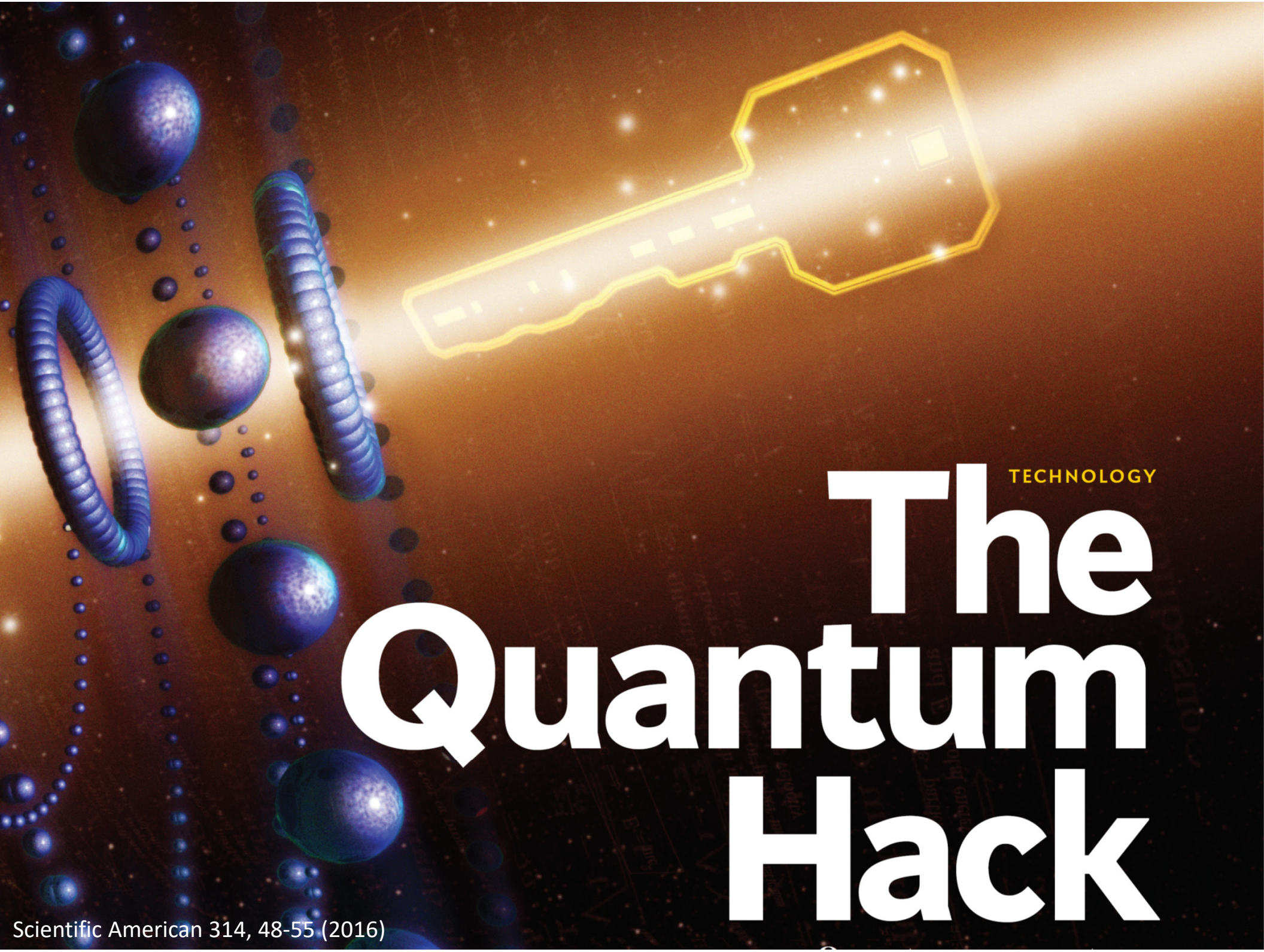
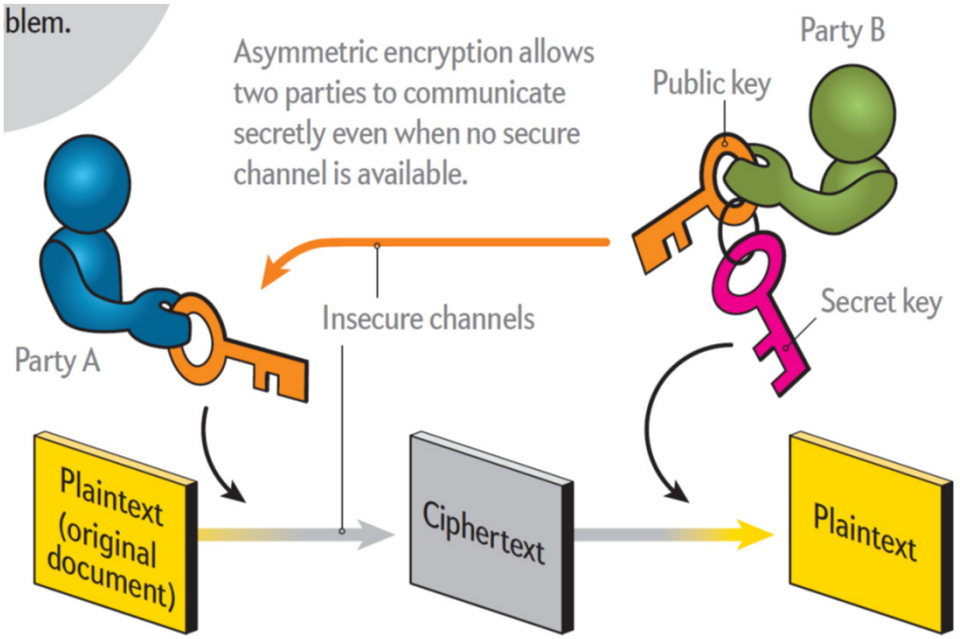



