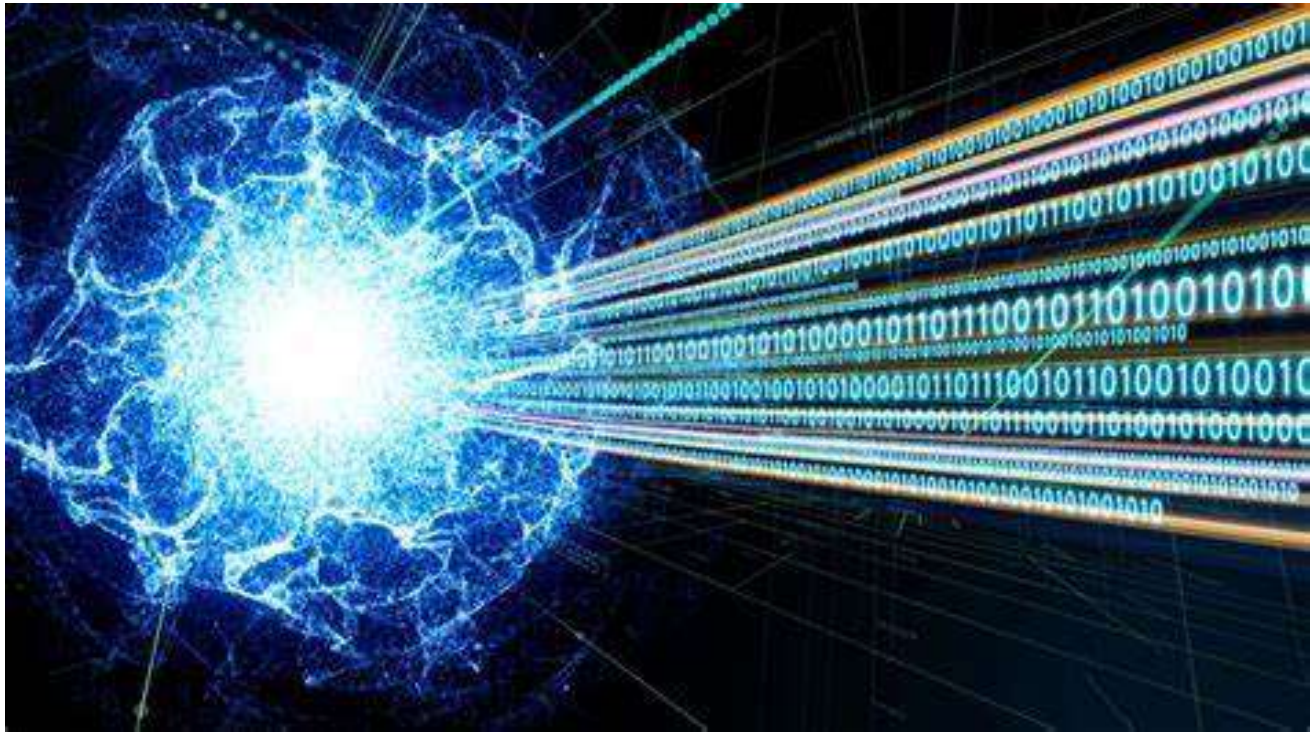
Quantum Information and Quantum Computation

Yuanyuan Chen

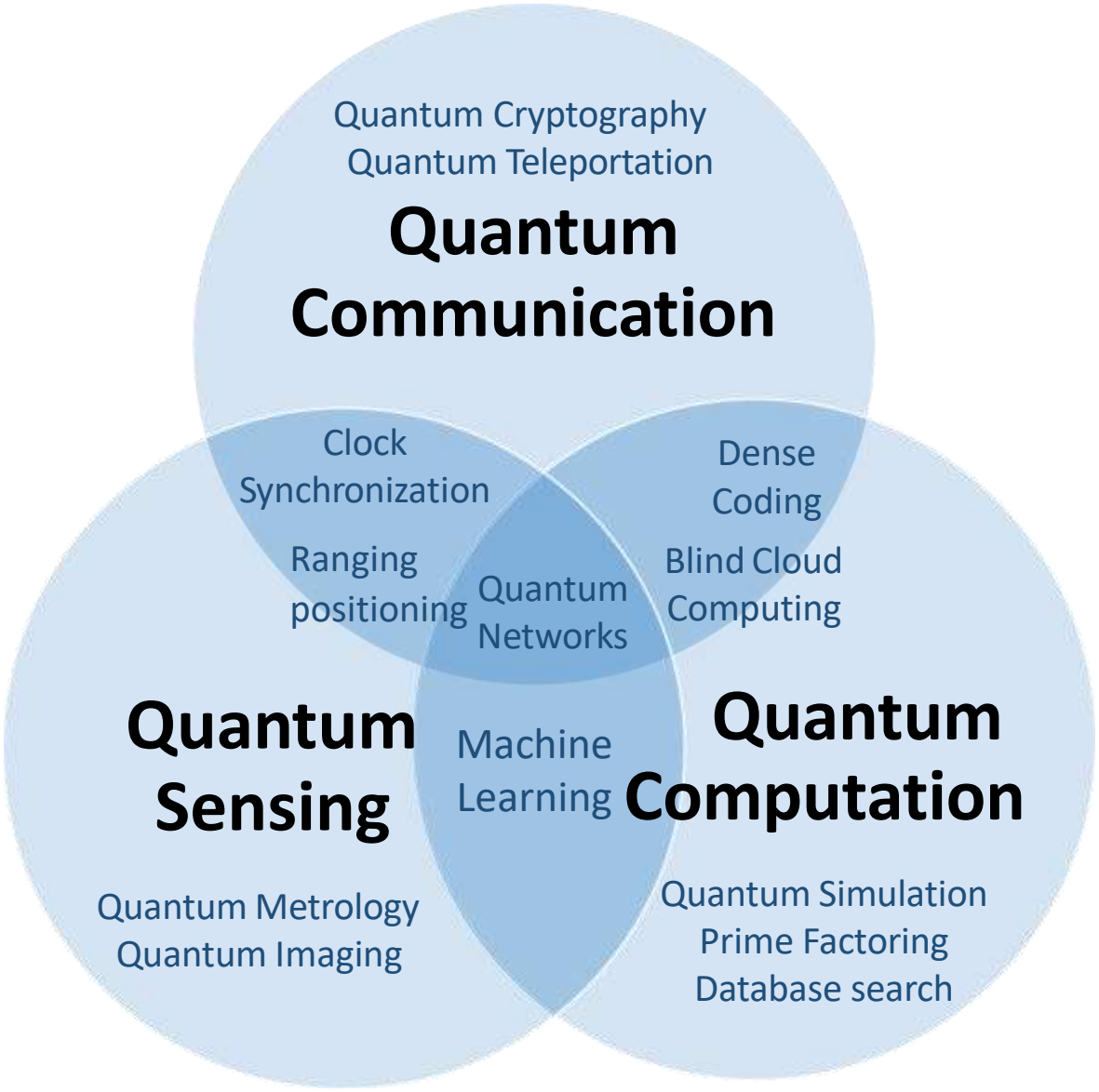
College of Physical Science and Technology
Xiamen University
Email: chenyy@xmu.edu.cn
http://qolab.xmu.edu.cn

