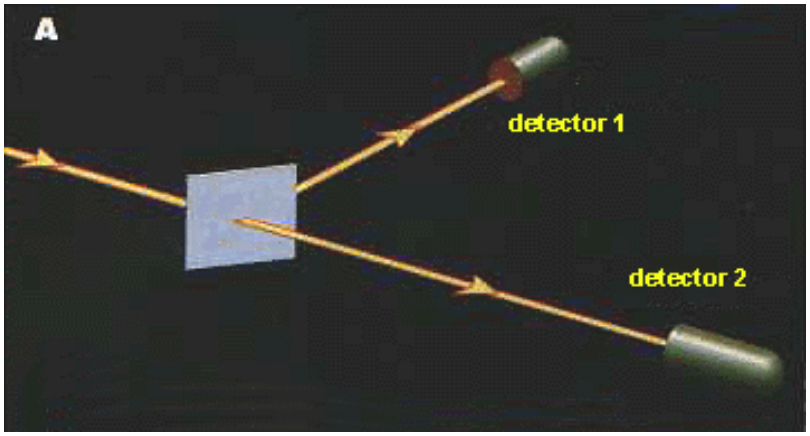
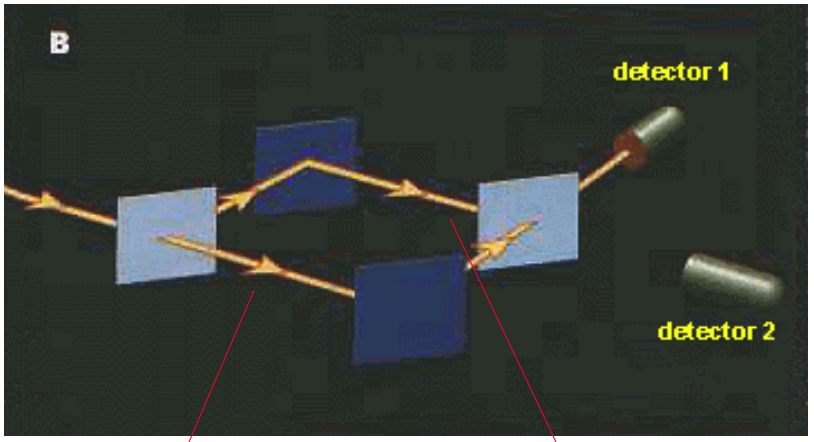
Lecture 1:
Quantum Communication: A primer

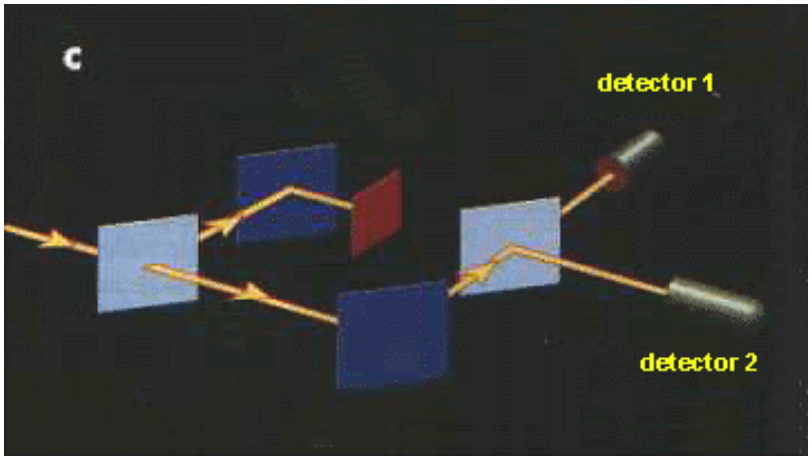
Bill Munro

email: bill.munro@oist.jp

The brave new world

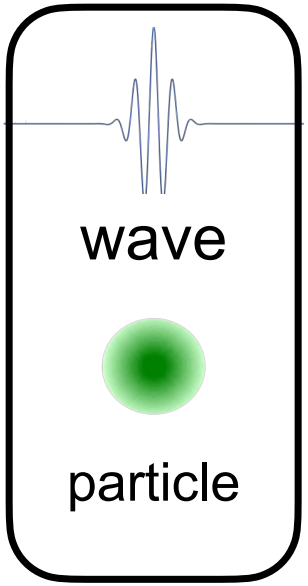






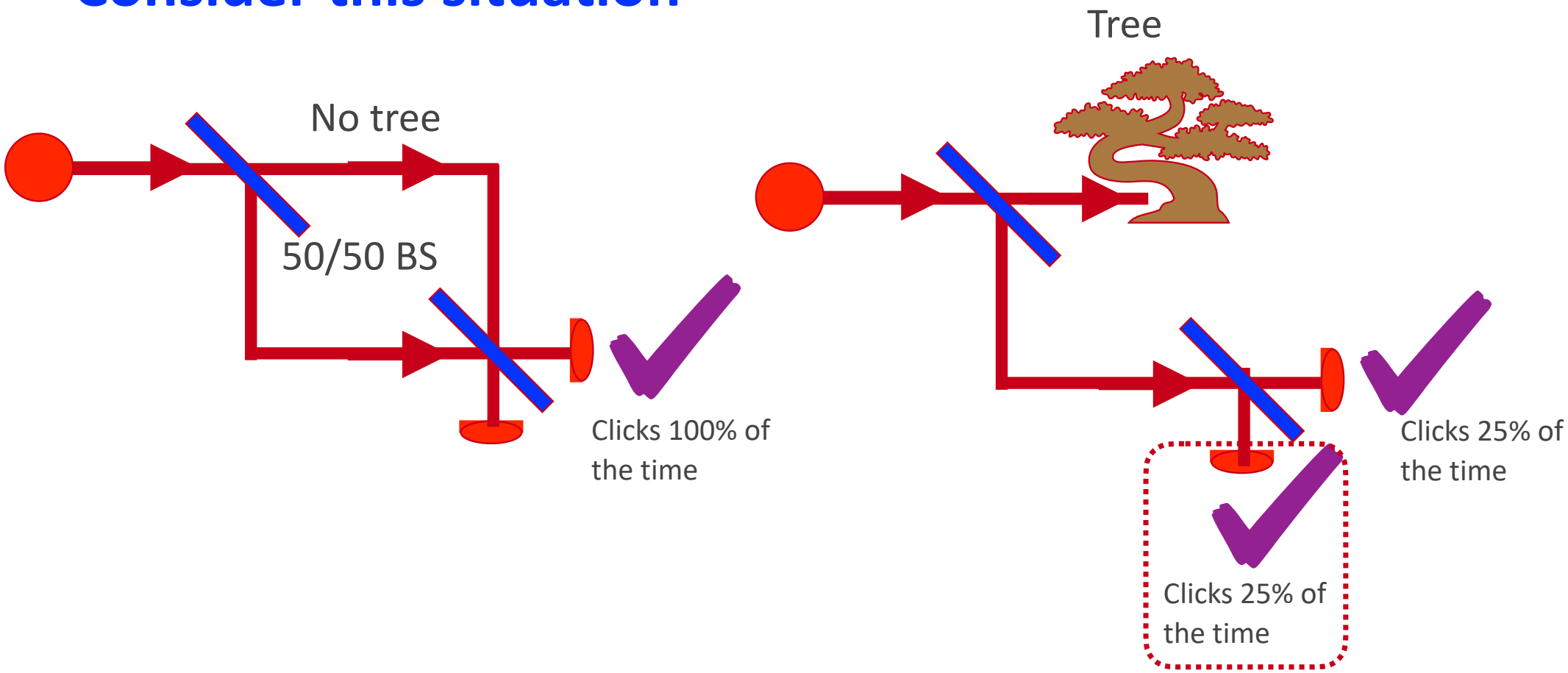
Which path is taken?

BOTH



Observing without looking

- **Consider this situation**



- **Known as interaction free measurements or ‘quantum bomb’ detection**

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Quantum technology: the second quantum revolution

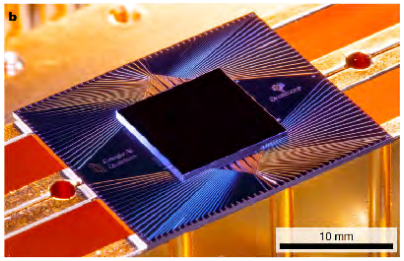
Jonathan P. Dowling and Gerard J. Milburn

Phil. Trans. R. Soc. Lond. A 2003 **361**, 1655-1674
doi: 10.1098/rsta.2003.1227

We are currently in the midst of a second quantum revolution. The first quantum revolution gave us new rules that govern physical reality. The second quantum revolution will take these rules and use them to develop new technologies. In this review we discuss the principles upon which quantum technology is based and the tools required to develop it.

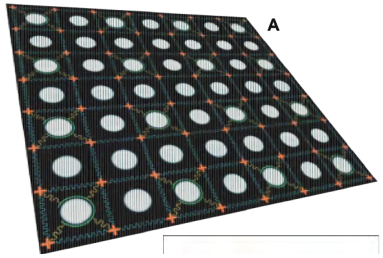
The move to the quantum regime

- **The quantum regime is interesting !!!**
  - We already have a range of small scale quantum technologies including NISQ processors, quantum sensors & quantum clocks.
  - The NISQ processors involve 100's of qubits



Elizabeth Gibney, Nature 574, 461 (2019)


Credit: Chao-Yang Lu/USTC



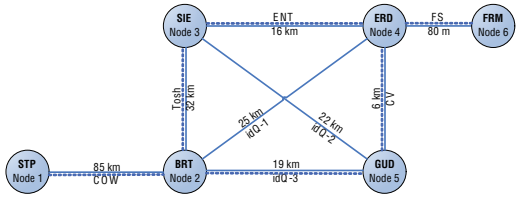
Science 372 (6545), 948 - 952 (2021)

- **Quantum communication systems are limited**
  - No large scale general purpose quantum network exists
  - Small-scale QNs have been distributed entangled resources.
    - The rate and quality of such resource is low
    - Will soon face **network issues like bandwidth, latency and congestion**

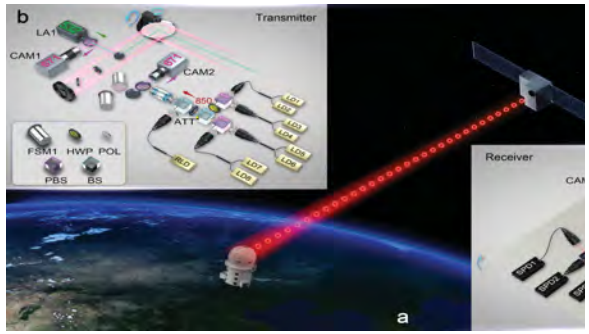
Where are we?