Scientific American 314, 48-55 (2016)

# A central problem in cryptography: the key distribution problem.

Mathematics solution:
**public key cryptography.**

Public-key cryptography relies on the computational difficulty of certain hard mathematical problems (for example factoring)




Security problems with public key cryptography:

(1) **The is no proof** that there is no "easy" solution to factoring: somebody can come up with new much quicker algorithm!

(2) **Quantum computer, if build, can break public key encryption** – fast quantum algorithm is already knows (Shor's algorithm)

# Another solution to the key distribution problem: Quantum key distribution

**Use quantum communication channel:**

**physical system capable delivering quantum systems more or less intact from one place to another.**

**What is this quantum system? Photons!**

**Why is this secure:**

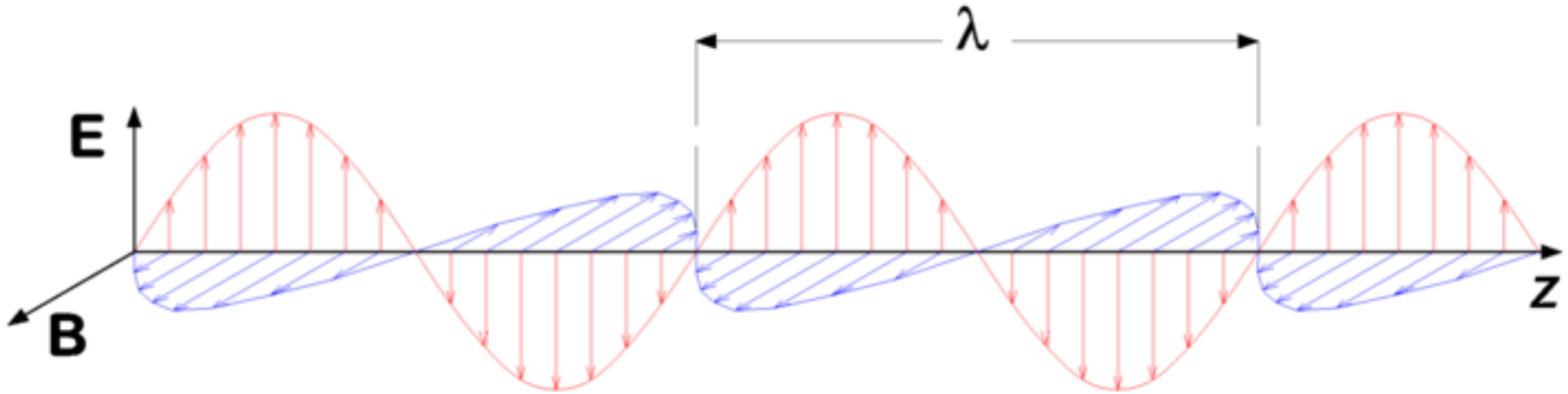
Quantum mechanics: quantum bits cannot be copied or monitored.

Any attempt to do so will result in altering it that can not be corrected.