Lecture 7

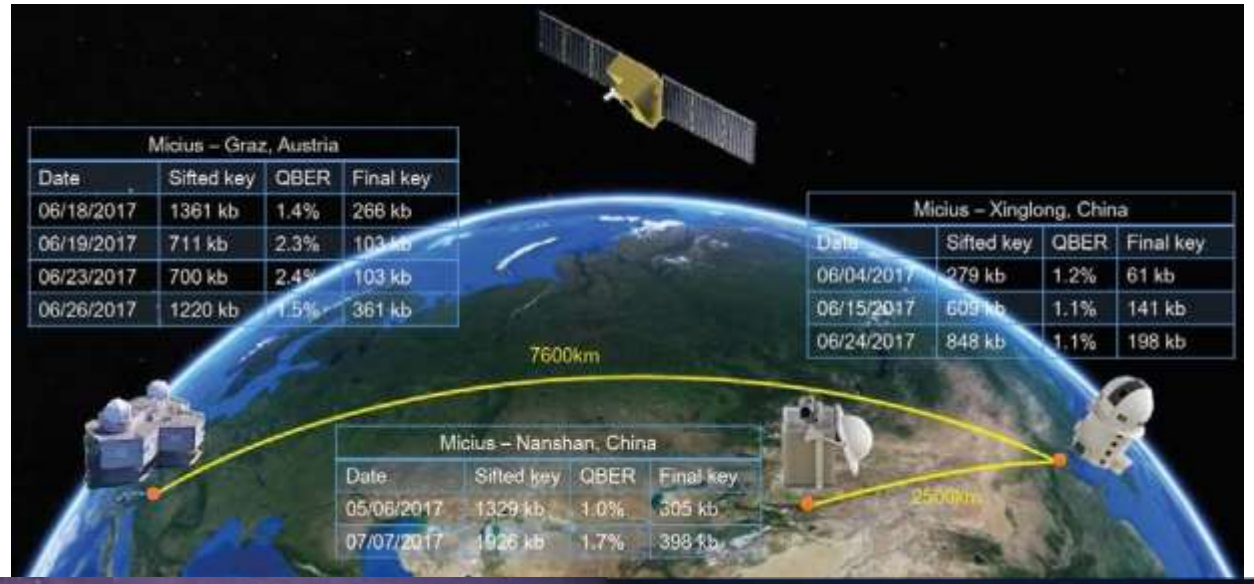
Quantum communication



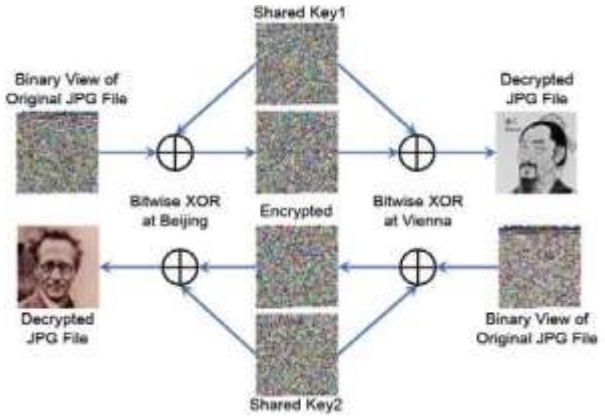
Quantum Information Processing



First intercontinental QKD session



One-time-pad encrypted image transfer



Quantum-secure Video Conference

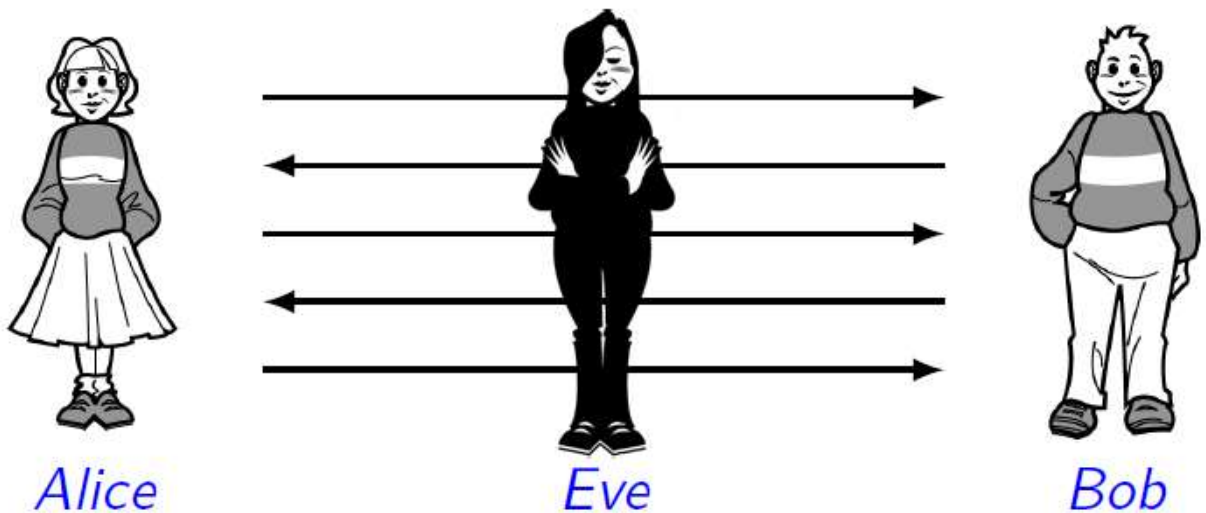
Liao et al., Phys. Rev. Lett. **120**, 030501 (2018)

Quantum information: applications

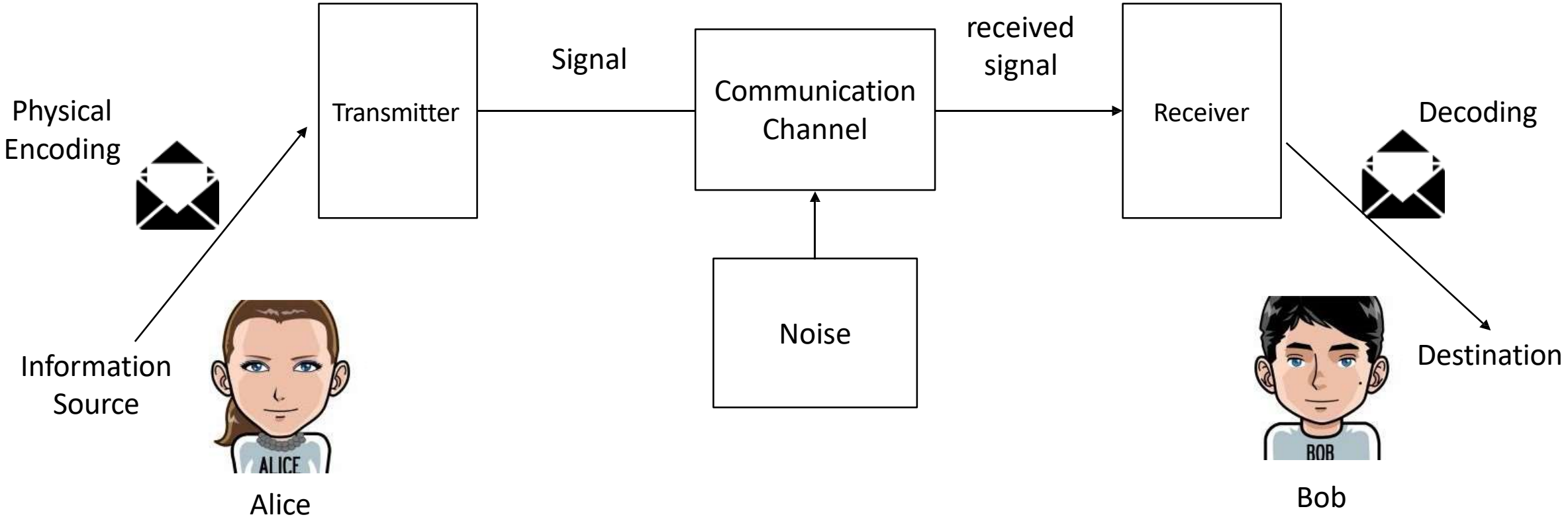
This lecture is on communication and the benefits of using quantum states to encode information. We will discuss three protocols:

- **Quantum key distribution**
- **Superdense coding**
- **Quantum teleportation**

These do not rely on quantum computation as such, but the properties of information encoded in quantum states: superposition and entanglement.



Communication



Shannon's model of a communication channel.

The history of communication is a history of *secure* communication

Skytale

a	b	c	d	e	f	g
s	c	y	t	a	l	e

as bc cy dt ea fl ge

transposition cipher

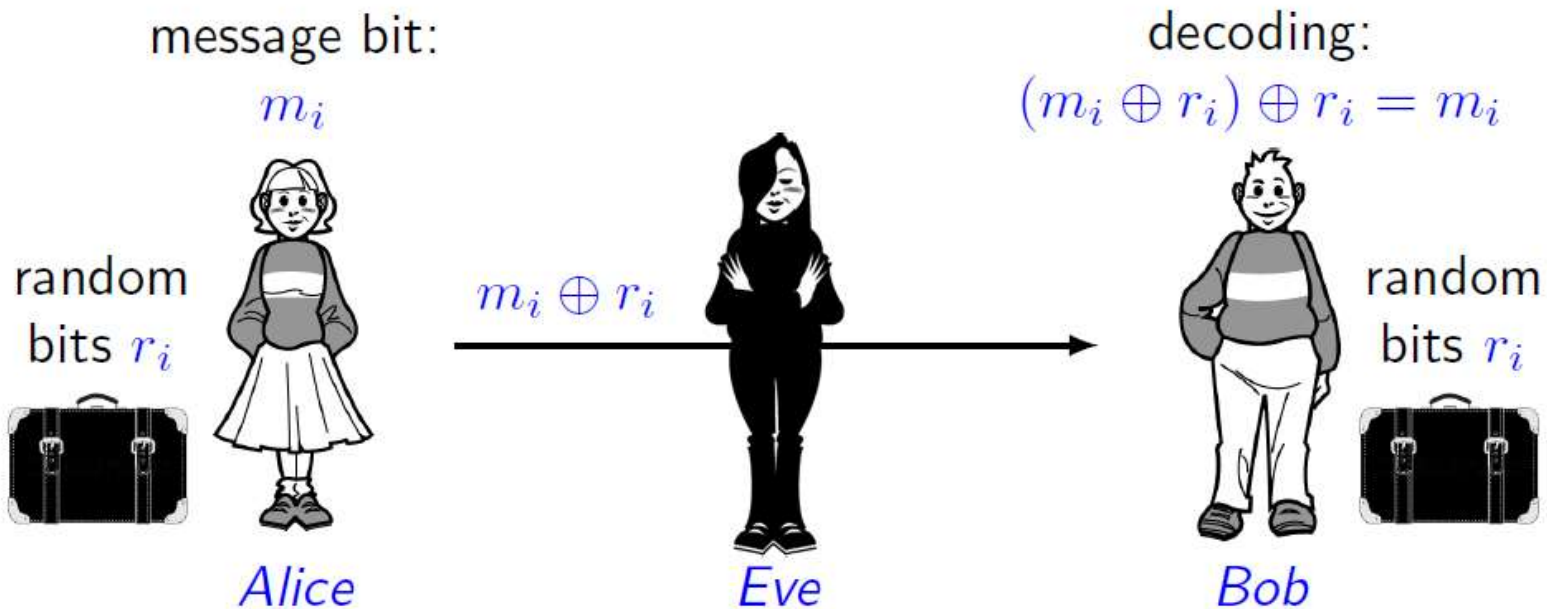
Enigma

One-time pad

Goal: Send a private message using public communication.
Protocol:

1. **Preparation:** *Alice* and *Bob* meet upfront to generate random bits $r_1, r_2, \ldots$ and both take a copy of these bits with them.
2. **Encoding:** If the i-th message bit is m_i, *Alice* sends $m_i \oplus r_i$.
3. **Decoding:** If *Bob* receives $\tilde{m}_i$, the actual message bit is $\tilde{m}_i \oplus r_i$.

Security: Eve gains no information about the message.



One-time pad

Resource trade-off: 1 shared random bit + 1 bit of public communication = 1 bit of private communication

Good:

- *Eve* gets no information about m_i as she observes a uniformly random bit (if r_i is uniform, then so is $m_i \oplus r_i$ irrespectively of m_i).
- One-time pad is unconditionally secure (there are no computational hardness assumptions).

Bad:

- The encryption key $r_1, r_2, \ldots$ is the same length as the message.
- The key cannot be replenished and should not be reused.
- How can *Alice* and *Bob* establish the key in the first place?