Range/rate limited?

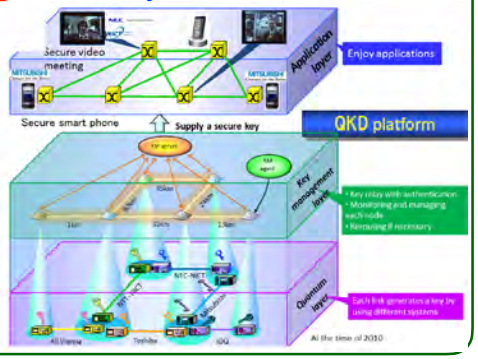
SECOQC - EU network inVienna



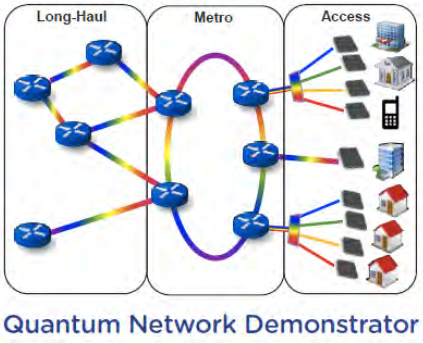
China - Q Networking satellite



Japan - Tokyo QKD network



UK - Quantum Communications Hub



Quantum Key Distribution is being tested!!!

Global Quantum Internet

How?

Quantum Communications is much more than QKD

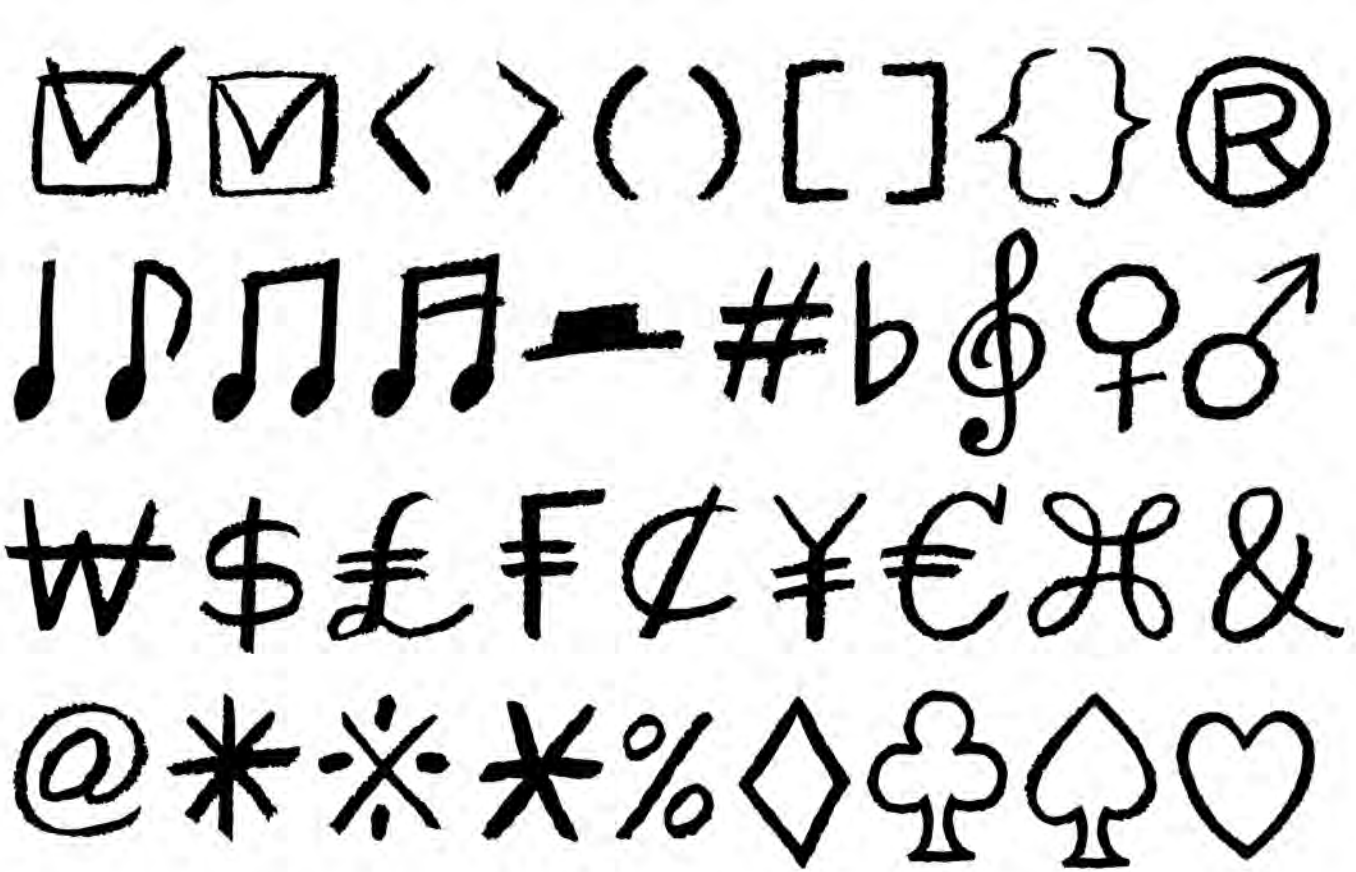
N. Gisin et. al. *Nature Photon. 1,* 165 (2007)
H. J. Kimble, 453,1023 (2008)
W. J. Munro et. al, Nature Photonics 6, 777 (2012).
K. Azuma et. al, Nature Commun. 6, 10171 (2015).

The post-quantum cryptography apocalypse will be televised in 10 years, says UK's NCSC

The UK's National Cyber Security Centre (NCSC) today started the post-quantum cryptography (PQC) countdown clock by claiming organizations have ten years to migrate to a safer future.

https://www.theregister.com/2025/03/20/ncsc_post_quantum_cryptogrpahy/

A bit of notation for the rest of the school

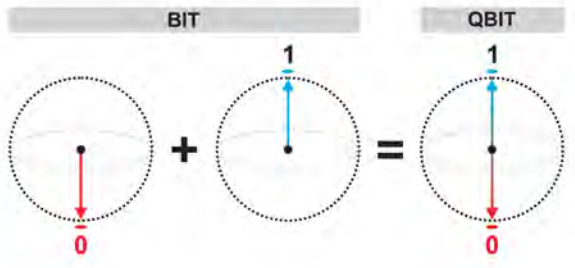


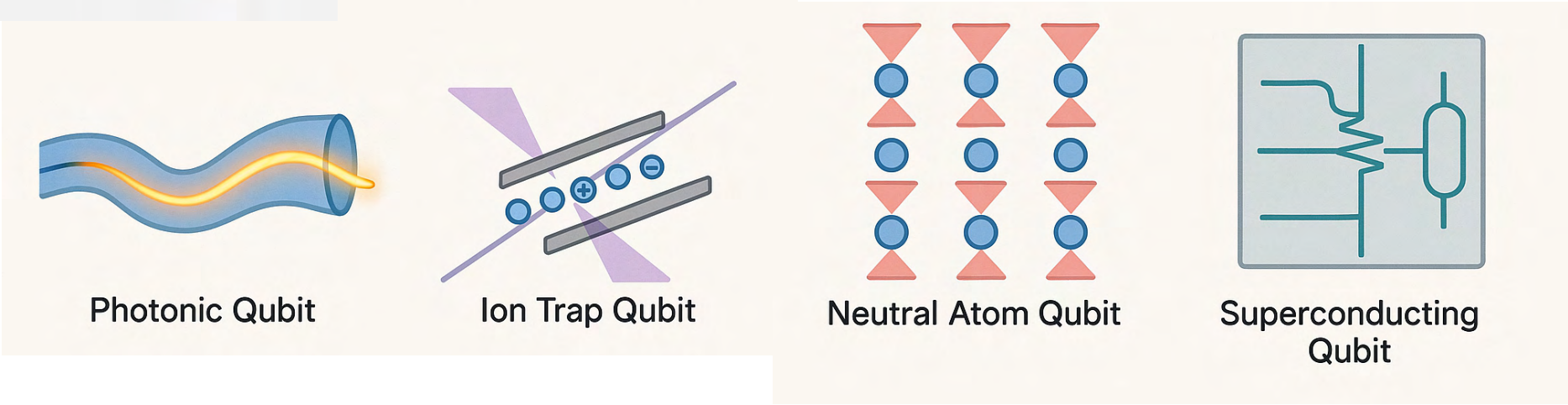
Qubits

- **A qubit (short for quantum bit) is the fundamental unit of quantum information, analogous to the classical bit in conventional computing —but with key differences that make quantum computing powerful.**

- **Unlike a classical bit, which is either 0 or 1, a qubit can exist in a superposition of both**

$$\alpha|0\rangle + \beta|1\rangle$$





Basic Qubit Quantum Gates

Identity I $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Pauli-X X $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

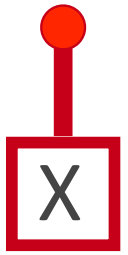
Pauli-Z Z $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Hadamard H $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

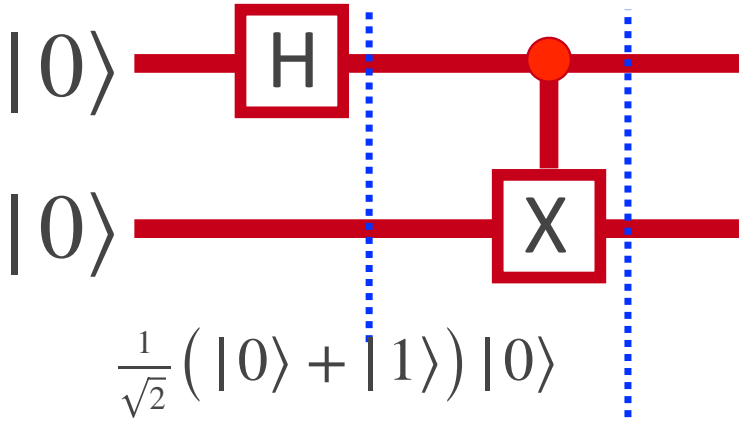
Phase S $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