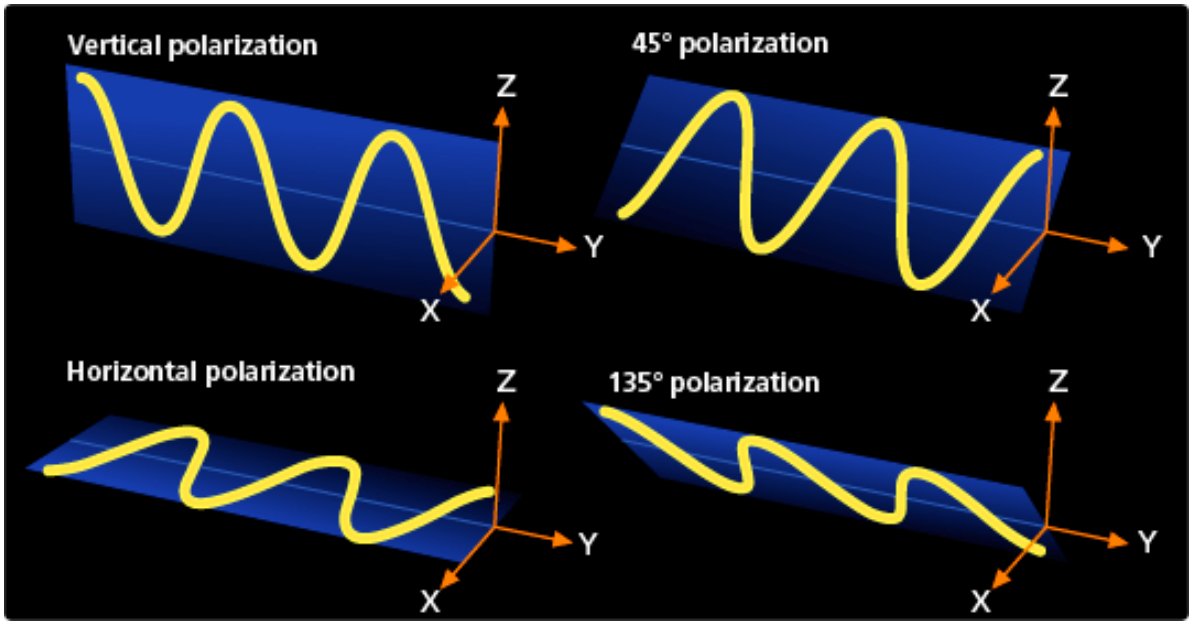
How to use photons as qubits?

Use polarization of photons to encode 0 and 1.

# Electromagnetic waves



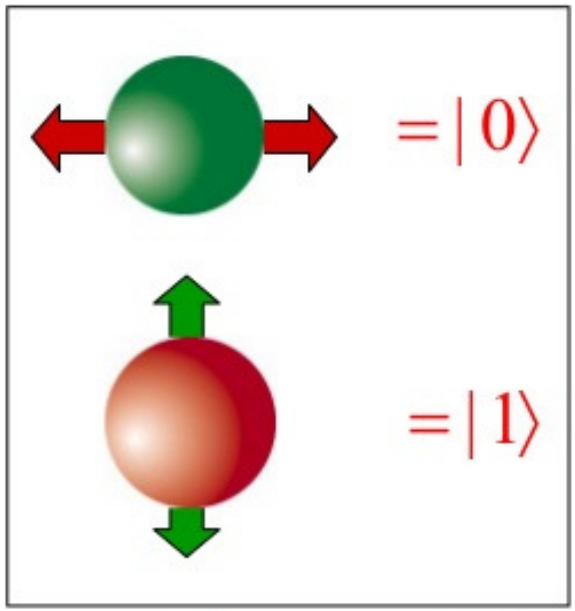

A "vertically polarized" electromagnetic wave of wavelength λ has its electric field vector **E** (red) oscillating in the vertical direction. The magnetic field **B** (or **H**) is always at right angles to it (blue), and both are perpendicular to the direction of propagation (**z**).

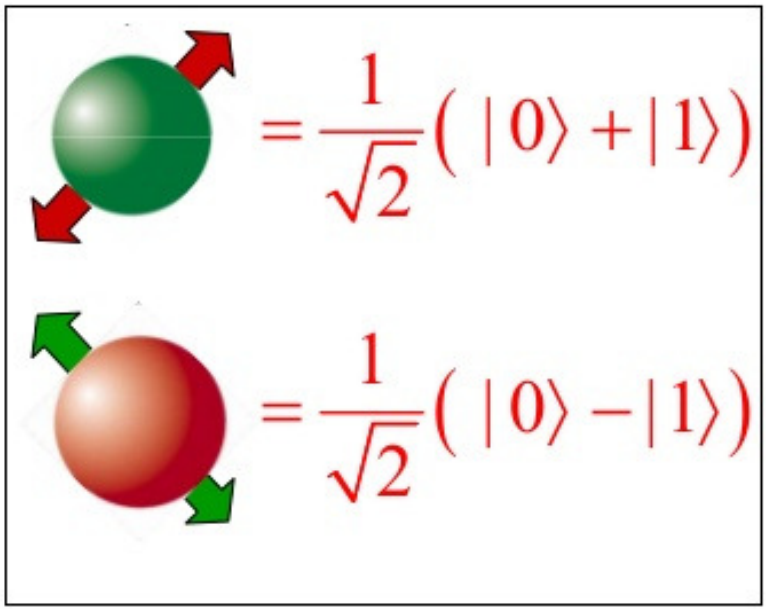



http://www.nikon.com/about/feelnikon/light/chap04/sec01.htm

https://en.wikipedia.org/wiki/Polarization_(waves)