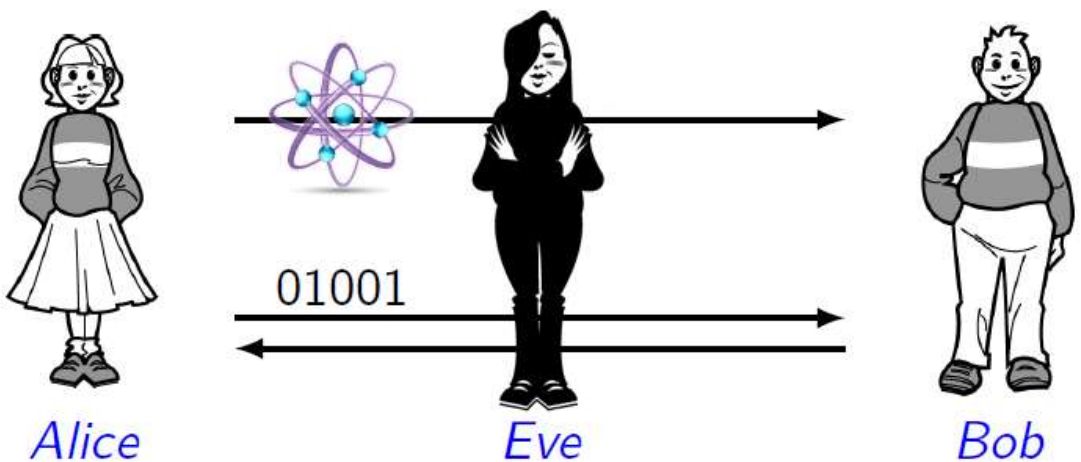
Quantum key distribution (QKD)

A quantum protocol for key distribution was invented by Bennett and Brassard in 1984 (it is known as BB84).

It provides means of establishing a private key—a random sequence of bits shared between *Alice* and *Bob* but unknown to any third party.

Later this key can be used in one-time pad to transmit a private message.

The protocol uses only public classical and quantum communication.



Key principle: Information gain implies disturbance!
(This is closely related to Heisenberg's uncertainty principle.)

Requirements for BB84

Public communication:

- *Alice* and *Bob* share a public authenticated classical channel.
- *Alice* can publicly send qubits to *Bob*.

Local operations:

- *Alice* has a private source of random classical bits.
- *Alice* can produce qubits in states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$.
- *Bob* can measure each of the incoming qubits in
  - either the standard basis $\{|0\rangle, |1\rangle\}$
  - or the Hadamard basis $\{|+\rangle, |-\rangle\}$.

Experimental implementations normally use polarised photons that are transmitted either through air or through optical fibre.

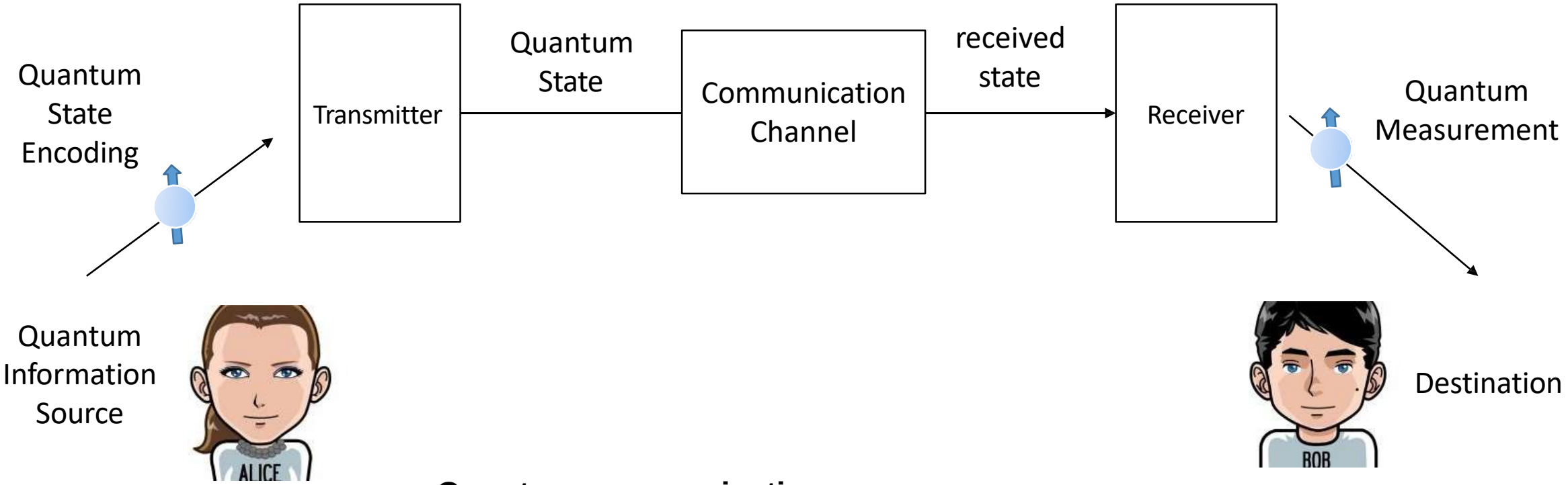
The BB84 rotocol

The basic BB84 protocol:

1. For $i = 1$ to n (below "$\in_R$" means "a random element of")
   - *Alice* picks $a_i \in_R \{0,1\}$ and $U_i \in_R \{I, H\}$ and sends $U_i|a_i\rangle$ to *Bob*.
   - *Bob* guesses $V_i \in_R \{I, H\}$ and applies it on the received state.
   - *Bob* measures the resulting state $V_iU_i|a_i\rangle$ in the standard basis. We denote his measurement outcome by $b_i \in \{0,1\}$.
2. *Bob* announces (over the public classical channel) which basis he used for each measurement (i.e., the string $V_1, \ldots, V_n$).
3. *Alice* announces $S \subseteq \{1, \ldots, n\}$ indicating which measurements where made in the correct basis.
4. Note that $a_i = b_i$ for all $i \in S$, so the shared key is $(a_i : i \in S)$.

	i	1	2	3	4	5	6	
Alice	$\|a_i\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	
	U_i	I	H	I	I	H	H	
	$U_i\|a_i\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	← public
Bob	V_i	H	H	I	H	I	H	← public
	$V_iU_i\|a_i\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	
	$\|b_i\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	
Alice	S		✓	✓			✓	← public
Key			0	1			1	

Quantum Communication

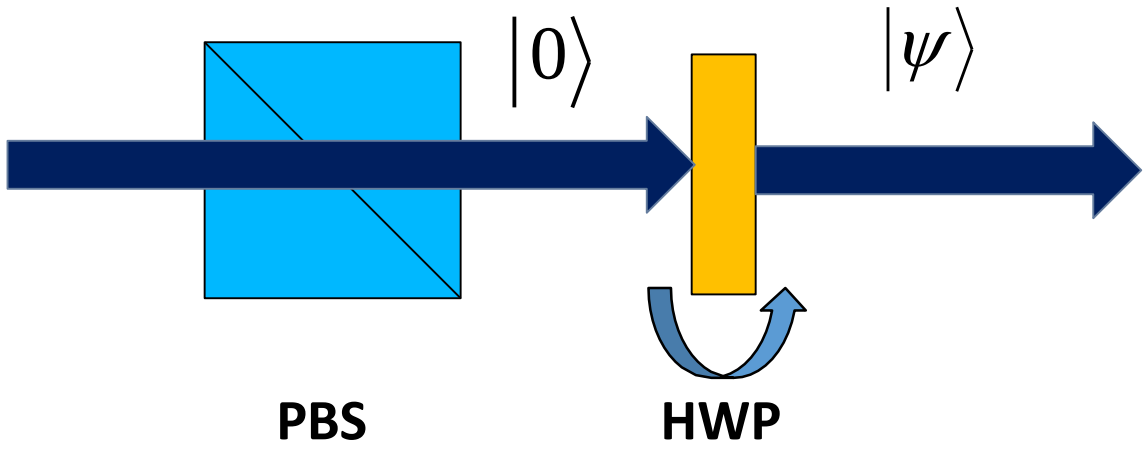


Quantum communication:
signal is encoded in a quantum system

→ new applications and communication protocols
→ modified **Sources, Transmitters, Receivers**
→ How these may be realized will be discussed over the course

Encoding information in polarization of single photons

encoding a qubit in polarization via half-wave plate (HWP) with rotatable optical axis:



HWP angle:	qubit:
HWP @ 0º	$\|H\rangle$
HWP @ 45º	$\|V\rangle$
HWP @ 22.5º	$\|D\rangle$
HWP @ -22.5º	$\|A\rangle$

Detection of polarization-encoded qubits

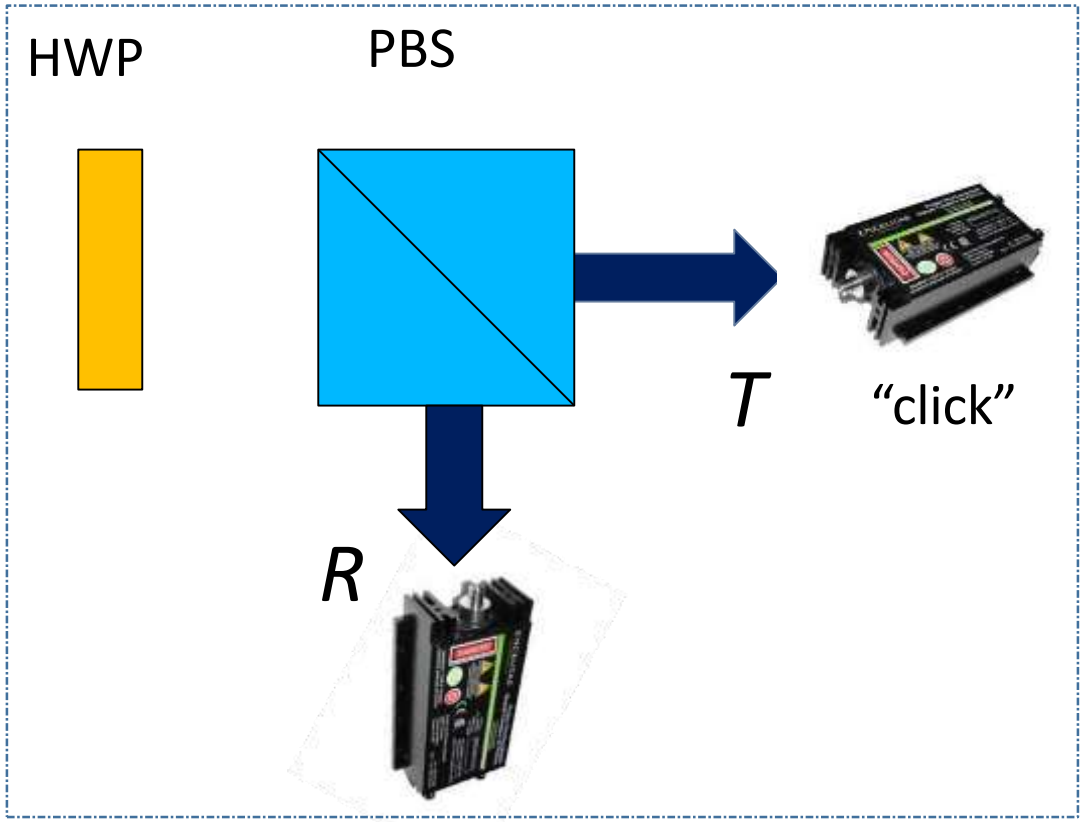
Polarization analyzer (Bob-module):

$|H\rangle$

$|V\rangle$

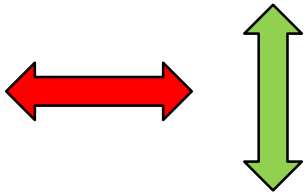
$|D\rangle$

$|A\rangle$



HWP @ 0º :

H or V ?



