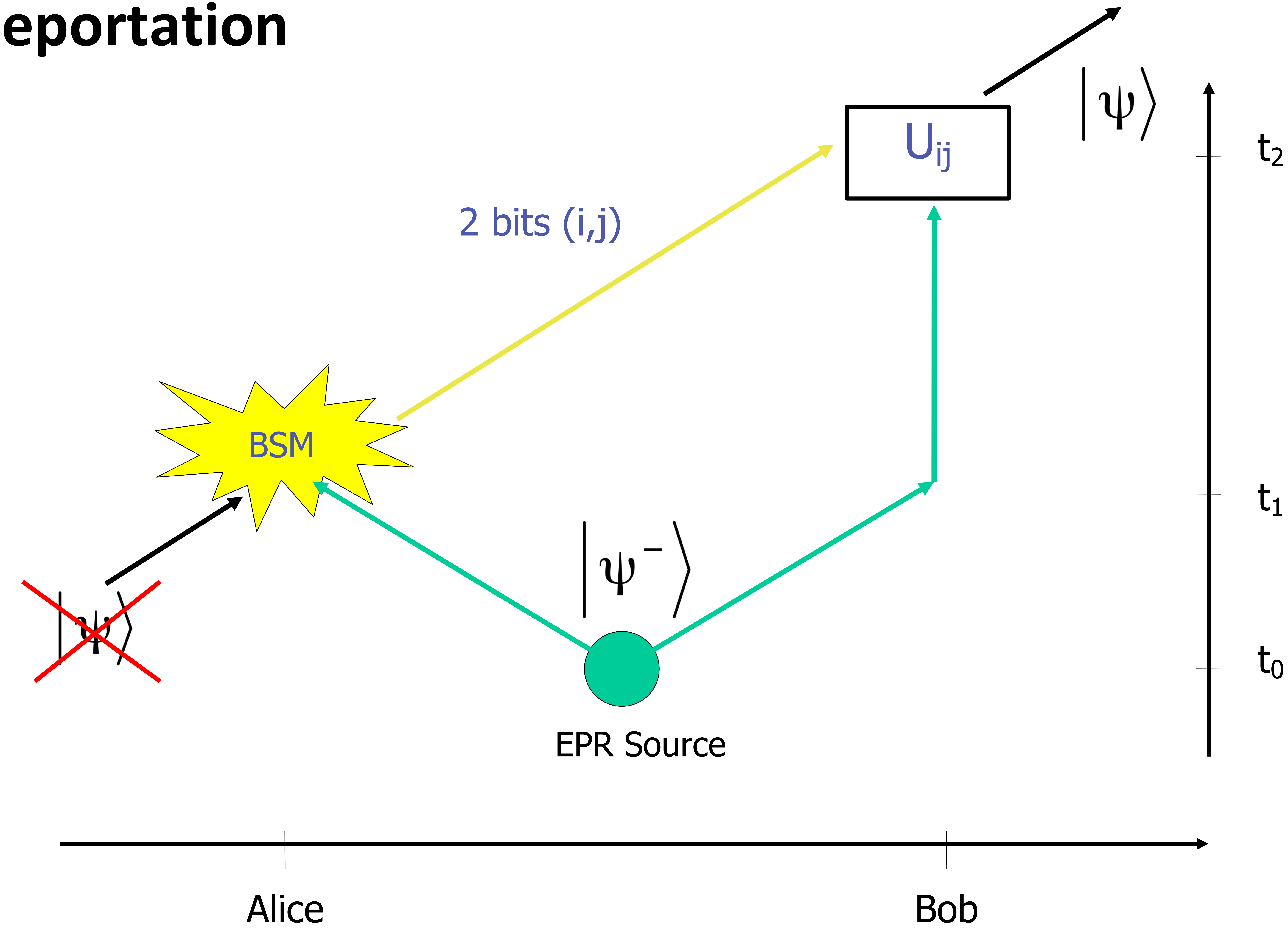
Quantum Teleportation



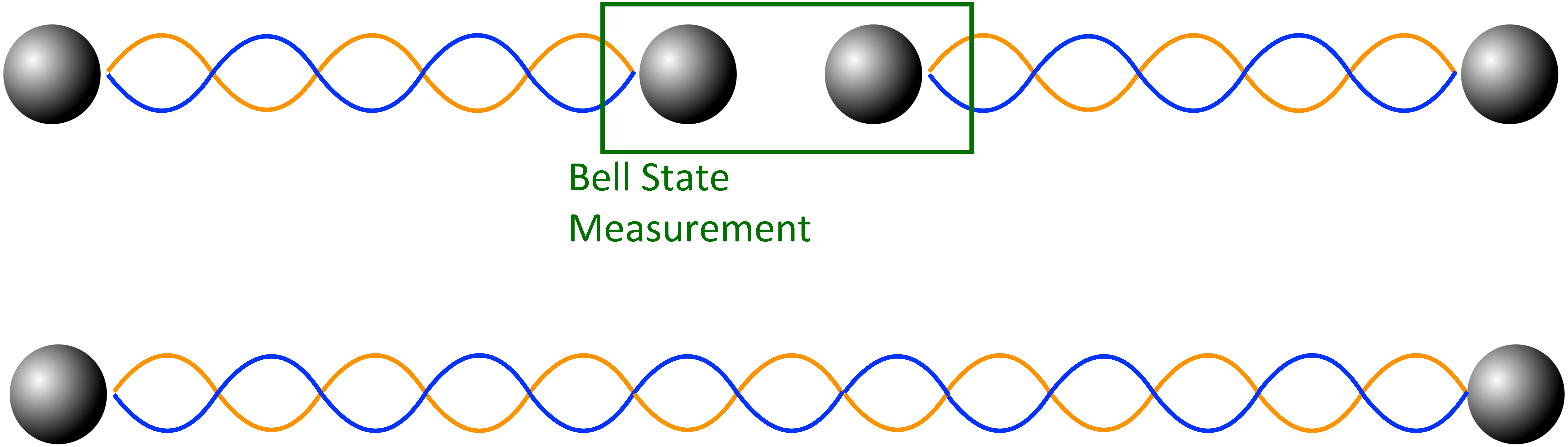
What is “teleported” is the quantum state of the particle

C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. Wooters, PRL 70, 1895 (1993)

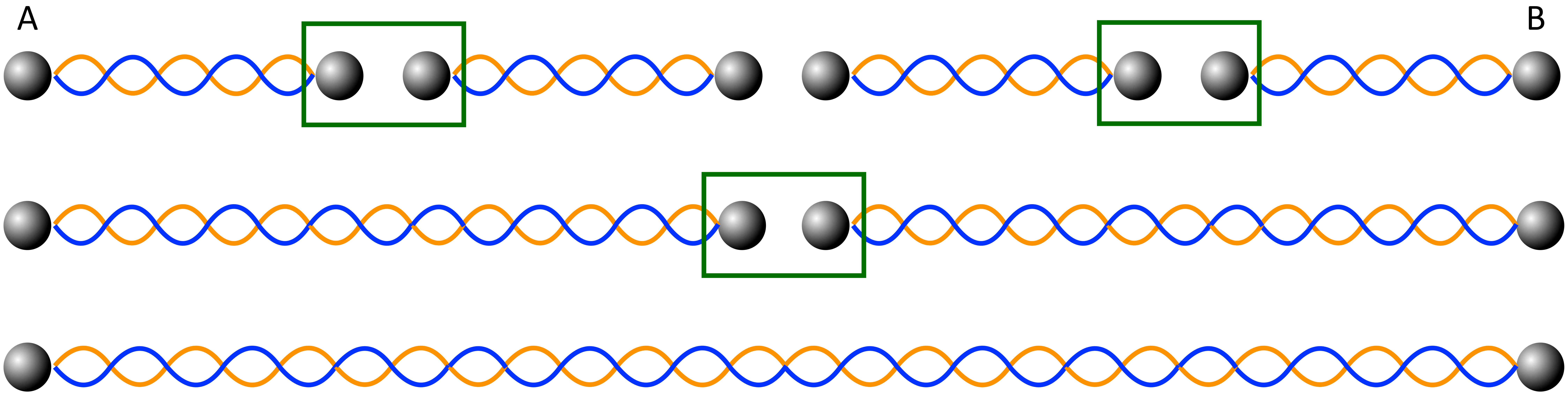
Quantum Teleportation



Entanglement Swapping



Quantum Repeaters



- Create entanglement independently for each link. Extend by Entanglement Swapping.
- Requires the ability to store and retrieve qubits (quantum memory) - heralded process
- Can improve maximum distances in QKD

$$T \sim \frac{1}{t^n} \longrightarrow T \sim \frac{1}{t}$$

H.-J. Briegel et al., PRL 81, 5932 (1998)

Challenges in Quantum Communications

- Multimode, long-coherence-time quantum memories for Q repeaters
- Wavelength conversion for interfacing with Q computers
- High brightness entangled photon pair sources (GHz)
- Efficient protocols for entanglement purification
- Coexistence with classical signals in optical fibers
- Development of routing protocols in quantum networks

Thank You!

temporao@puc-rio.br