# Photon polarization as a qubit

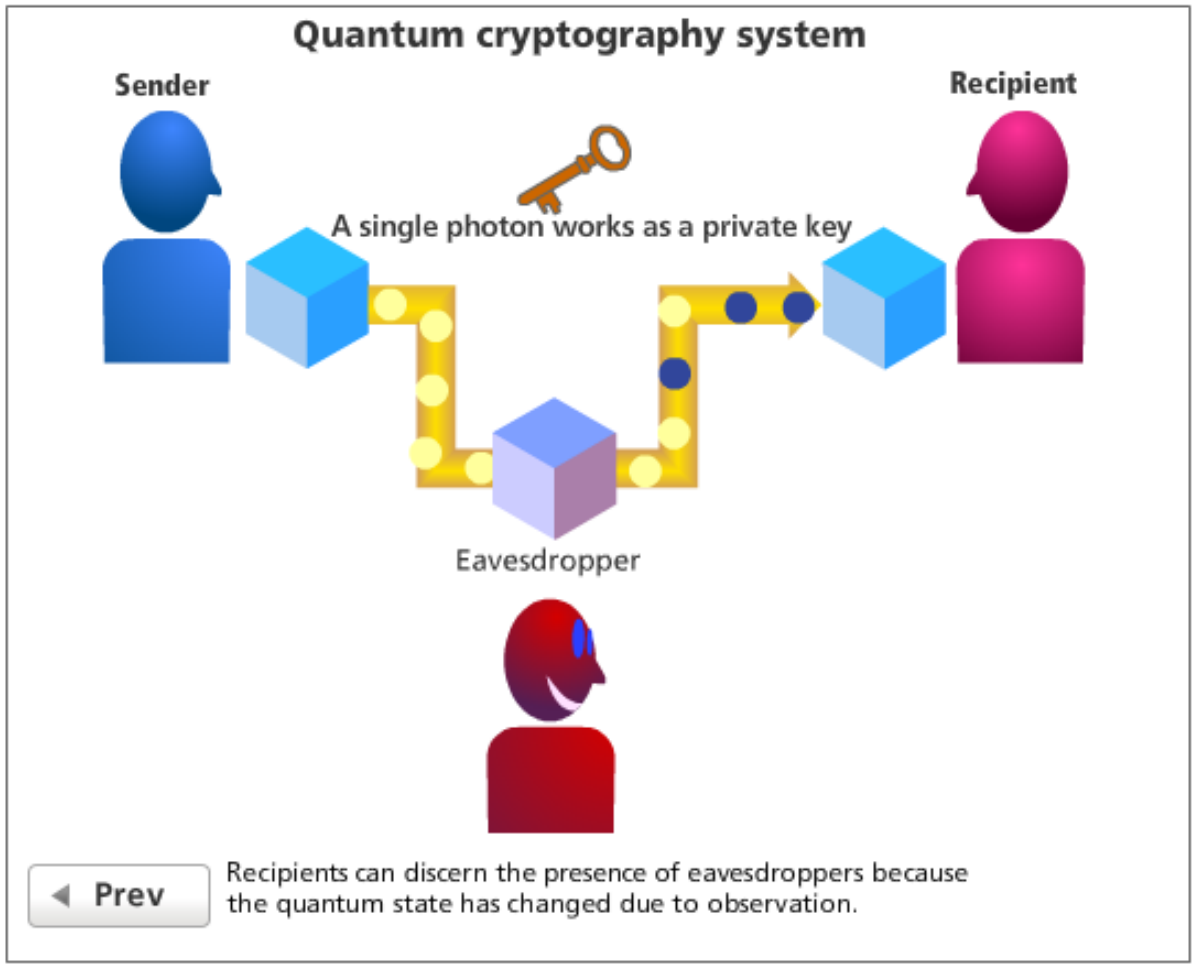




# Quantum key distribution

http://www.nikon.com/about/feelnikon/light/chap04/sec01.htm

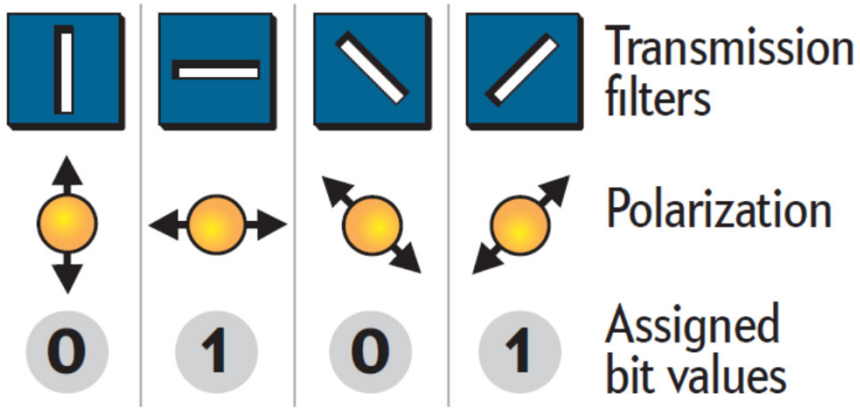


# The Quantum Future of Cryptography

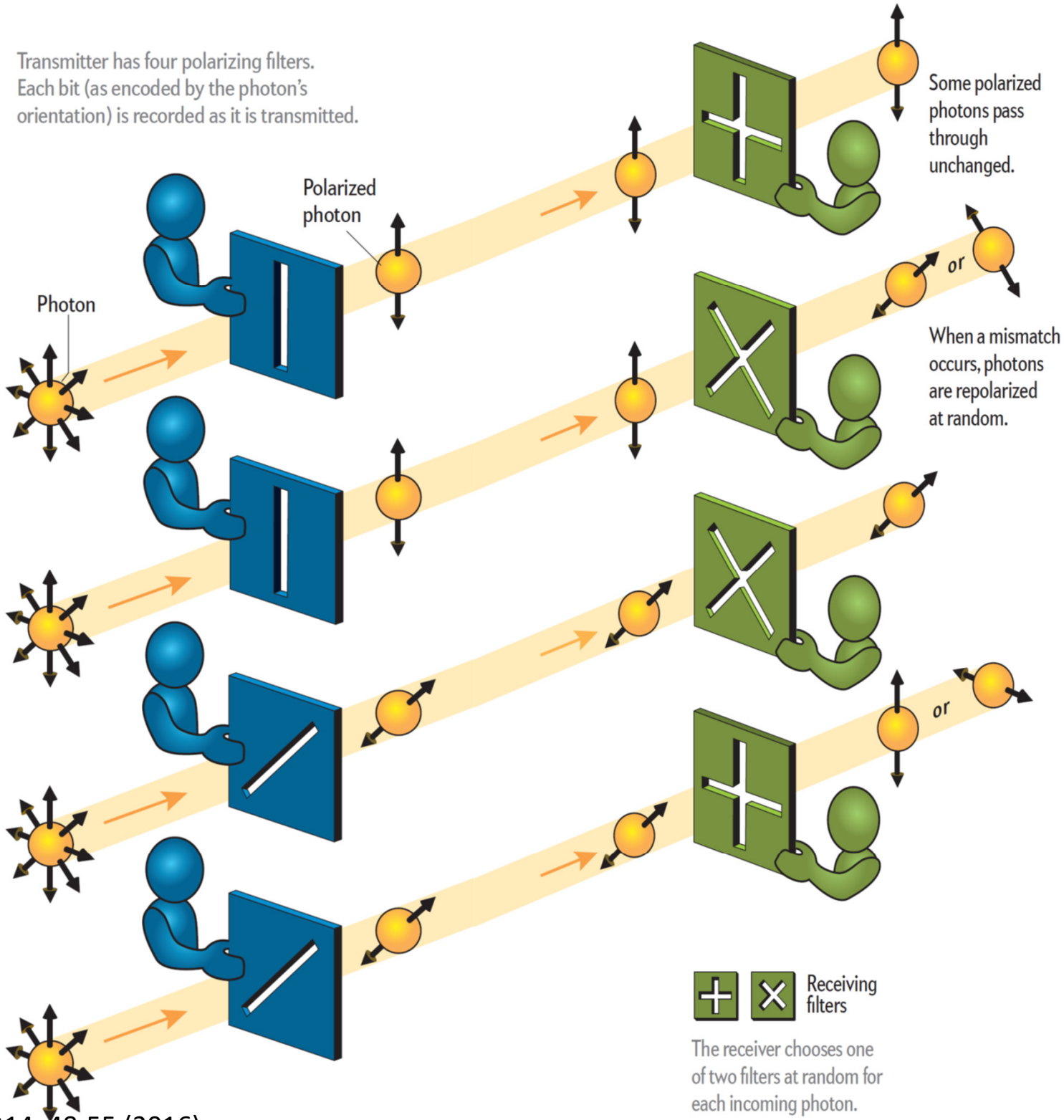
**Quantum-key distribution** is a way of securely sharing a cryptographic key using a stream of light particles, or photons, that are polarized. If an eavesdropper measures those photons while they are in transit, the act of measurement will change the polarization of some of those photons, and the sender and recipient will know that their message has been tampered with.

## Sending and Receiving Polarized Photons

The sender (*blue*) transmits a series of photons; each passes through one of four polarizing filters. Each filter—and therefore polarization direction—is assigned a bit value of 0 or 1 (*below*). The sender writes down the bit value of each photon. The recipient (*green*) can only determine the bit value of each photon after it has passed through a receiving filter.