Detection of polarization-encoded qubits

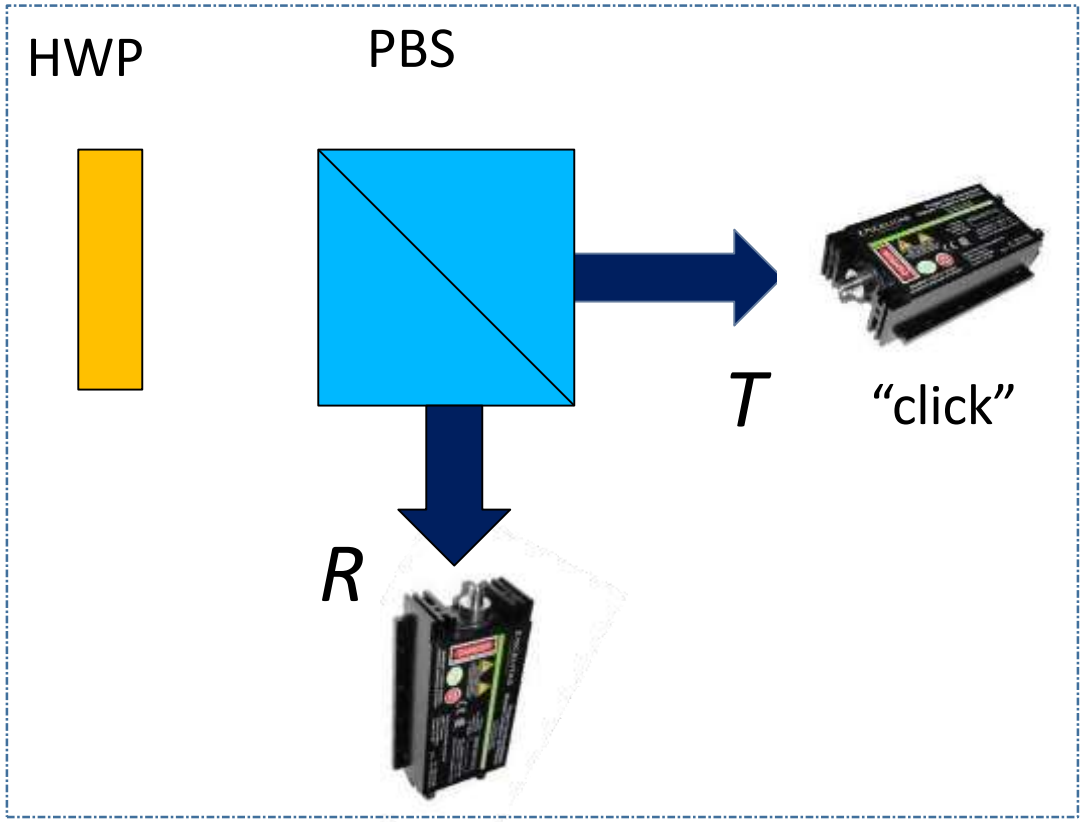
Polarization analyzer (Bob-module):

$|H\rangle$

$|V\rangle$

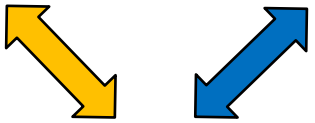
$|D\rangle$

$|A\rangle$



HWP @ 22.5º :

D or A ?

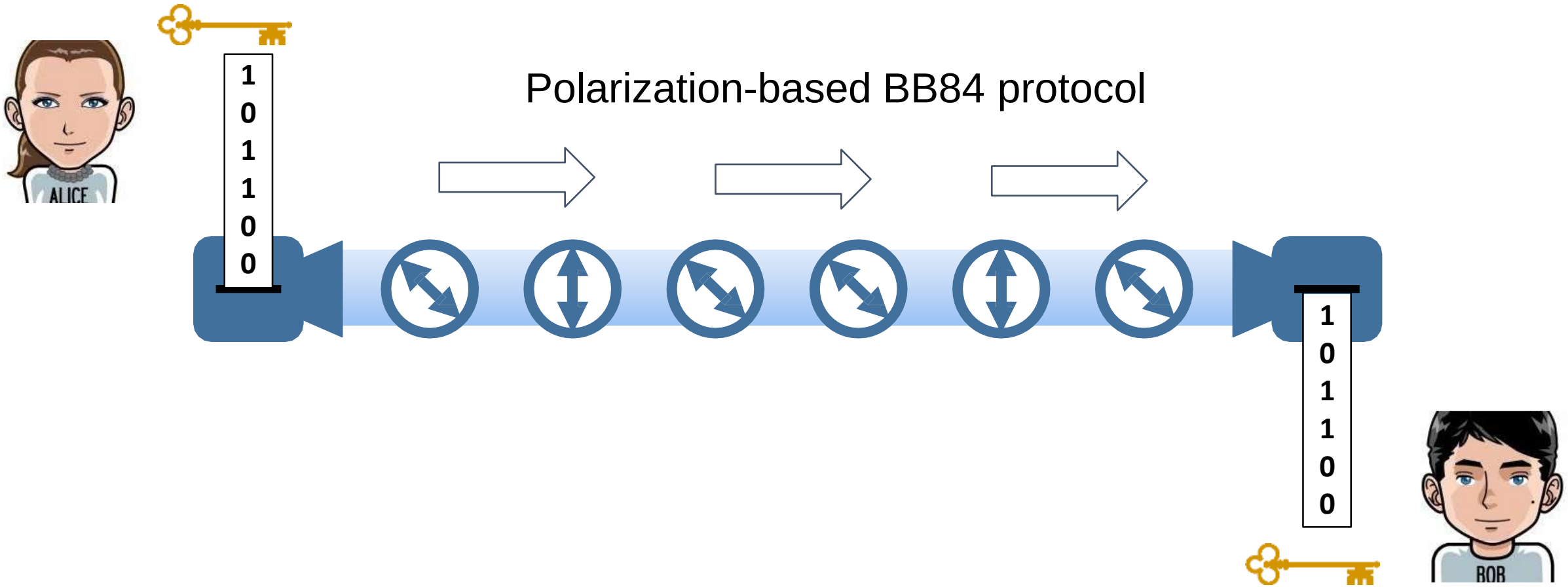


→ impossible to distinguish H/V and D/A using the same measurement setting

→ Certain properties **cannot be known** simultaneously

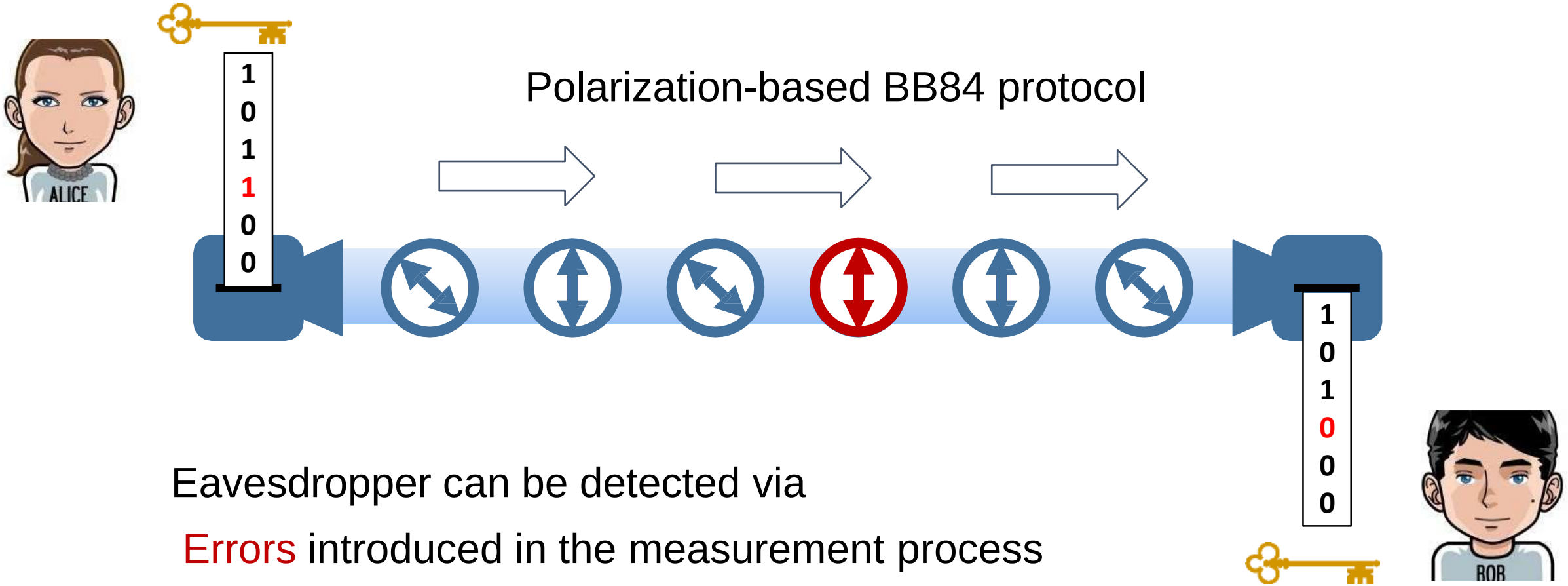
Quantum Key Distribution

Alice and Bob can have an unbreakable code if they
share newly created identical strings of random bits (one time pad)