$T(\pi/8)$ T $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

CNOT



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

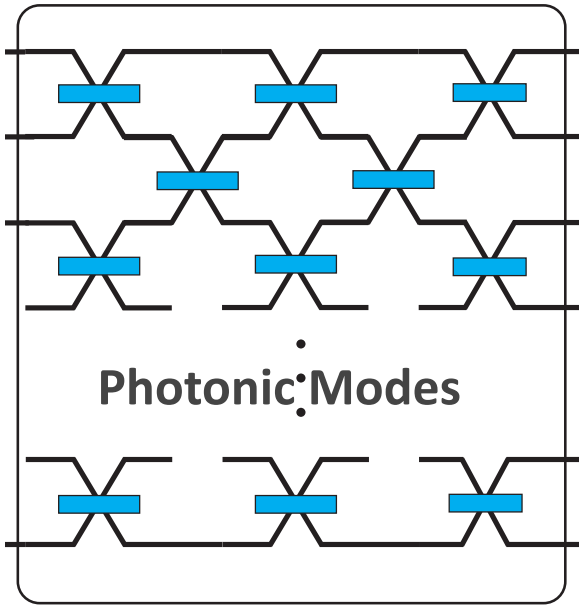
Qudits

- A qudit (short for quantum digit) is the generalization of a qubit to d-dimensional quantum systems.
- We can write them in the form

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{d-1} |d-1\rangle$$

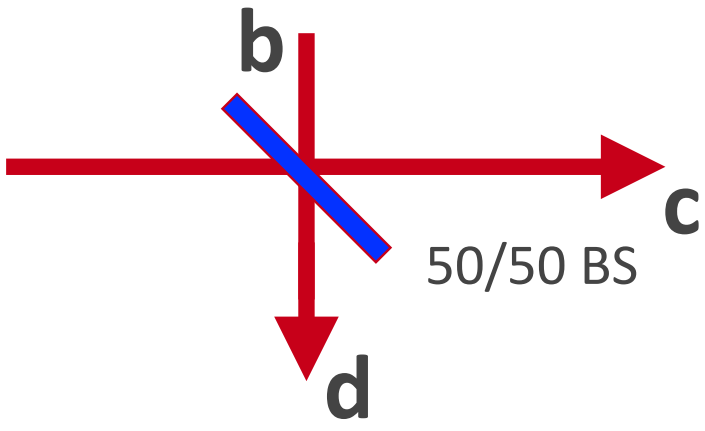
Why Use Qudits?

- More information per particle
- Many physical systems naturally have more than 2 levels.



Photons and Beamsplitters

Beamsplitters



$$c = \frac{a+b}{\sqrt{2}} \qquad d = \frac{-a+b}{\sqrt{2}}$$

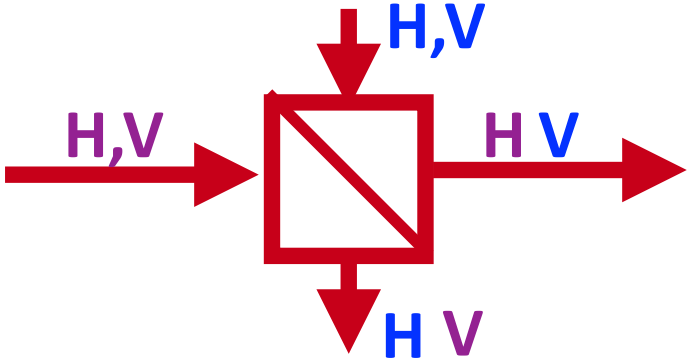
or

$$c = \frac{a+ib}{\sqrt{2}} \qquad d = \frac{ia+b}{\sqrt{2}}$$

Phase shifter

$$c = ae^{i\theta}$$

Polarization Beamsplitters



Quantum Random Number Generators

- **Depending on the amount of trust on the quantum device:**

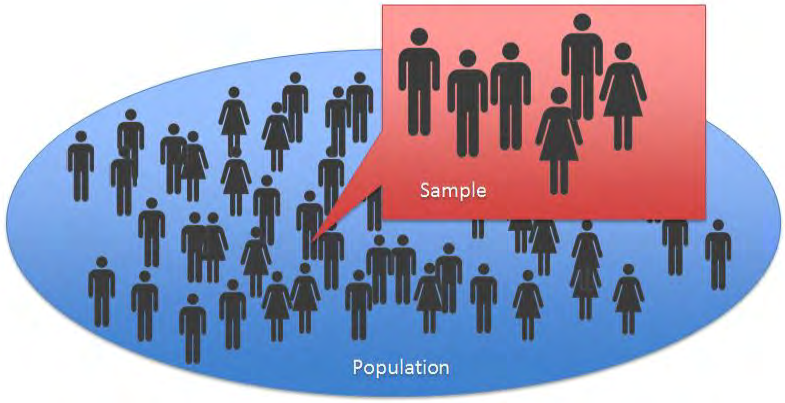
- Device-dependent QRNG
- Semi-device-independent QRNG
- Device-independent QRNG

robustness

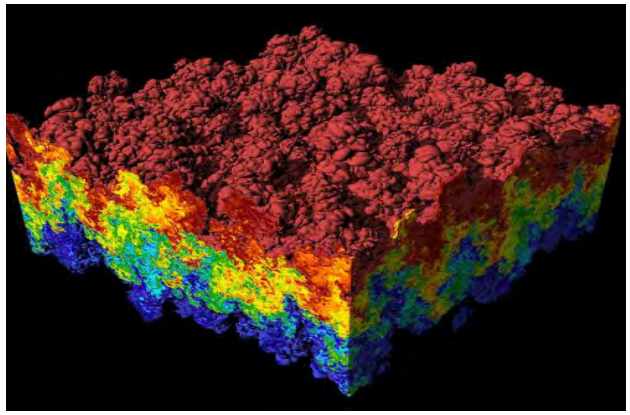
practicality

Why is randomness important?