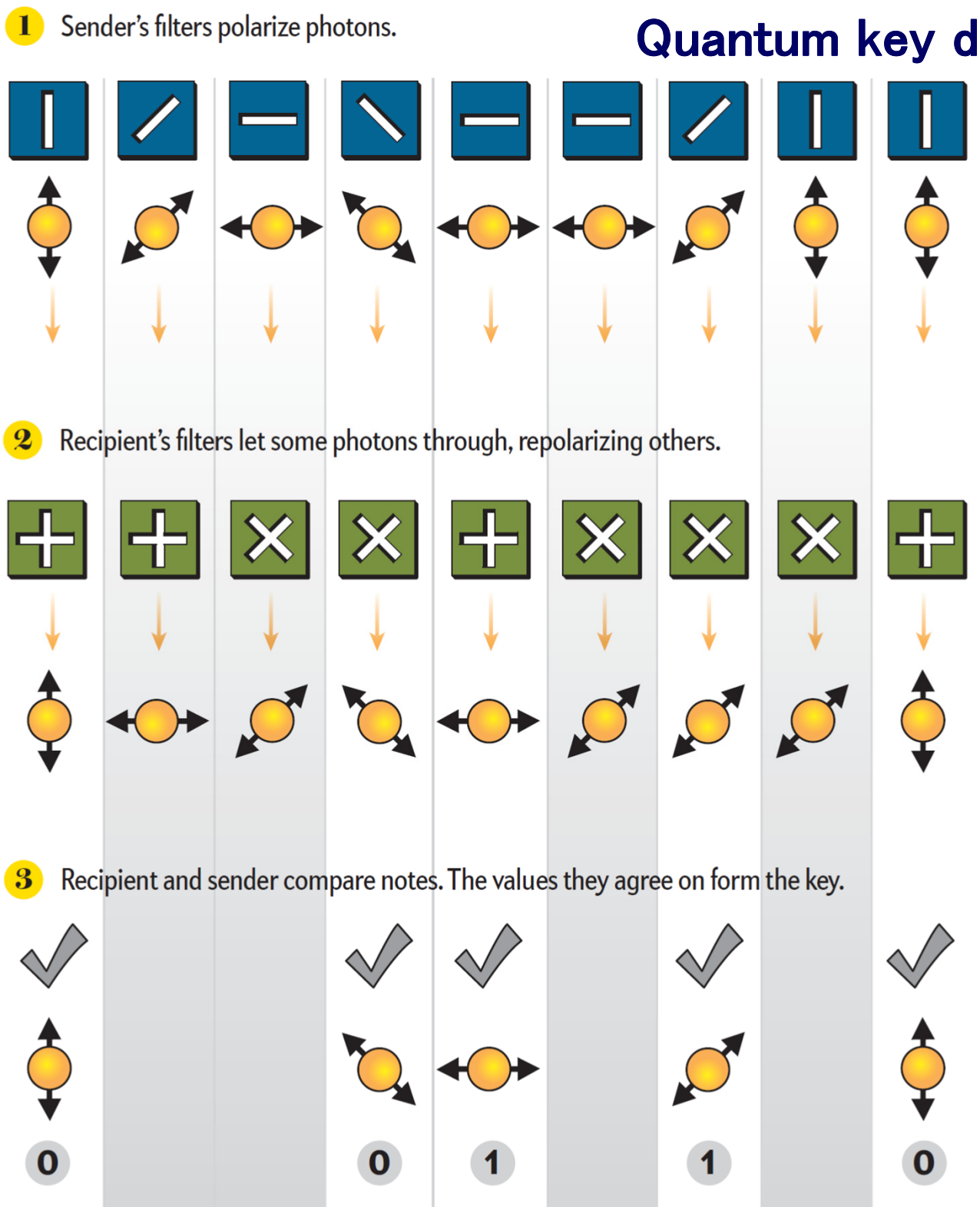



Scientific American 314, 48-55 (2016)




Scientific American 314, 48-55 (2016)

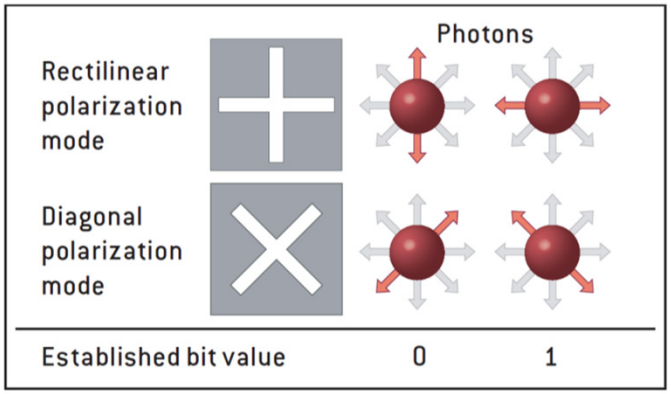
# Quantum key distribution




Scientific American 314, 48-55 (2016)

Alice and Bob try to keep a quantum-cryptographic key secret by transmitting it in the form of polarized photons, a scheme invented by Charles Bennett of IBM and Gilles Brassard of the University of Montreal during the 1980s and now implemented in a number of commercial products.