Quantum Key Distribution

Alice and Bob can have an unbreakable code if they
share newly created identical strings of random bits (one time pad)



Eavesdropper can be detected via

Errors introduced in the measurement process

Entanglement: Multi-partite superposition states

The whole is more than
the sum of its parts (it's the tensor product) : $\mathcal{H}_1^2 \otimes \mathcal{H}_2^2$

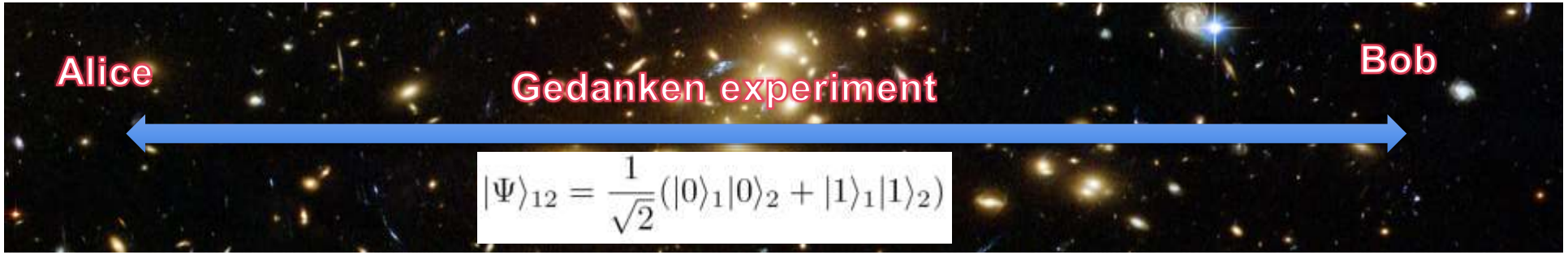
General bi-partite states

$$|\psi\rangle_{12} = \alpha|0\rangle_1|0\rangle_2 + \beta|0\rangle_1|1\rangle_2 + \gamma|1\rangle_1|0\rangle_2 + \delta|1\rangle_1|1\rangle_2$$

Only when $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$ $\longrightarrow$ $|\psi\rangle_{12} = |\eta\rangle_1 \otimes |\chi\rangle_2$

Bell- state in not a product (correlation)

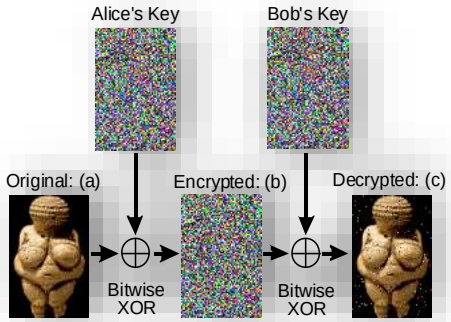
$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|1\rangle_1|0\rangle_2 - |0\rangle_1|1\rangle_2) \neq |\psi\rangle_1 \otimes |\phi\rangle_2$$



fundamental physics….

E. Schrödinger
Naturwissenschaften 23, 807 (1935)

and an application!



Why is quantum entanglement intresting?

- Information is carried by correlations only.
- In contradiction with classical physics, locality and realism.
- True for any distance.

Why quanutm cryptography?

- Classical cryptography is in principle insecure

Quantum key distribution (QKD) can guarantee security

Bell States

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

Maximally Entangled

All information shifted to correlations

Quizzing Entangled Photons

1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?

?

$|\phi\rangle_{AB}$

?

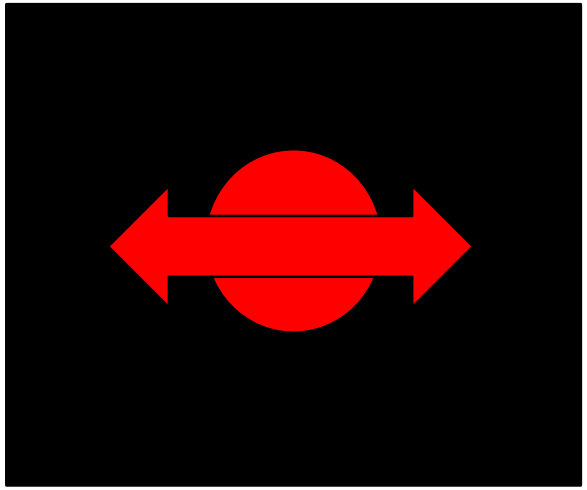
Quizzing Entangled Photons

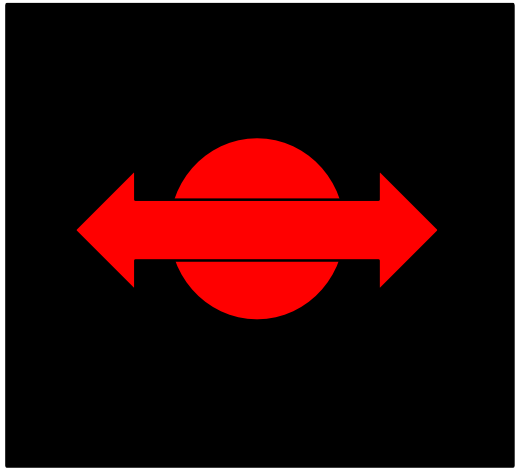
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





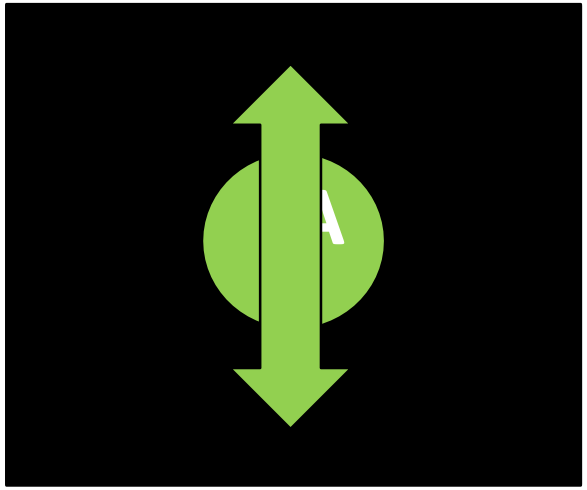
Quizzing Entangled Photons

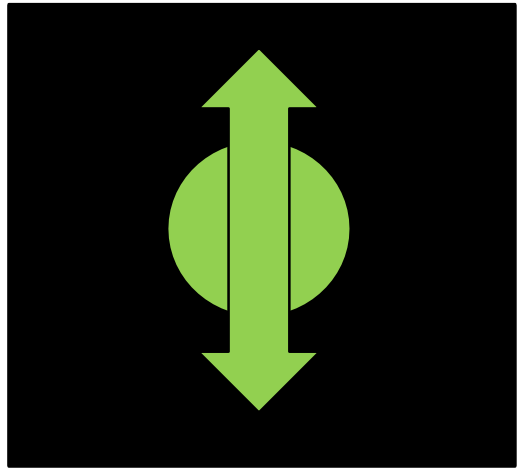
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





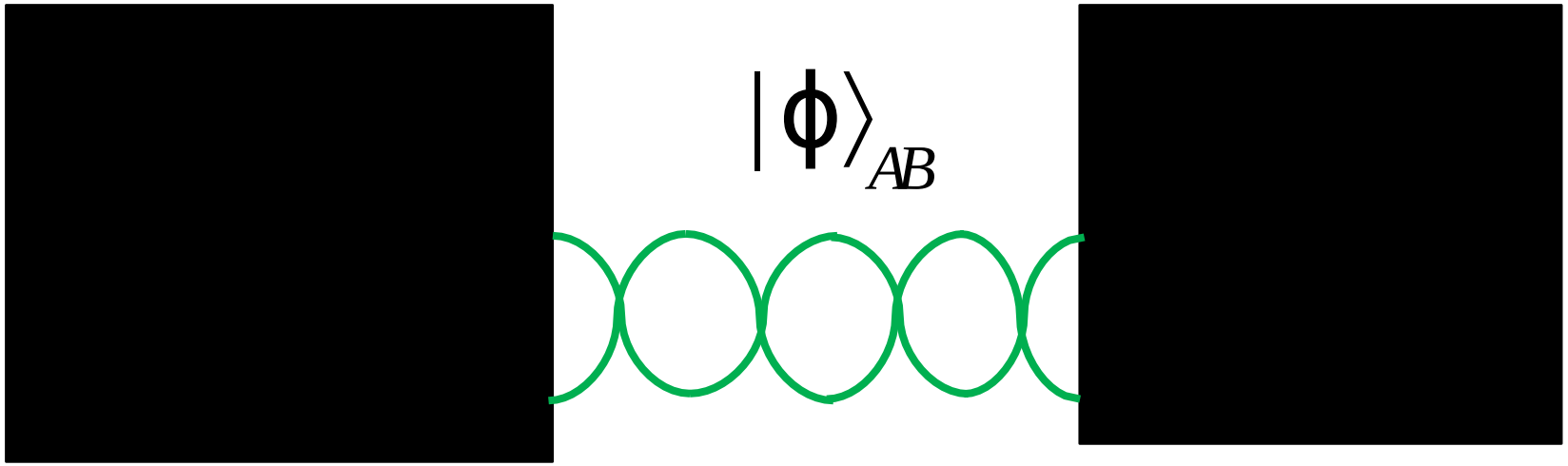
Quizzing Entangled Photons

1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?