Gambling



Sampling

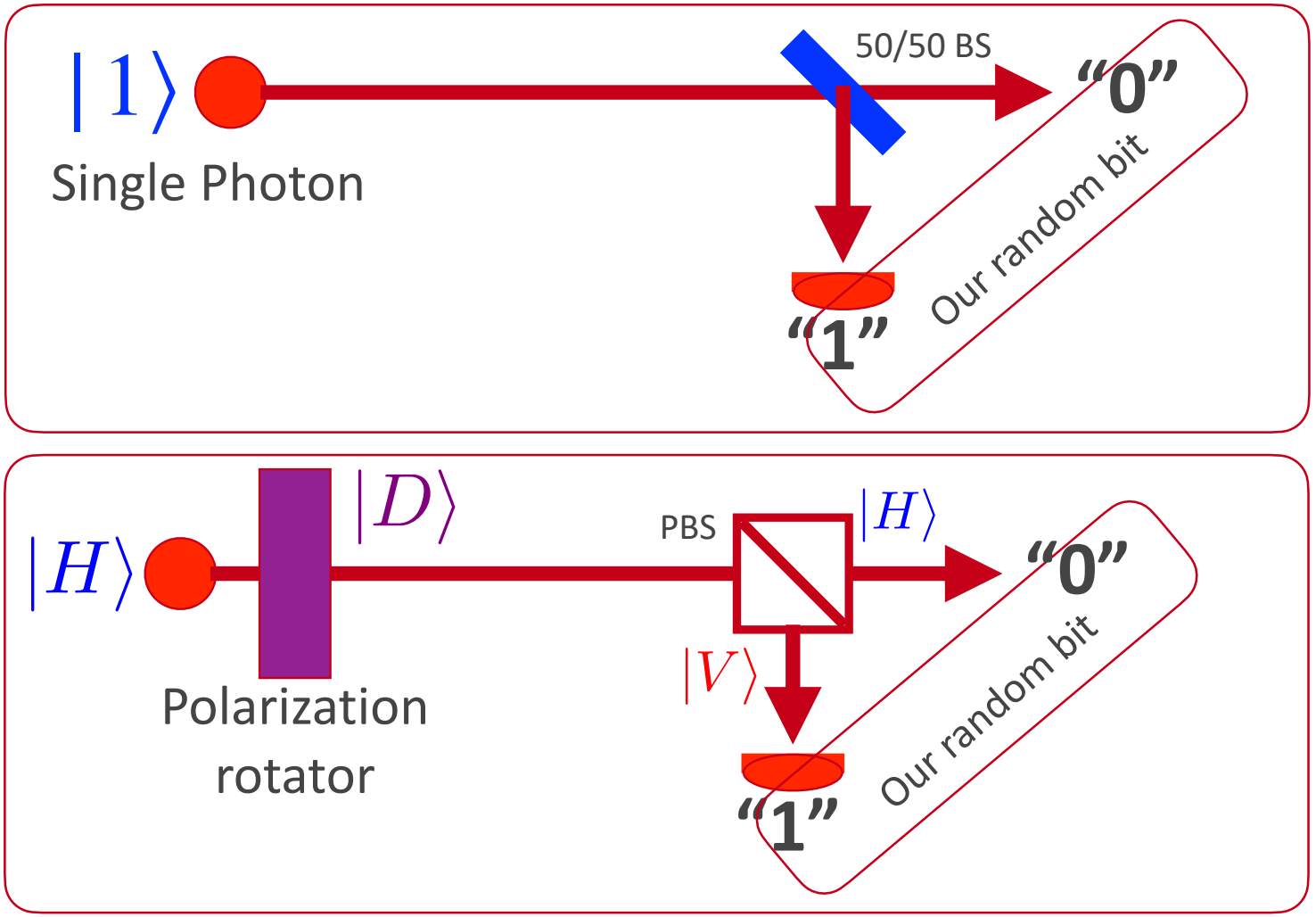


Simulation

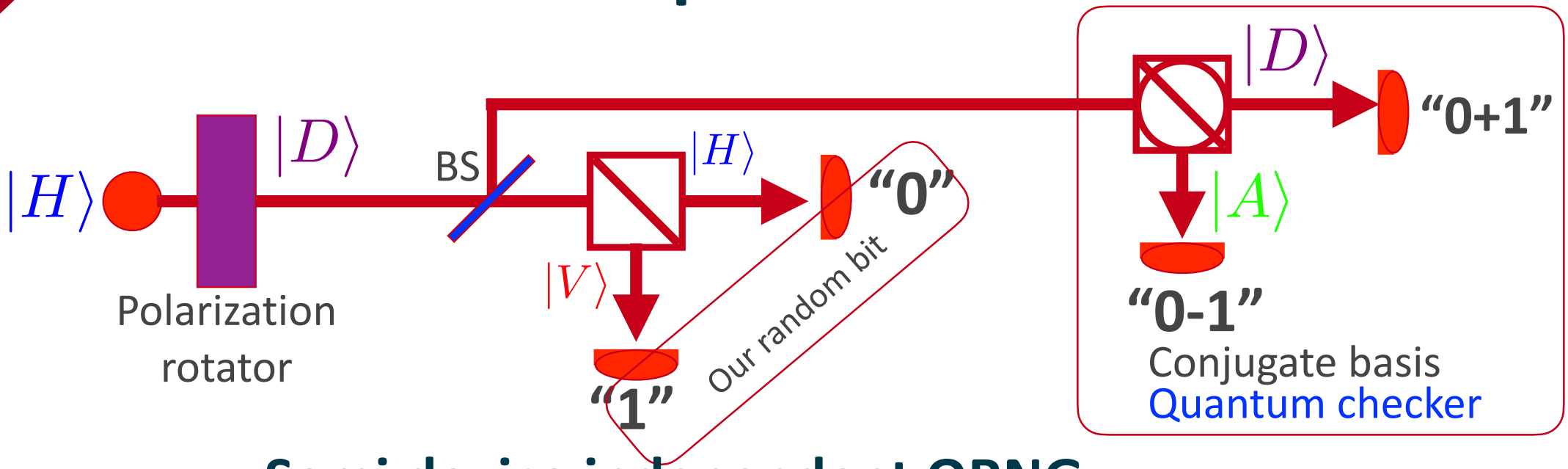
Cryptography

Couresty Yanbao Zhang (NTT BRL)

The Simplest QRNG



The next level - quantum certification



Semi device independent QRNG

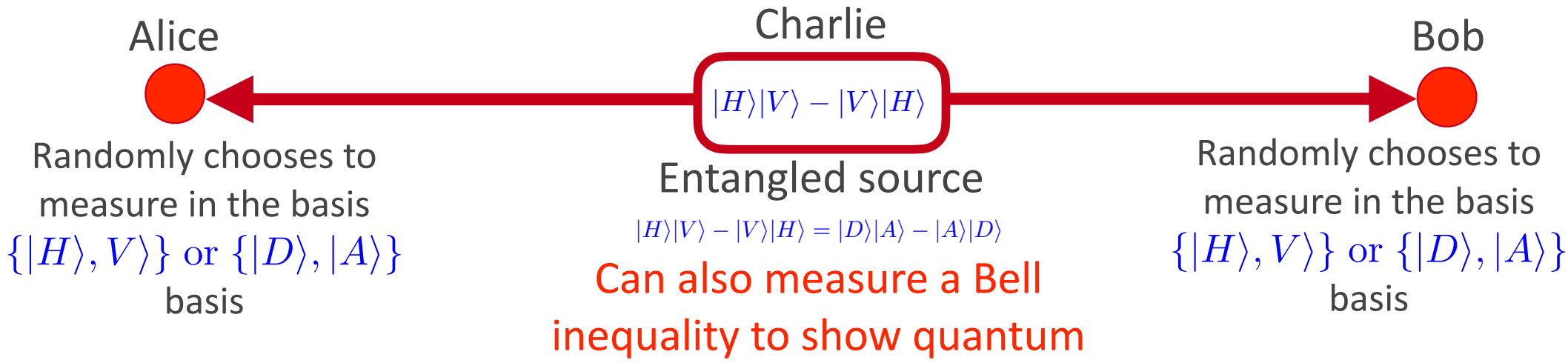
- Still in the labs - but is the next generation
- Certification is built in
- Safe against quantum attacks!!!!
- Ultimate level would be device independent QRNG

SiP

OIST | Quantum

Entanglement based QRNG

- So far we have been using superposition. What about entanglement?



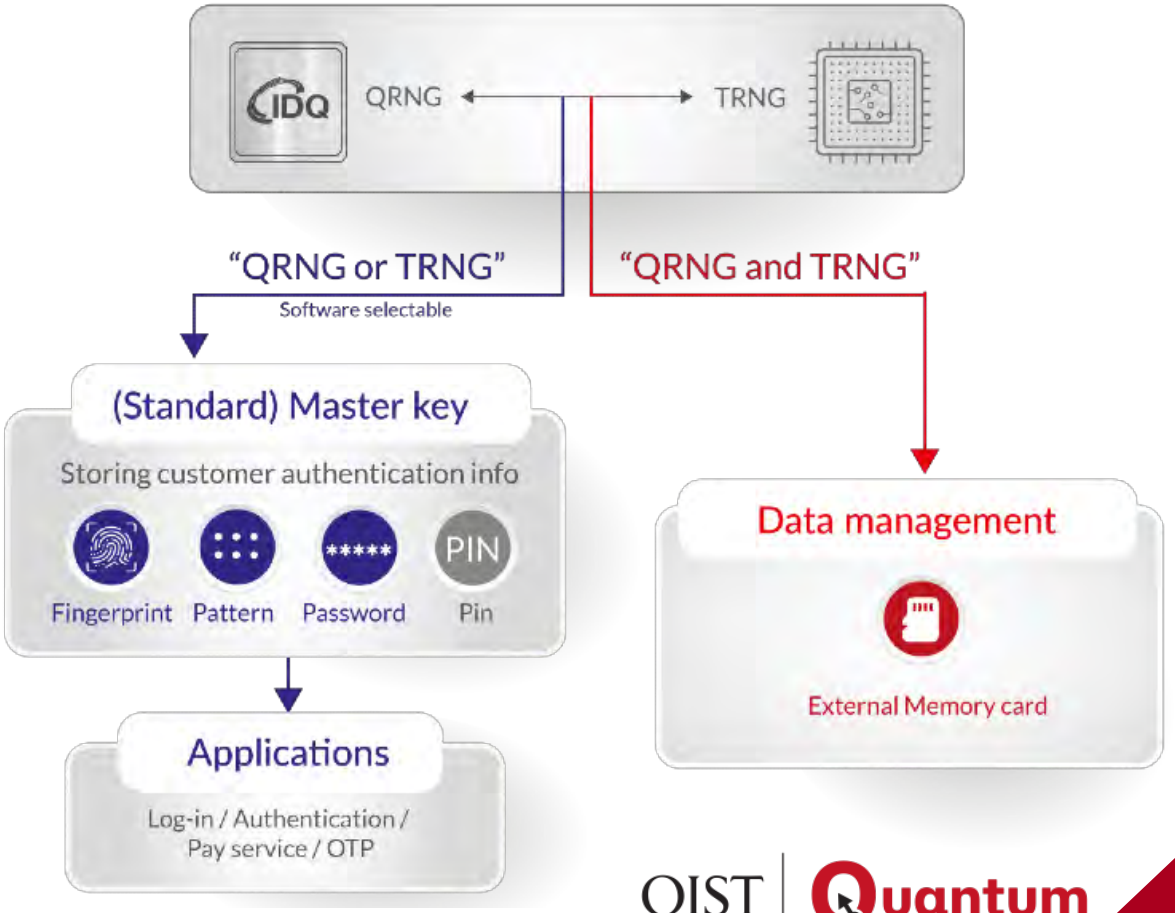
- Alice and Bob only keep the cases when they both received in the same basis - so need to communicate that and not the bit value

QRNG Use Case

QRNG 칩셋

2025

Samsung Galaxy Quantum 5



https://www.idquantique.com/random-number-generation/qrng-use-cases/samsung-qrng-use-case/

OIST | Quantum

QRNG Revisited

2025

Samsung Galaxy Quantum

QRNG - 2.5mm x length 2.5mm

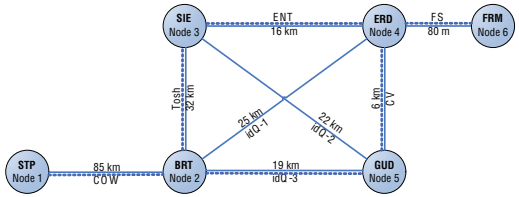
https://www.idquantique.com/random-number-generation/qrng-use-cases/samsung-qrng-use-case/

Quantum Key Distribution

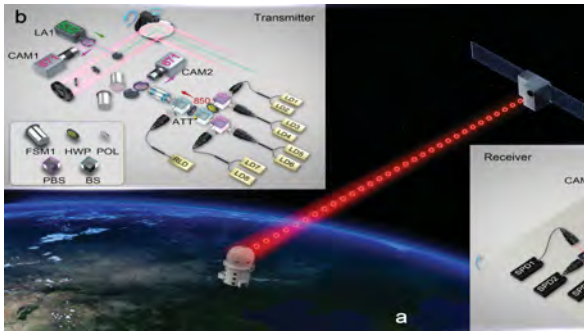
Where are we?

Range/rate limited?