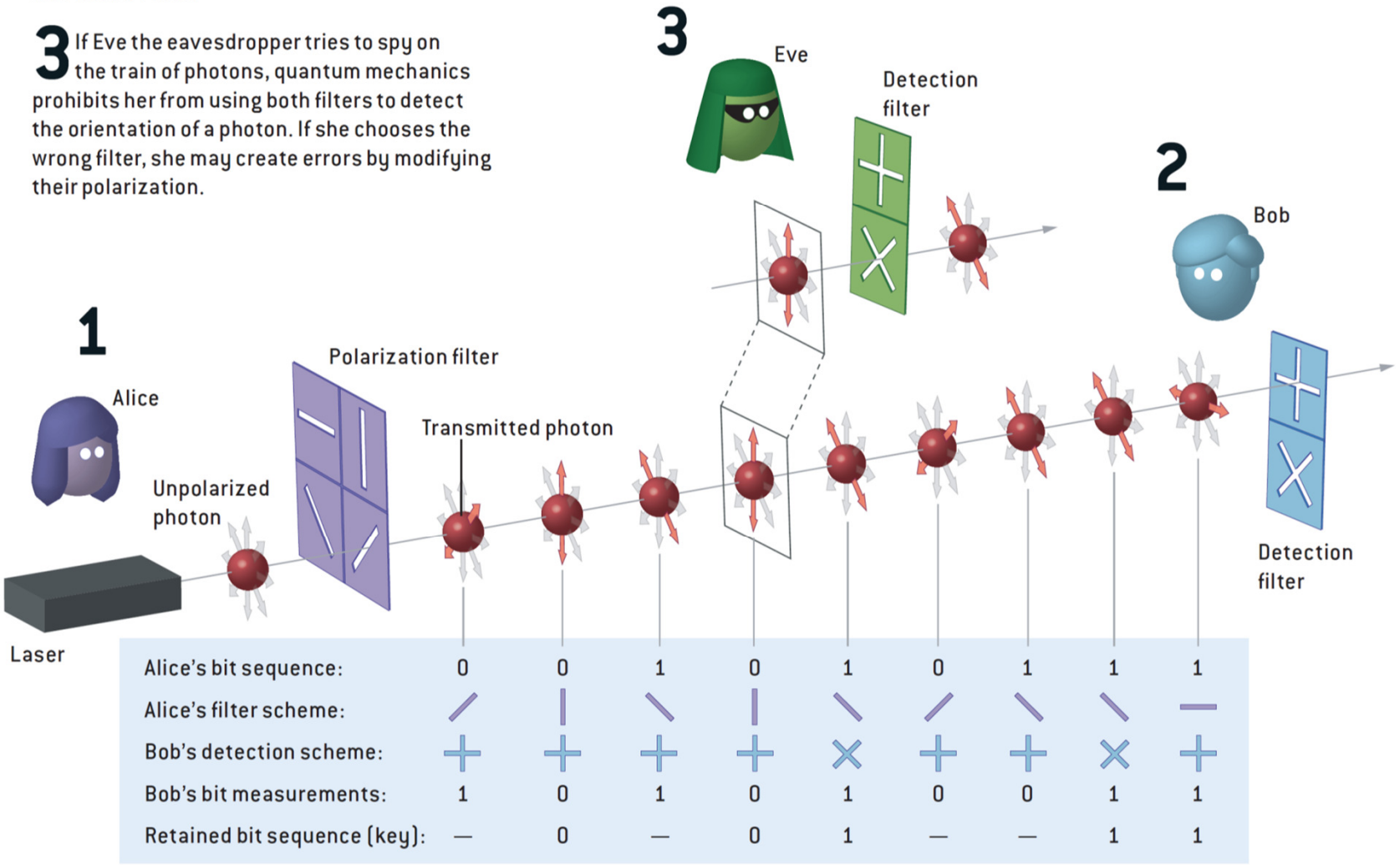
Scientific American 292, 78 (2005)