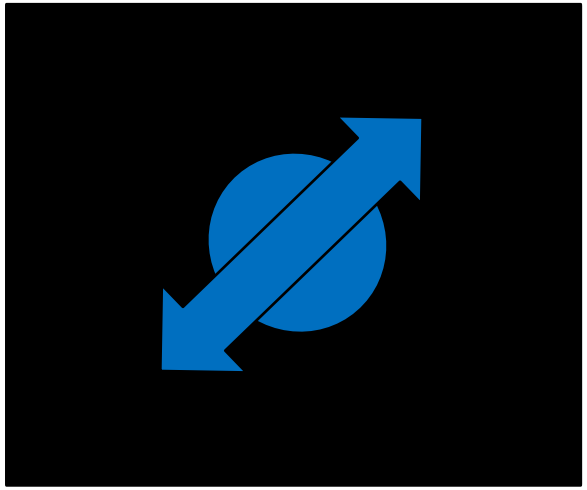
Quizzing Entangled Photons

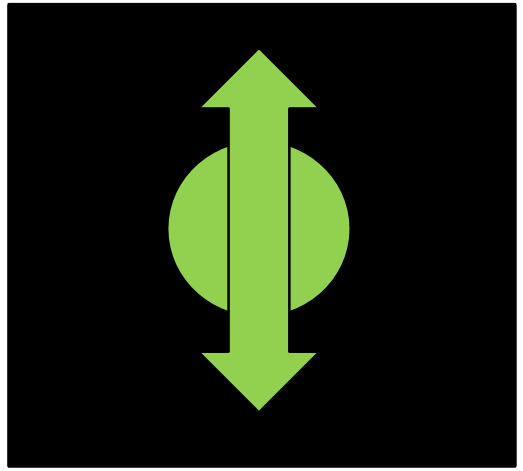
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





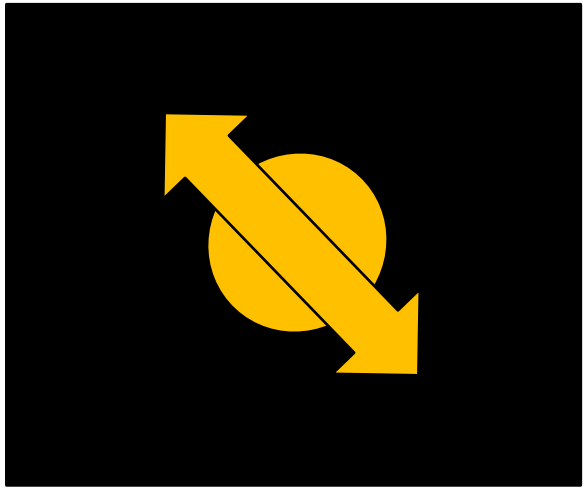
Quizzing Entangled Photons

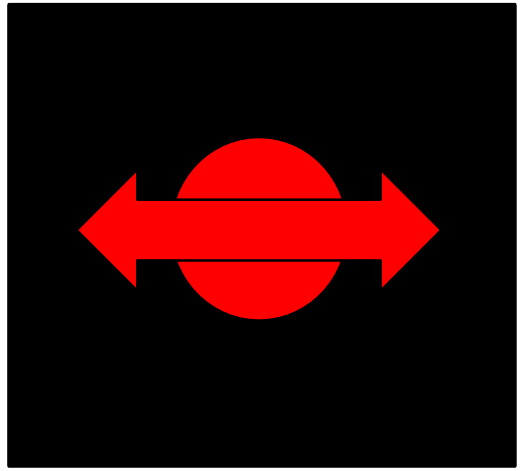
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





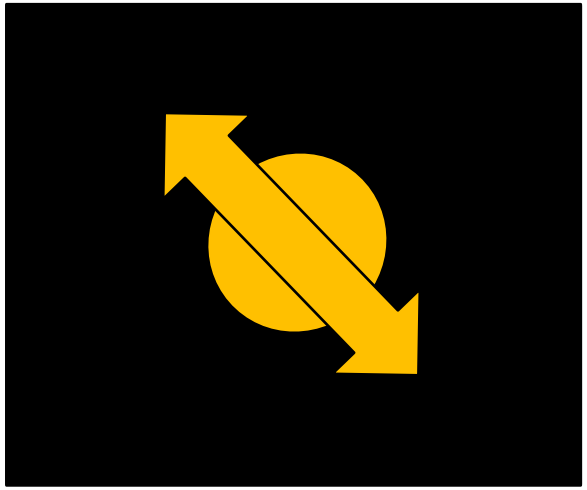
Quizzing Entangled Photons

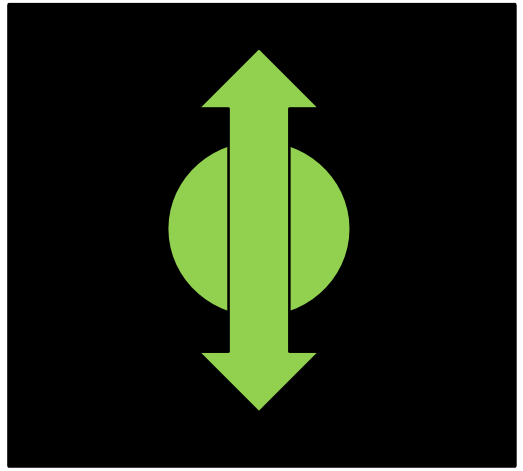
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





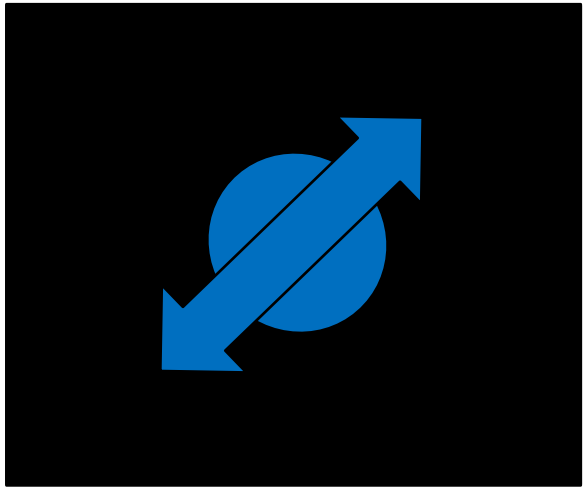
Quizzing Entangled Photons

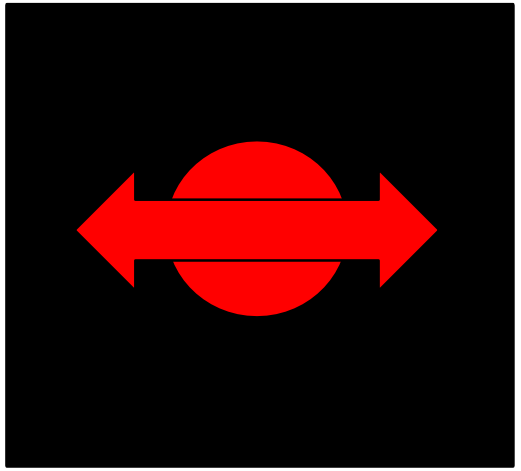
1 or 0 ?

+ or - ?

1 or 0 ?

+ or - ?





Extra post-processing

Ideal outcome: The strings of *Alice* and *Bob* are uniformly random, identical, and private from *Eve*.

More realistic: The strings might not agree either because of noise or because of *Eve*.

Extra steps:

- Information reconciliation: a form of error correction that ensures the keys shared by *Alice* and *Bob* are identical.
- Privacy Amplification: eliminates any partial information *Eve* might have about the key shared by *Alice* and *Bob*.

Sanity checks

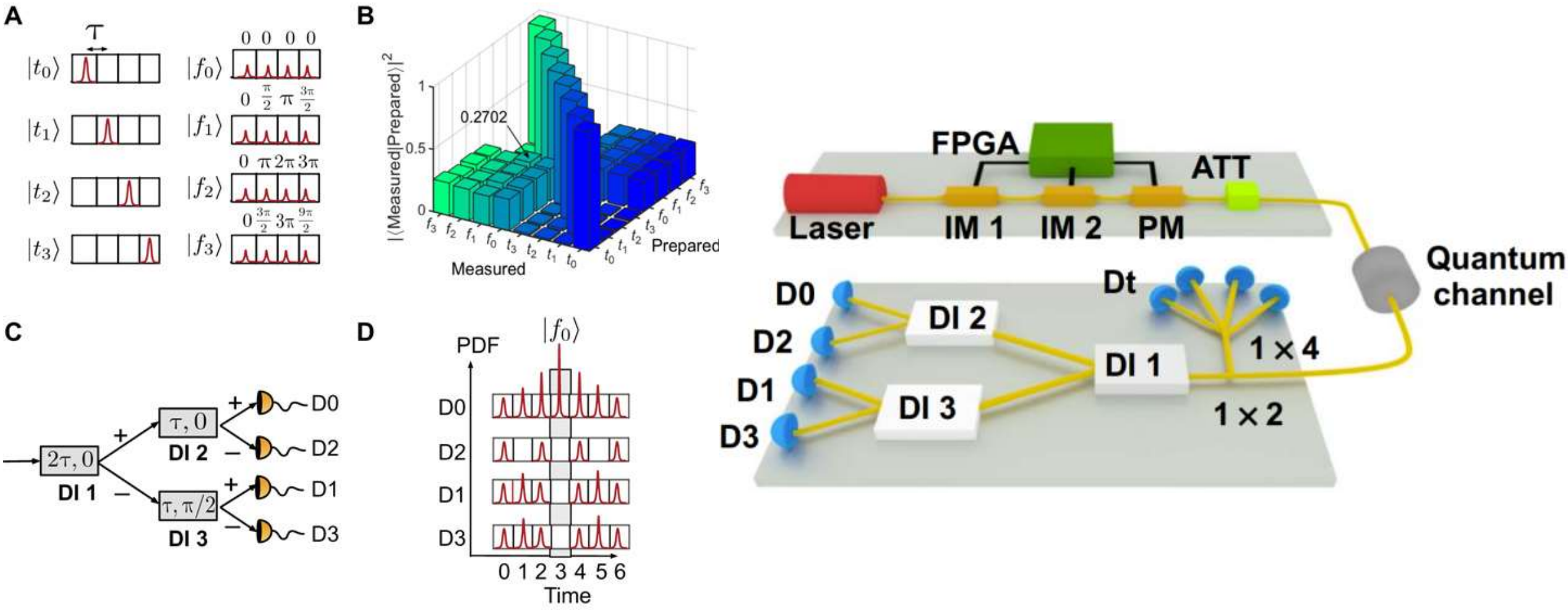
Why not announce the bases for all qubits before transmission, thus avoiding the loss of half the bits?