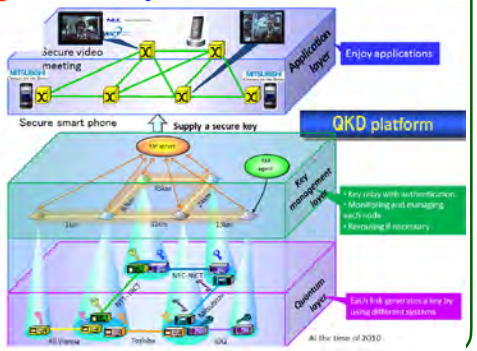
SECOQC - EU network inVienna



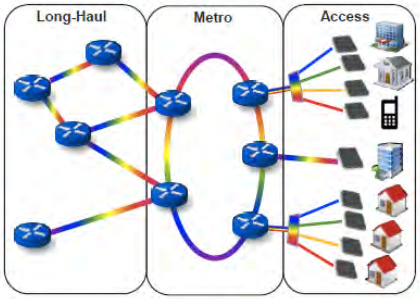
China - Q Networking satellite



Japan - Tokyo QKD network



UK - Quantum Communications Hub



Quantum Network Demonstrator

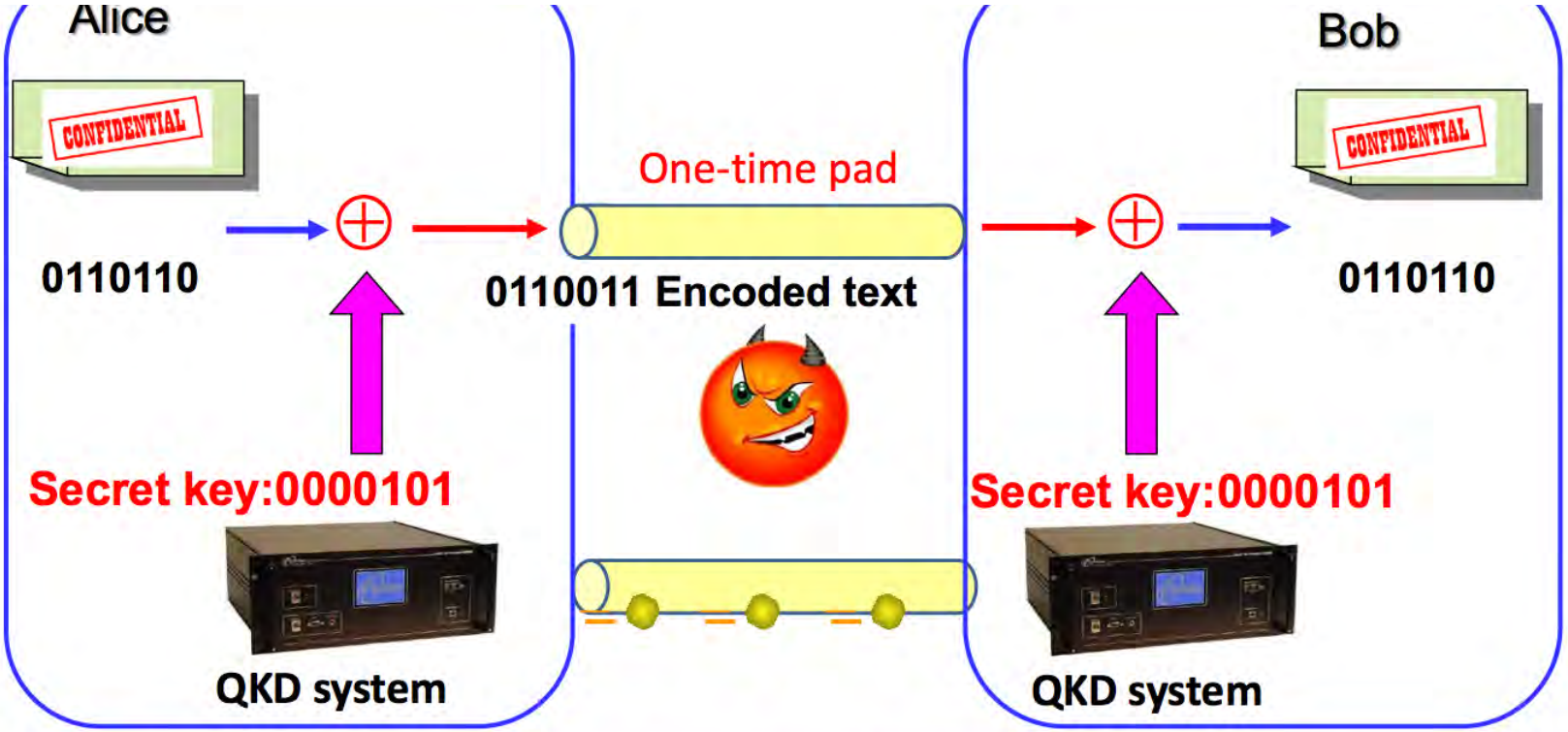
Quantum Key Distribution is being tested!!!

N. Gisin et. al. *Nature Photon. 1,* 165 (2007)
H. J. Kimble, 453,1023 (2008)
W. J. Munro et. al, Nature Photonics 6, 777 (2012).
K. Azuma et. al, Nature Commun. 6, 10171 (2015).

SiP

OIST | Quantum

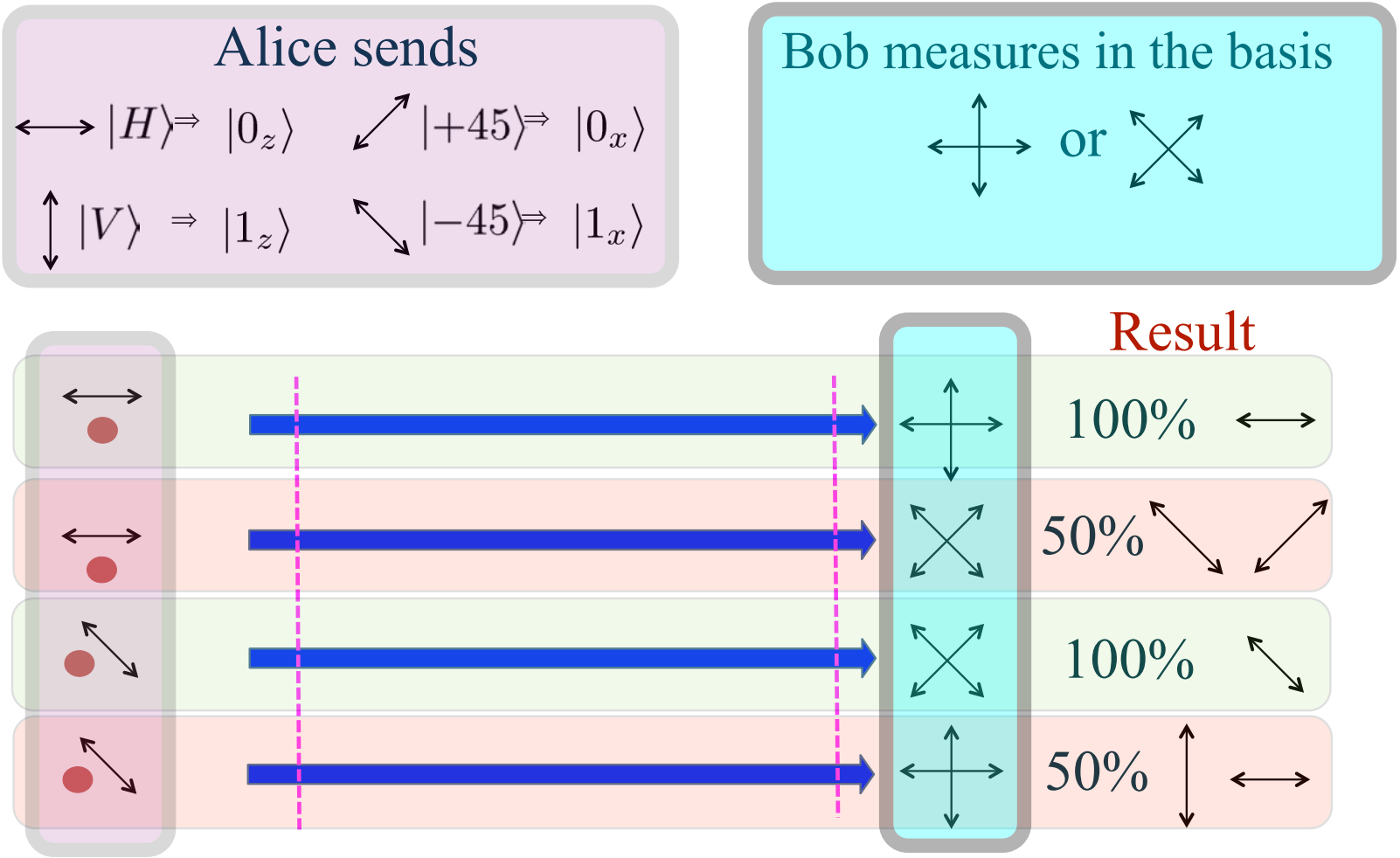
Quantum Key Distribution



QKD can achieve the unbreakable security, i.e., security against arbitrary attacks ☺

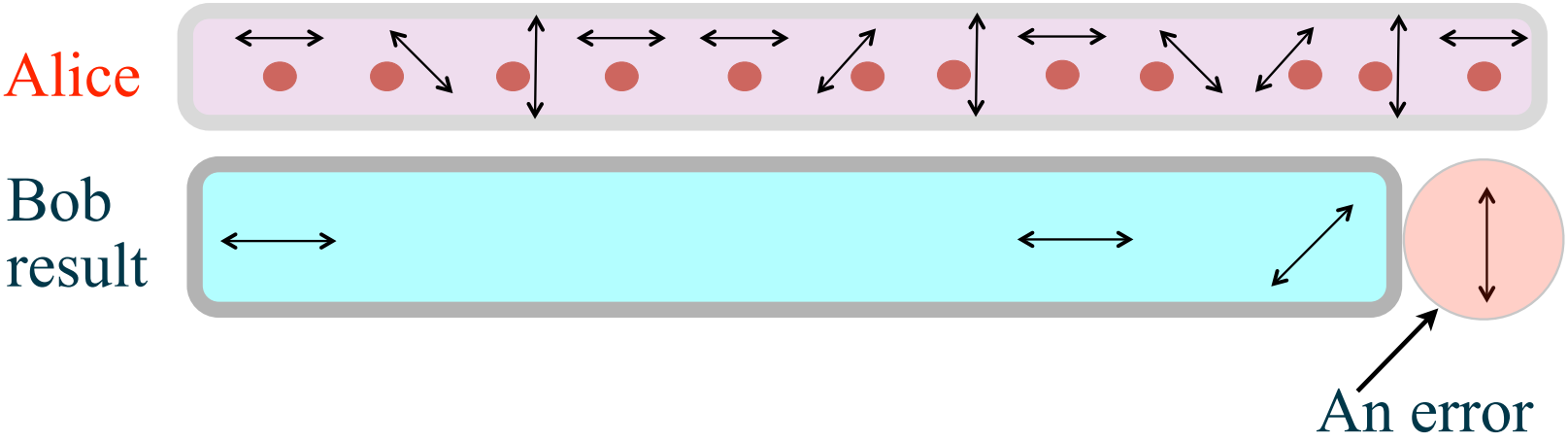
BB84 QKD

- Let us look at this protocol in a little more detail



BB84 QKD

- Lets look at a sequence of photons sent



- So Alice and Bob now have a sequence of shared bits

Alice: 0110101001110100011101....
Bob: 0100101001010100111101....