- This allows *Eve* to intercept, measure, and re-transmit the post-measurement state.

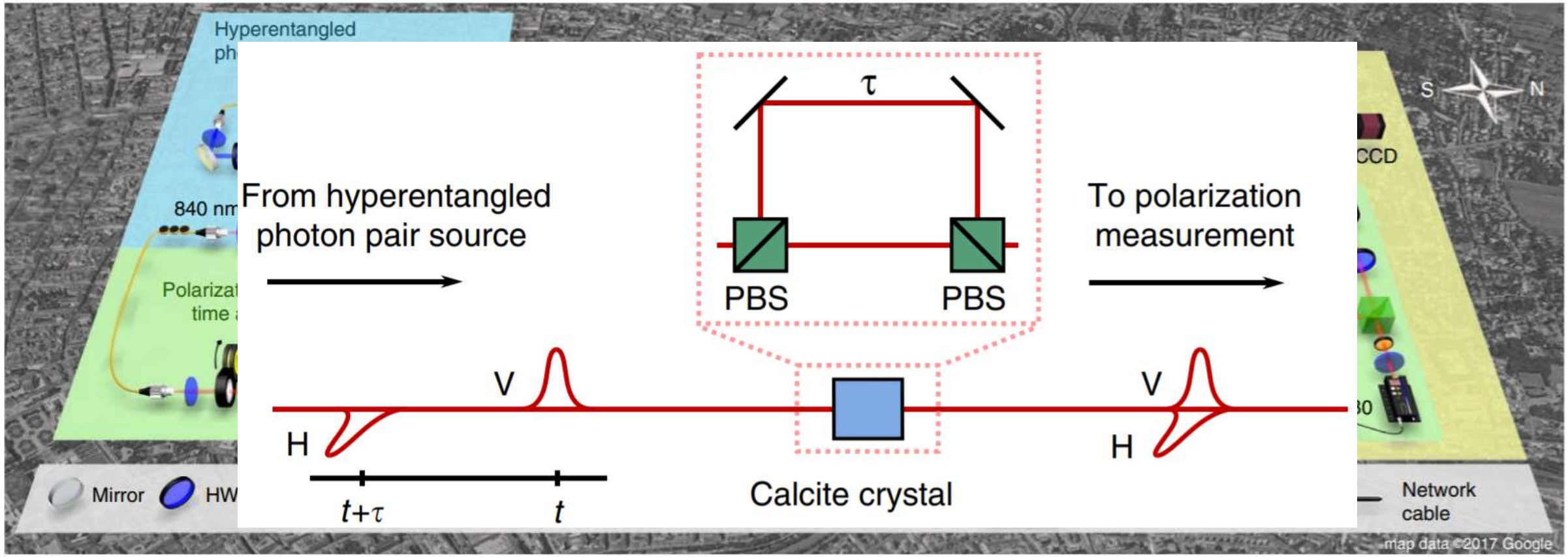
Why not announce the basis for each qubit after they are sent but before *Bob* measures them?

- Requires *Bob* to store the qubits (technologically difficult).
- If *Bob* can store them, so can *Eve*. She can perform the correct measurements and retransmit the post-measurement states to *Bob*.

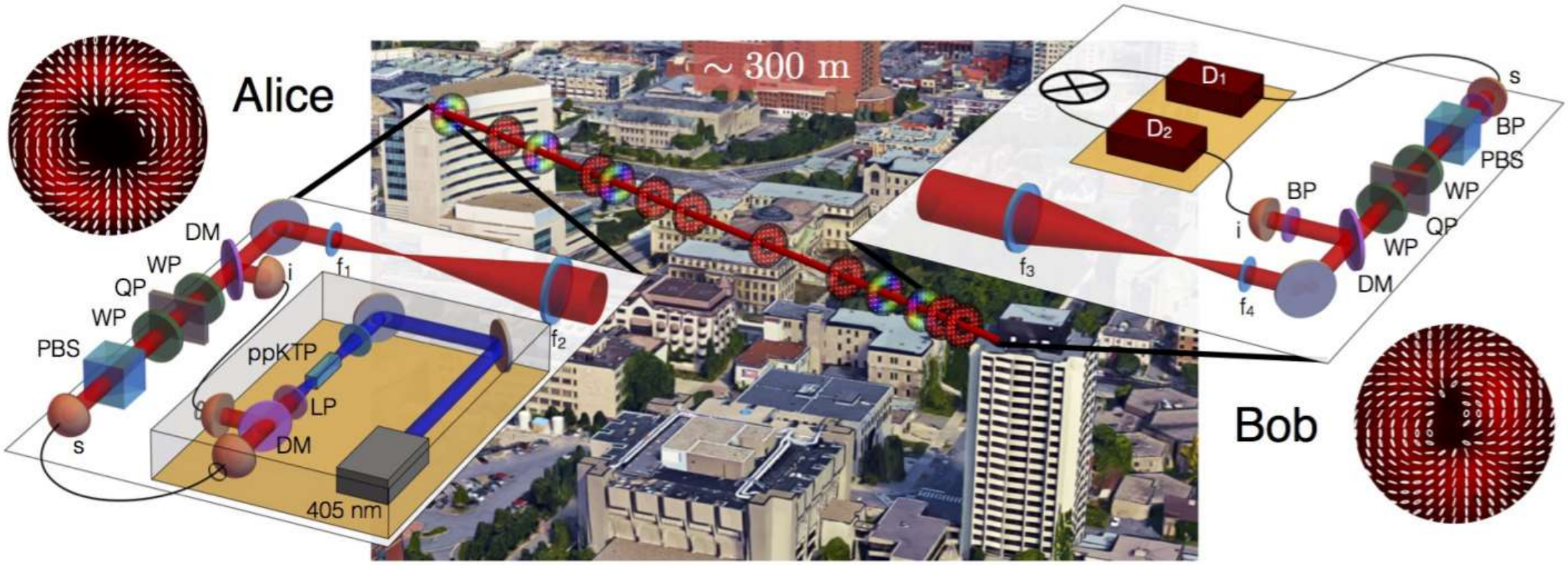
Quantum key distribution with time-bin qudits



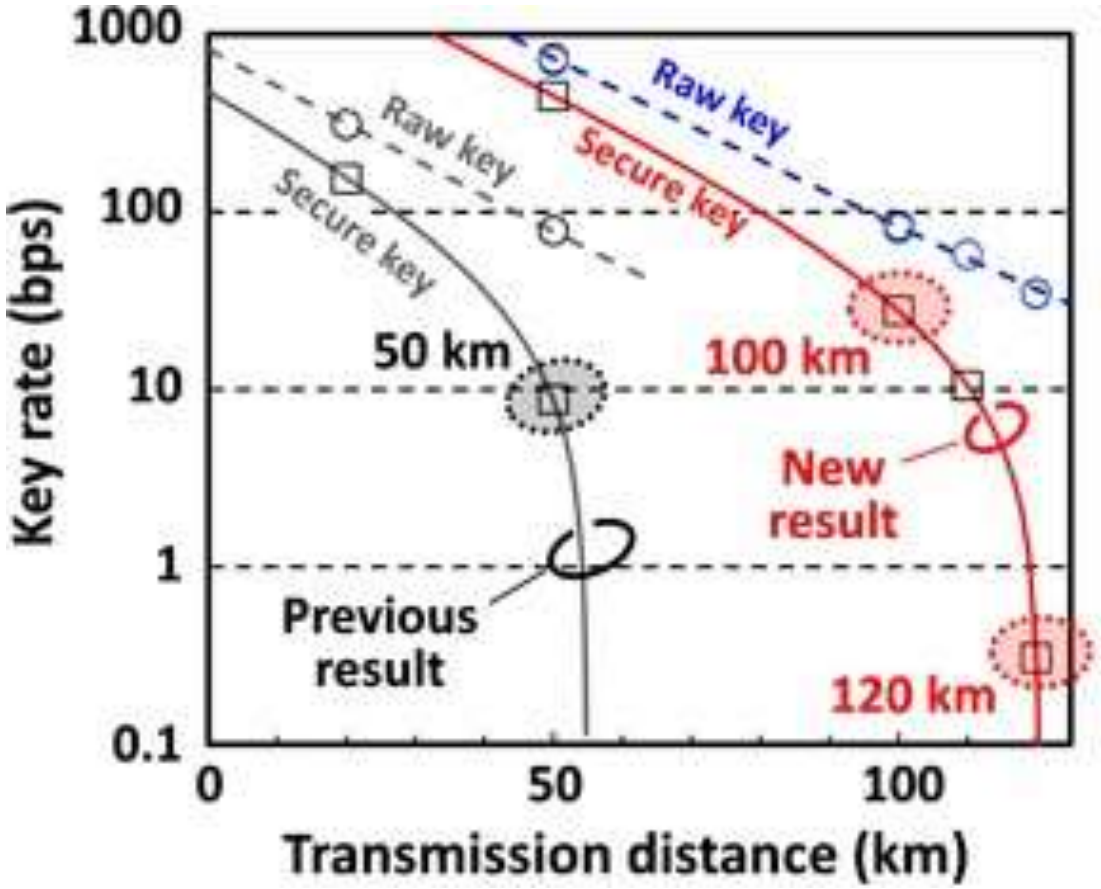
Distribution of high-dimensional entanglement via an intra-city free-space link