Error assumed to be caused by Eve

- What about the errors?

BB84 QKD Errors

Information reconciliation: Simplest is the cascade protocol

- Divide Alice and Bob raw key into blocks
- Block size chosen so not more than 1 error on average per block

Alice: 01101010 01110100 01101....

Bob: 01001010 01110100 01101....

- Calculate parity: e/o e /e ….
- Look at the blocks where parity disagrees and divide into smaller block

Alice: 0110 1010 ....

Bob: 0100 1010 ....

Completely discard this block. **Why?**

- Calculate parity: e/o e /e ….
- Now remove 1 bit per block where parity disclosed:

Alice: 101 0111010 01101....

Bob: 101 0111010 01101....

BB84 QKD Errors

Privacy amplification:

- Alice and Bob have the same shared sequence of key material

Alice: **101 0111010 01101....**
Bob: **101 0111010 01101....**

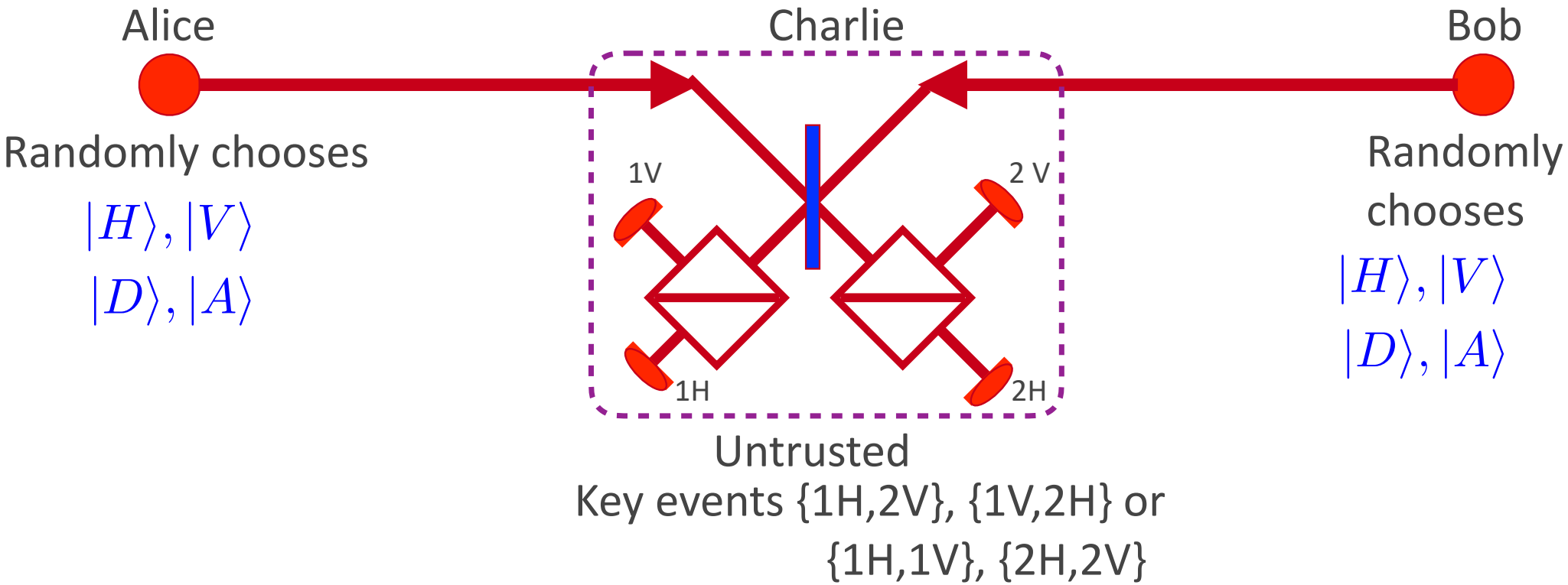
- Remember the QBER - that is assumed to be the information Eve has

- **Privacy amplification** is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key.

- **Use a universal hash function:** takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length.

We should now have shared random key material

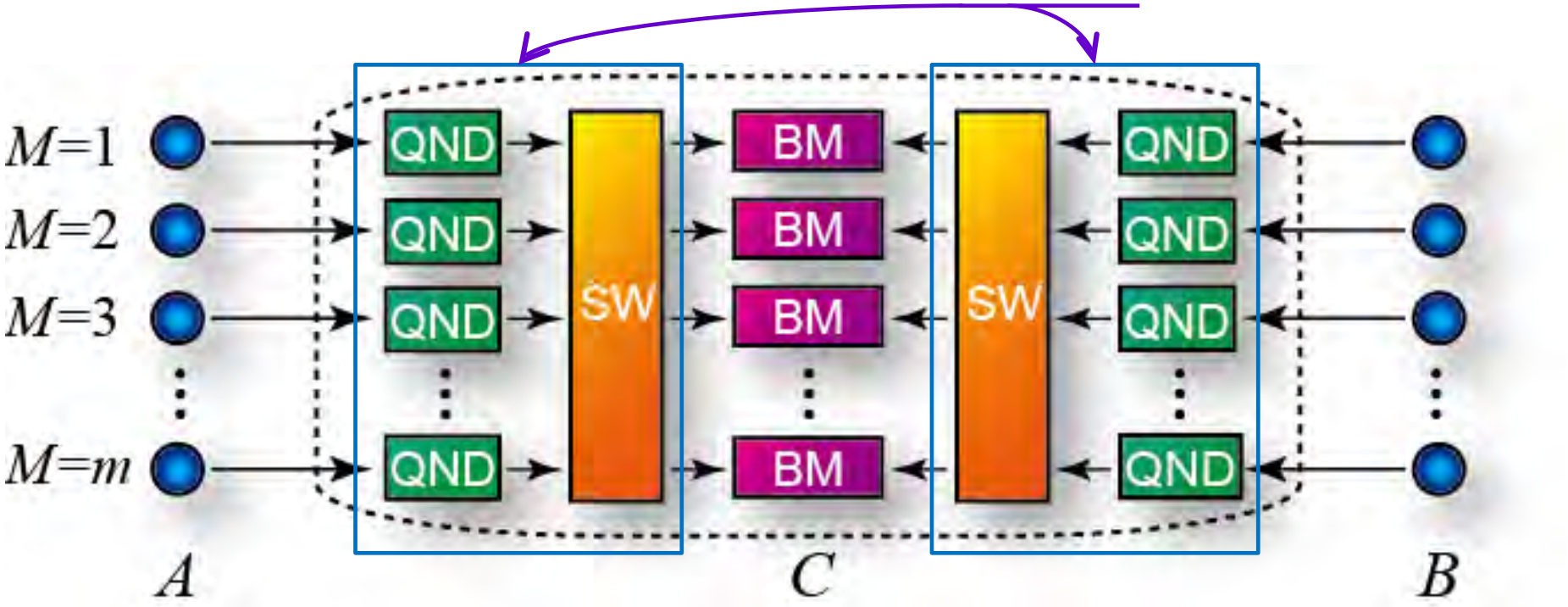
Measurement device independent QKD



- After Charlie indicates the measurement result, Alice and Bob only the cases when they both send in the same basis - so need to communicate that and not the bit value

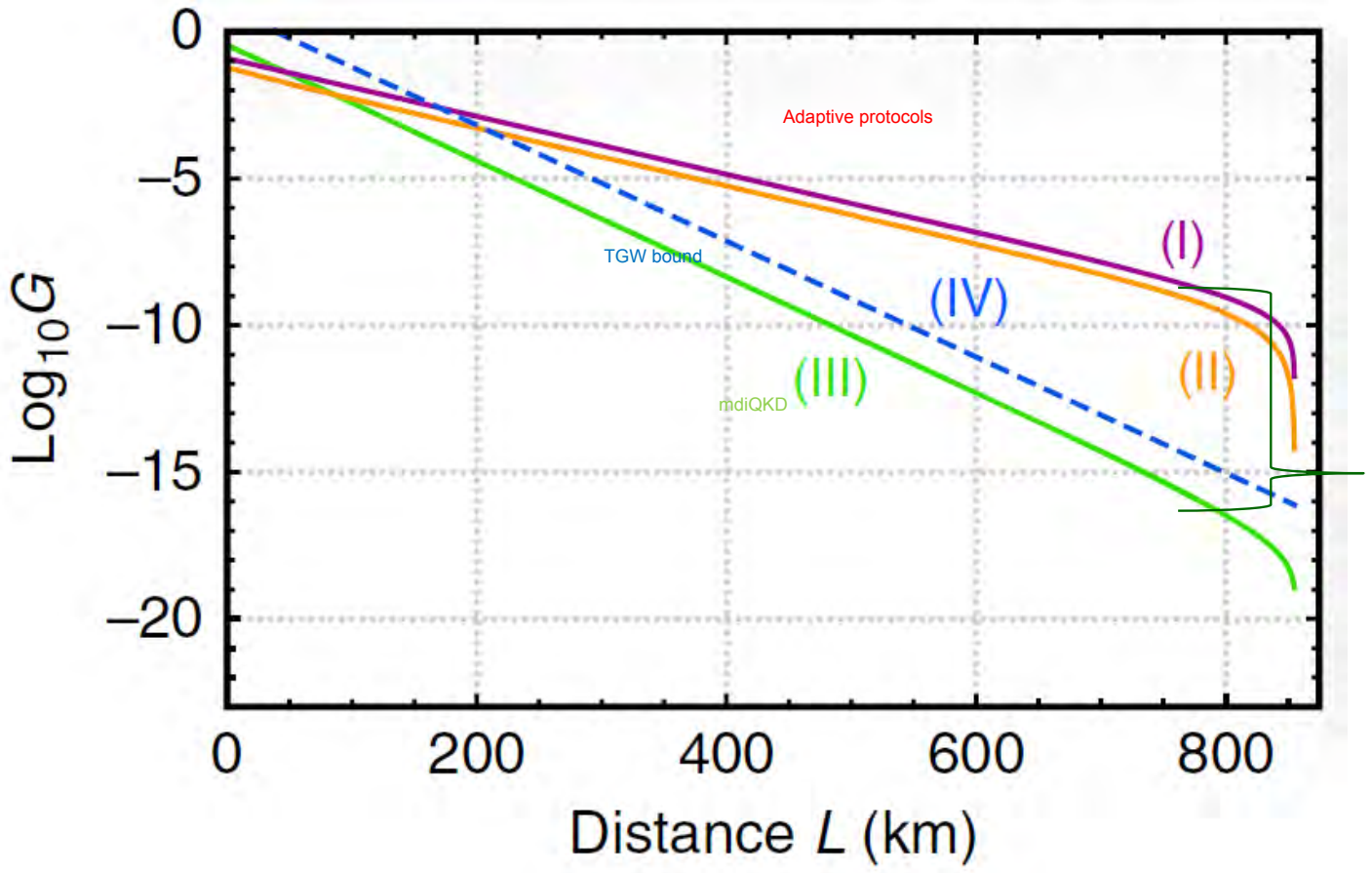
Adaptive MDI QKD

- **Replace the simply Bell state measurement with an adaptive one**



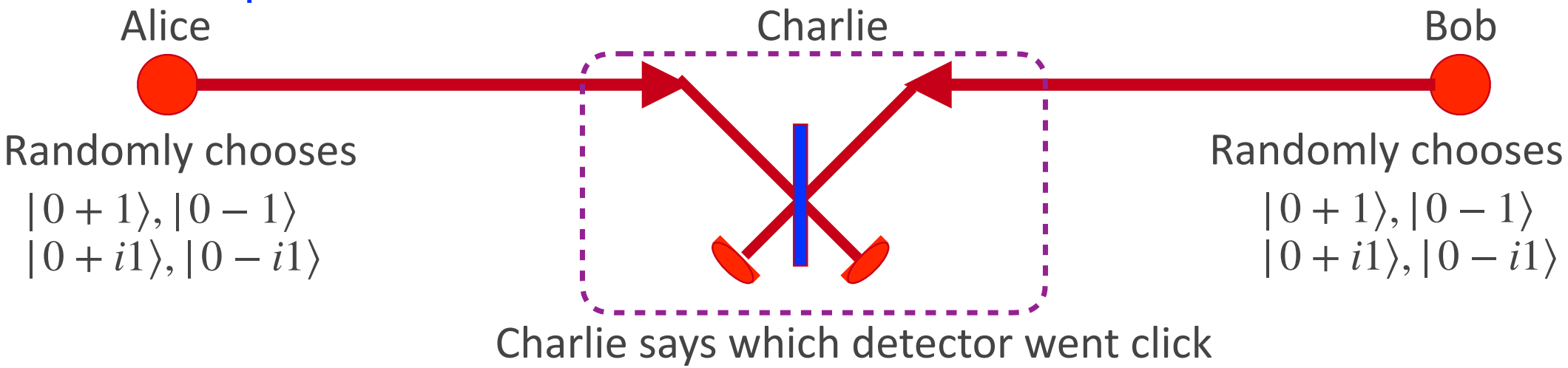
Adaptive MDI QKD

- **Replace the simply Bell state measurement with an adaptive one**

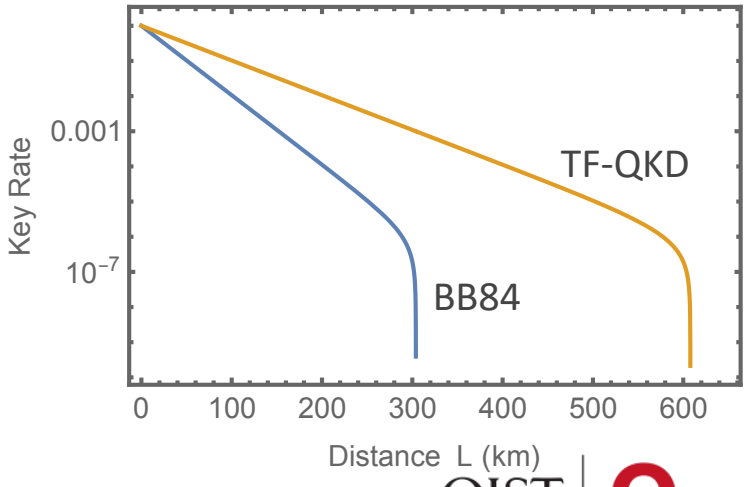


Advanced QKD Protocols: Twin field QKD

- A conceptual view

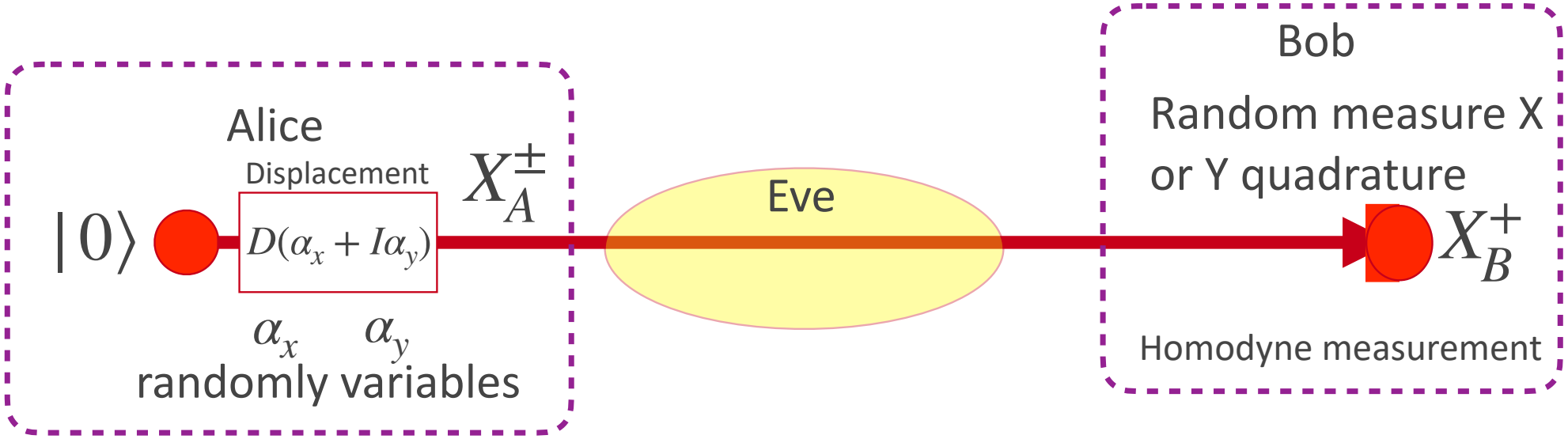


- The RHS figure shows the performance difference compared to BB84
- We observe that for the same key rate we can go twice the distance. Why?
- Hint: The photon travel half the distance



Advanced QKD Protocols: CV QKD

- Why Continuous variables?
  - Much more comparable with existing telecommunications systems



  - Will not go through the maths - but the systems tend to have higher rates at shorter distances
  - Currently not secure over long distances