High-Dimensional Intra-City Quantum Cryptography with Structured Photons



Distance limitation for direct transmission in Fiber

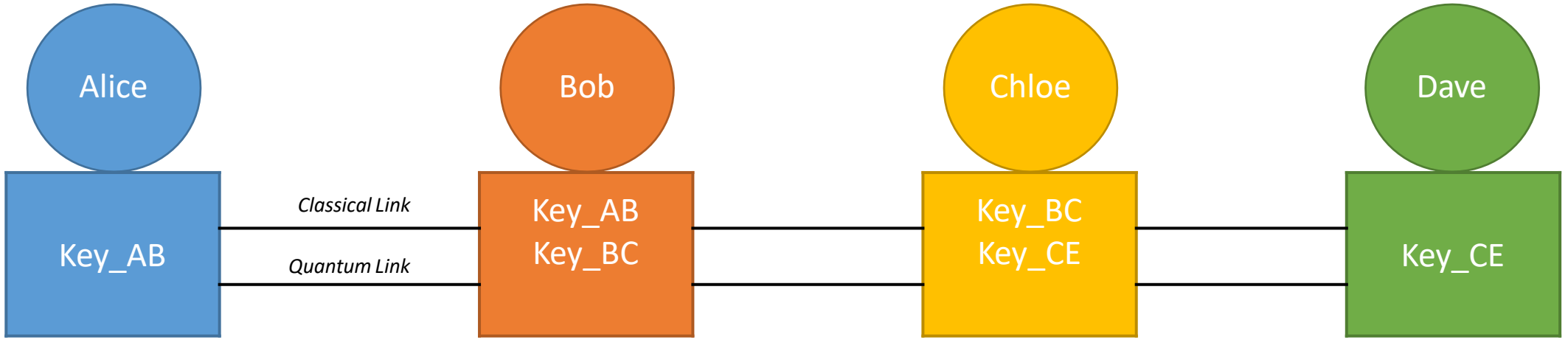


Fiber loss η

→ not practical, even without noise photons

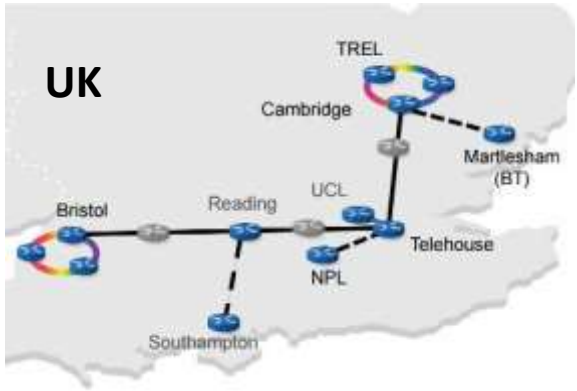
Trusted node network

1. Each pair of nodes establishes a pair of identical keys via BB84
2. Bob announced parity of Keys_AB & Key_BC → Alice now knows Key_BC
3. Chloe announces parity of Keys_BC & Key_CE → Alice now knows Key_CE



- the useful link is too long for direct transmission of single photons
- Alice has to trust Bob and Chloe when she communicates with Dave
- Single point of failure (in this simple implementation): if Eve breaks into a single node, the whole chain is compromised

Fiber Network Implementations



EU QKD Testbed 2019

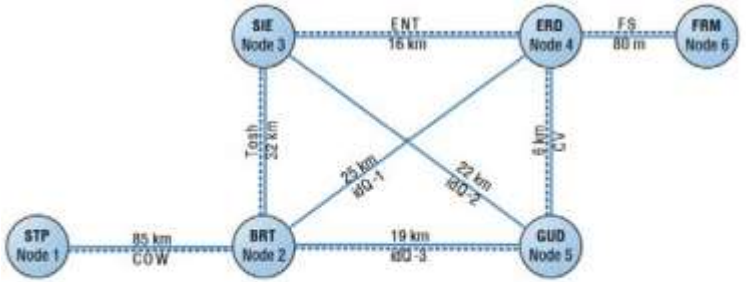
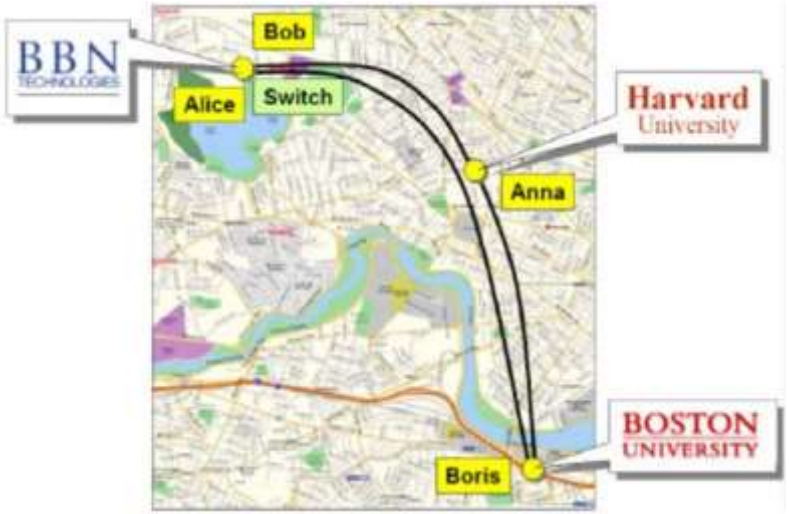
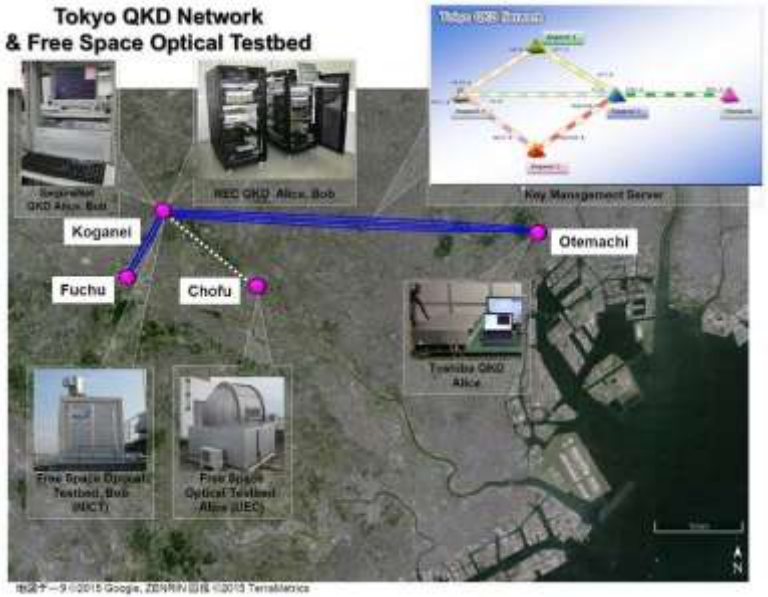


Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

Figure 3. Satellite map with the locations of the nodes of the prototype.



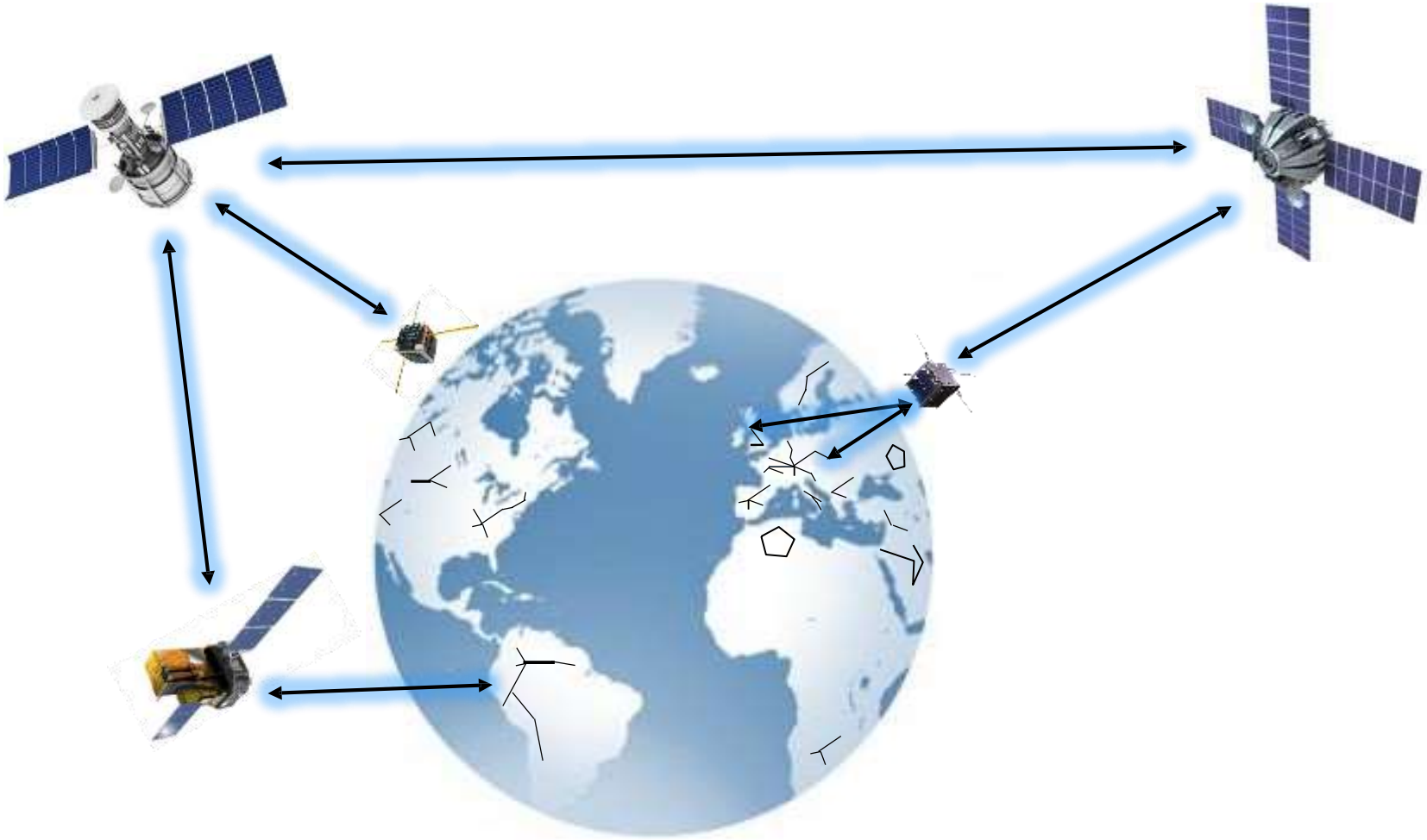
USA



Japan

Austria

A global “Quantum Internet”



Long-distance satellite links + local fiber networks + quantum repeaters

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2*] Jian-Yu Wang,[2,3*] Jian-Wei Pan[1,2*]