SiP

OIST | Quantum

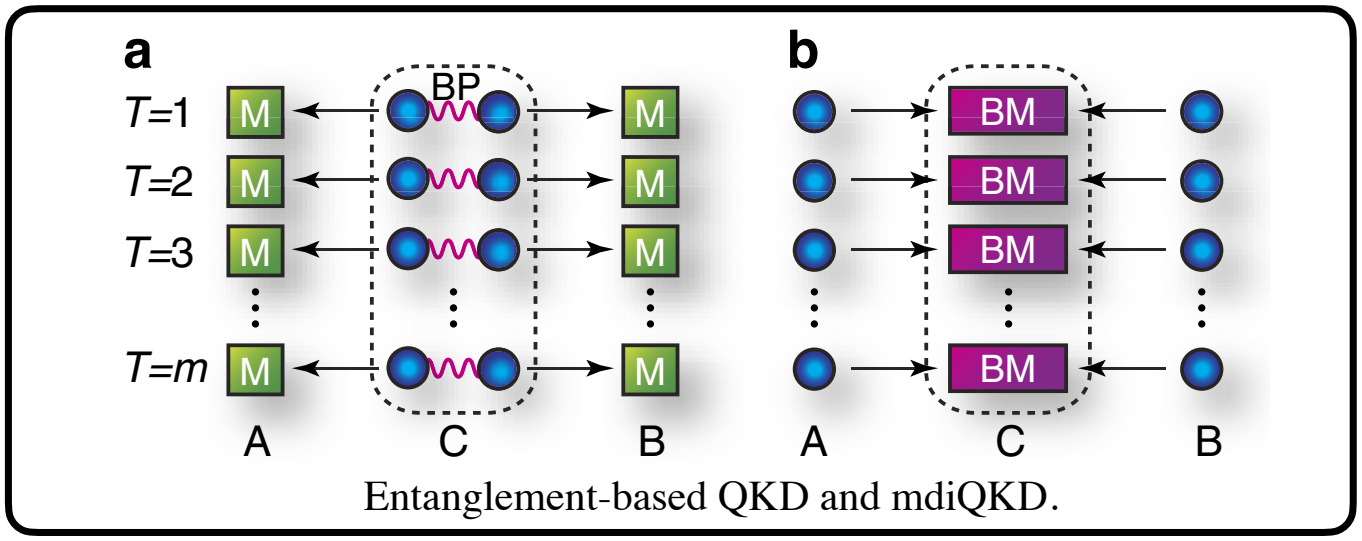
QKD in the commercial world

- Vendors:
  - Multiple vendors worldwide

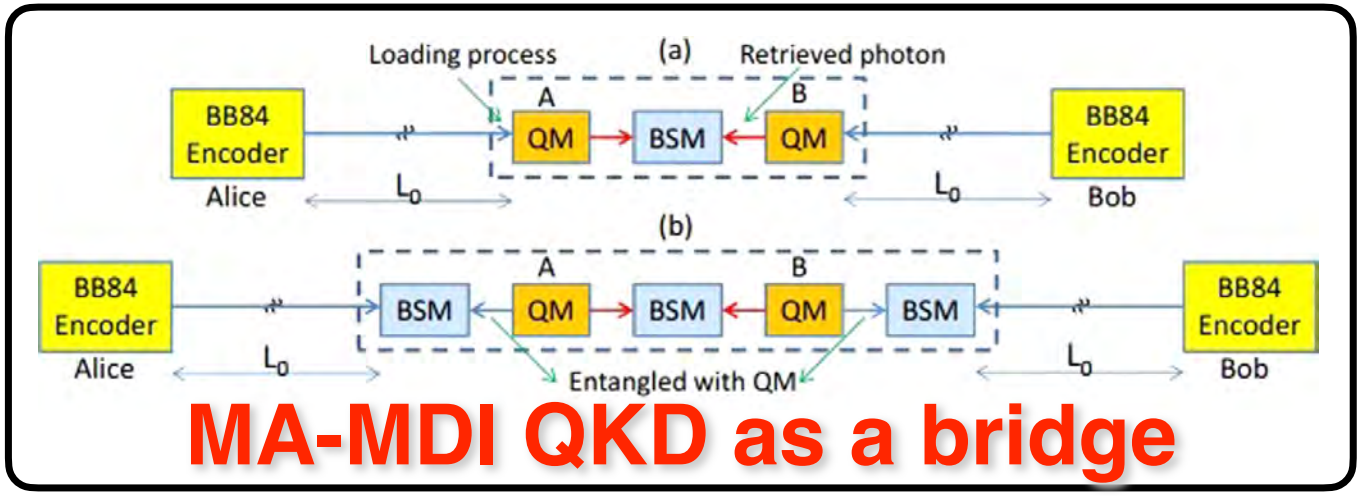
- Secure Systems:
  - are only point to point (trusted nodes compromise security)
- Applications:
  - Securing the high speed transfer of sensitive genome data between remote sites
  - Securing front office and back office operations of major financial institutions

QKD is not a cryptography system: it is only part of one that establishes shared key material

Memory assisted MDI-QKD as a bridge

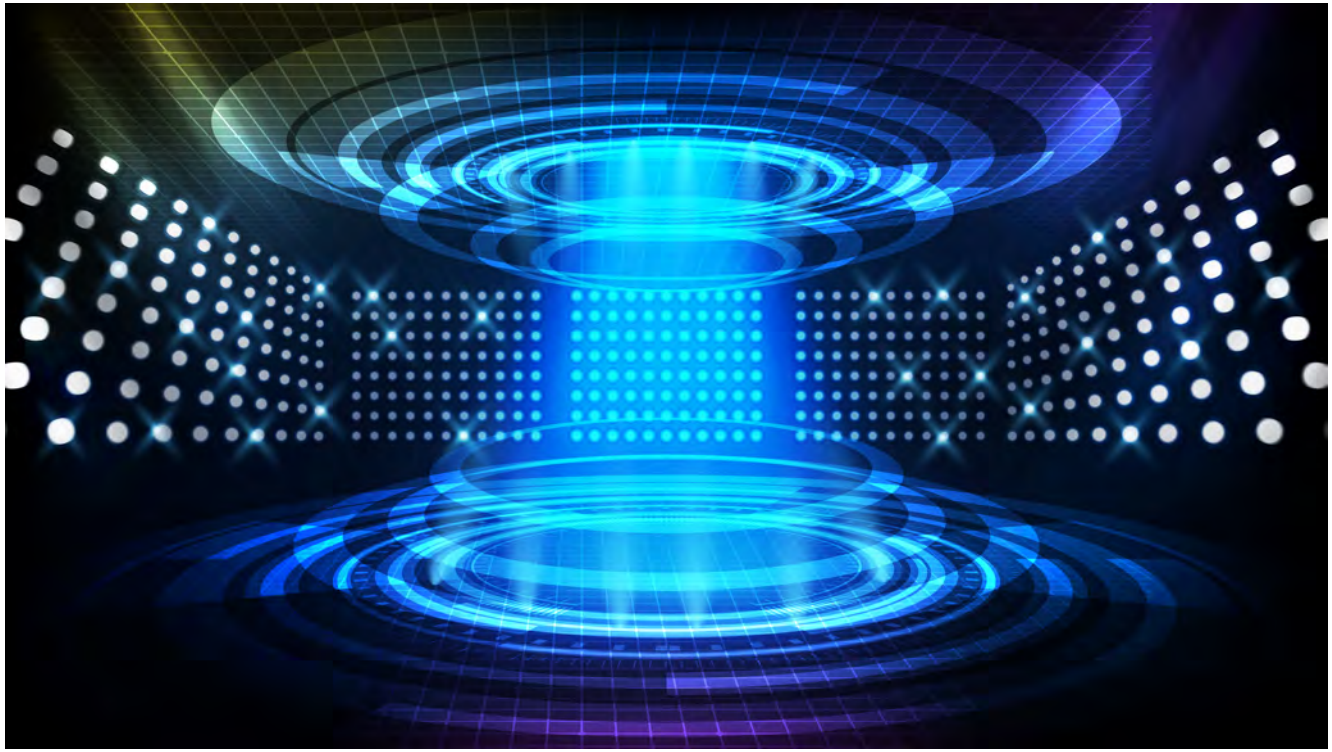


Entanglement-based QKD and mdiQKD.



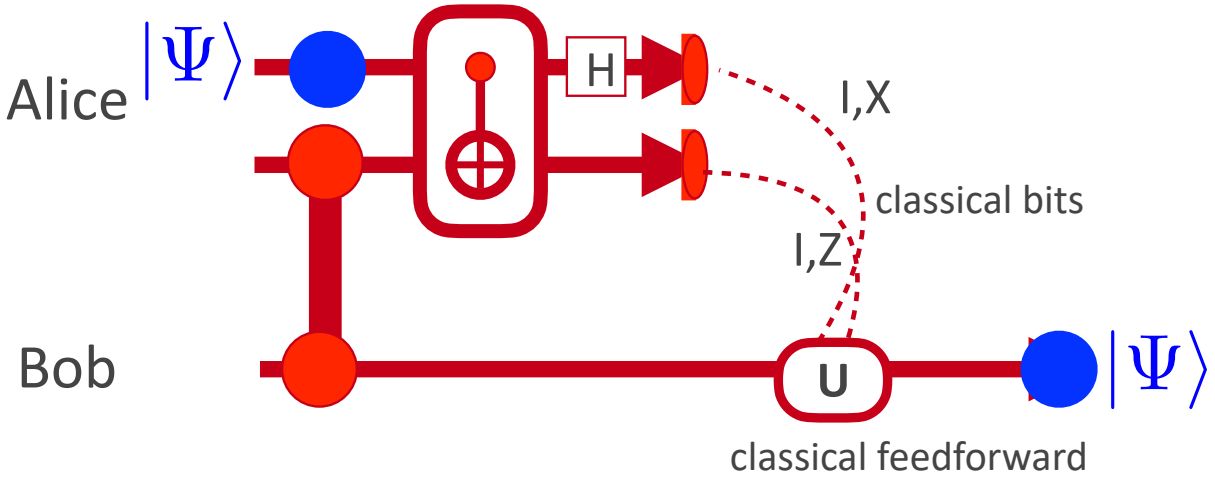
MA-MDI QKD as a bridge

Quantum Teleportation



Quantum teleportation

- The basic quantum teleportation is the most fundamental way of moving information between remote users

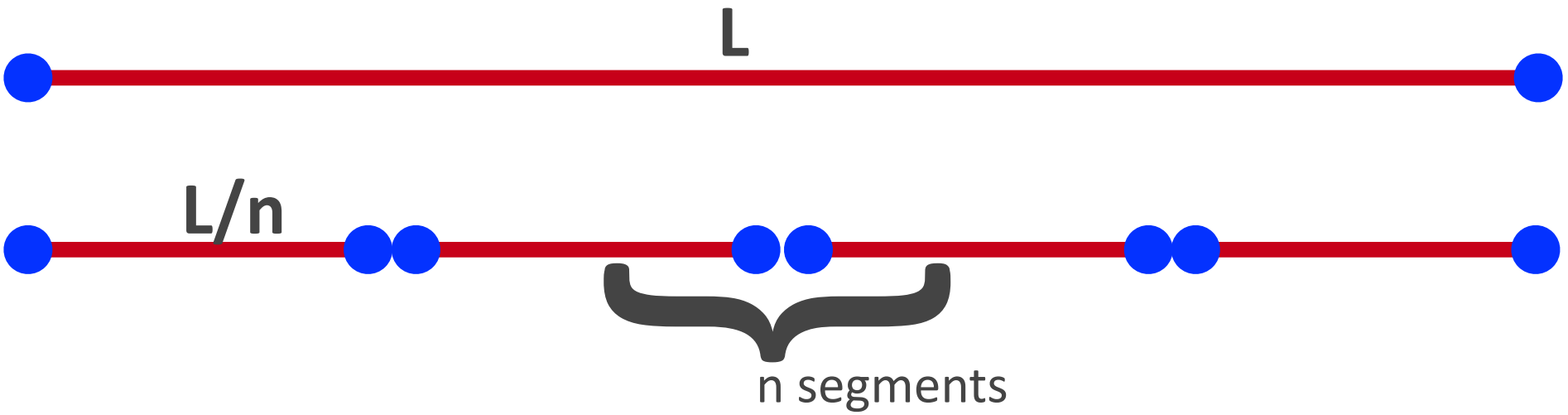


$$\{\alpha|0\rangle_A+\beta|1\rangle_A\}\{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\}$$
$$\longrightarrow \alpha|0\rangle_A\{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\}$$
$$+\beta|1\rangle_A\}\{|1\rangle_A|0\rangle_B+|0\rangle_A|1\rangle_B\}$$
$$\longrightarrow \alpha|0\rangle_B+\beta|1\rangle_B$$

with correction {I, X, Z, ZX}

- It requires that we establish an entanglement links between Alice and Bob
  - not so simple if they separated by large distances.
- We also need to send two bits of classical information from Alice to Bob as fast as we can. Bob can not use there state until it arrives - and that communication time is limited by the speed of light!!!

Generating long range entanglement



Next Lecture

This work was partially by Japan’s Council for Science, Technology and Innovation (CSTI) under the Cross-Ministerial Strategic Innovation Promotion Program (SIP) for “Promoting the application of advanced quantum technology platforms to social issues” (Funding agency: QST, Grant Number JPJ012367) and the JSPS KAKENHI Grant No. 21H04880.