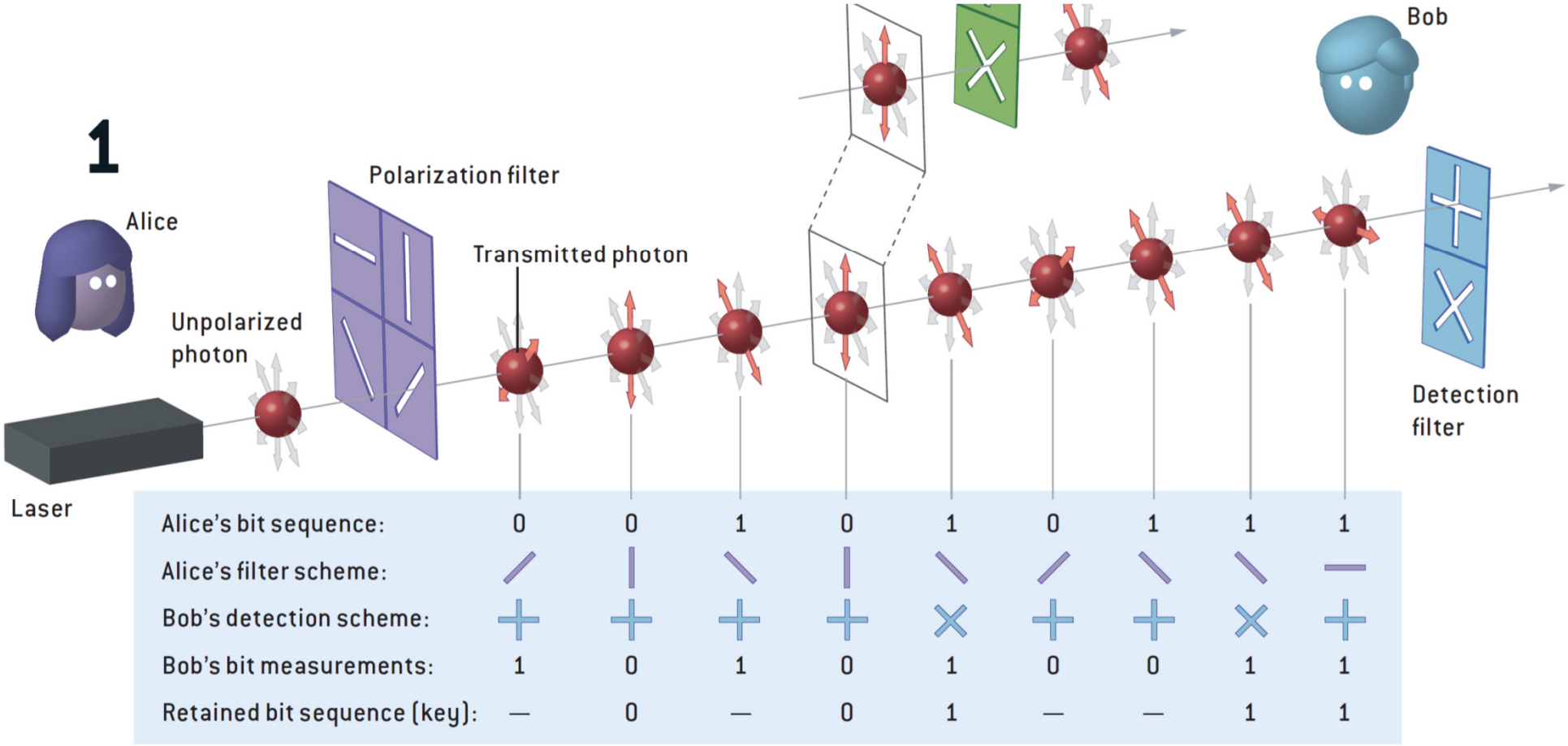



**1** To begin creating a key, Alice sends a photon through either the 0 or 1 slot of the rectilinear or diagonal polarizing filters, while making a record of the various orientations.

**2** For each incoming bit, Bob chooses randomly which filter slot he uses for detection and writes down both the polarization and the bit value.

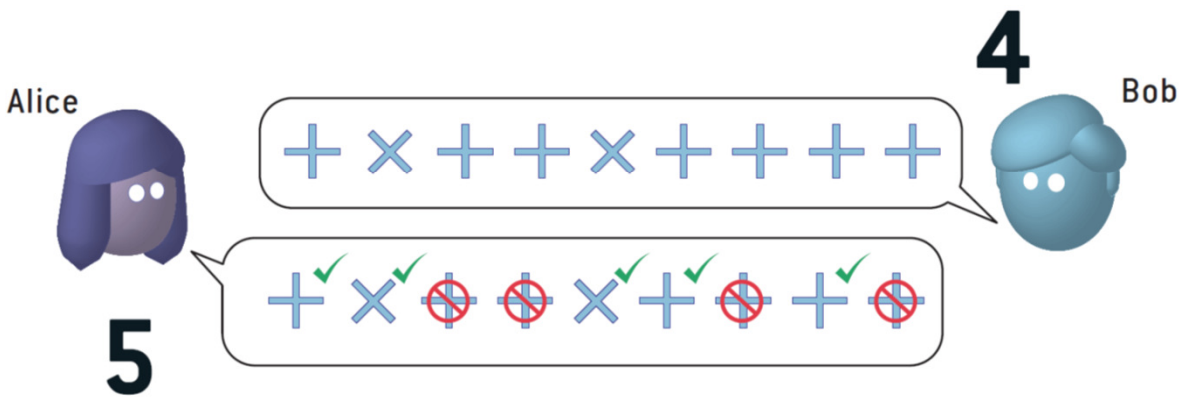
**3** If Eve the eavesdropper tries to spy on the train of photons, quantum mechanics prohibits her from using both filters to detect the orientation of a photon. If she chooses the wrong filter, she may create errors by modifying their polarization.





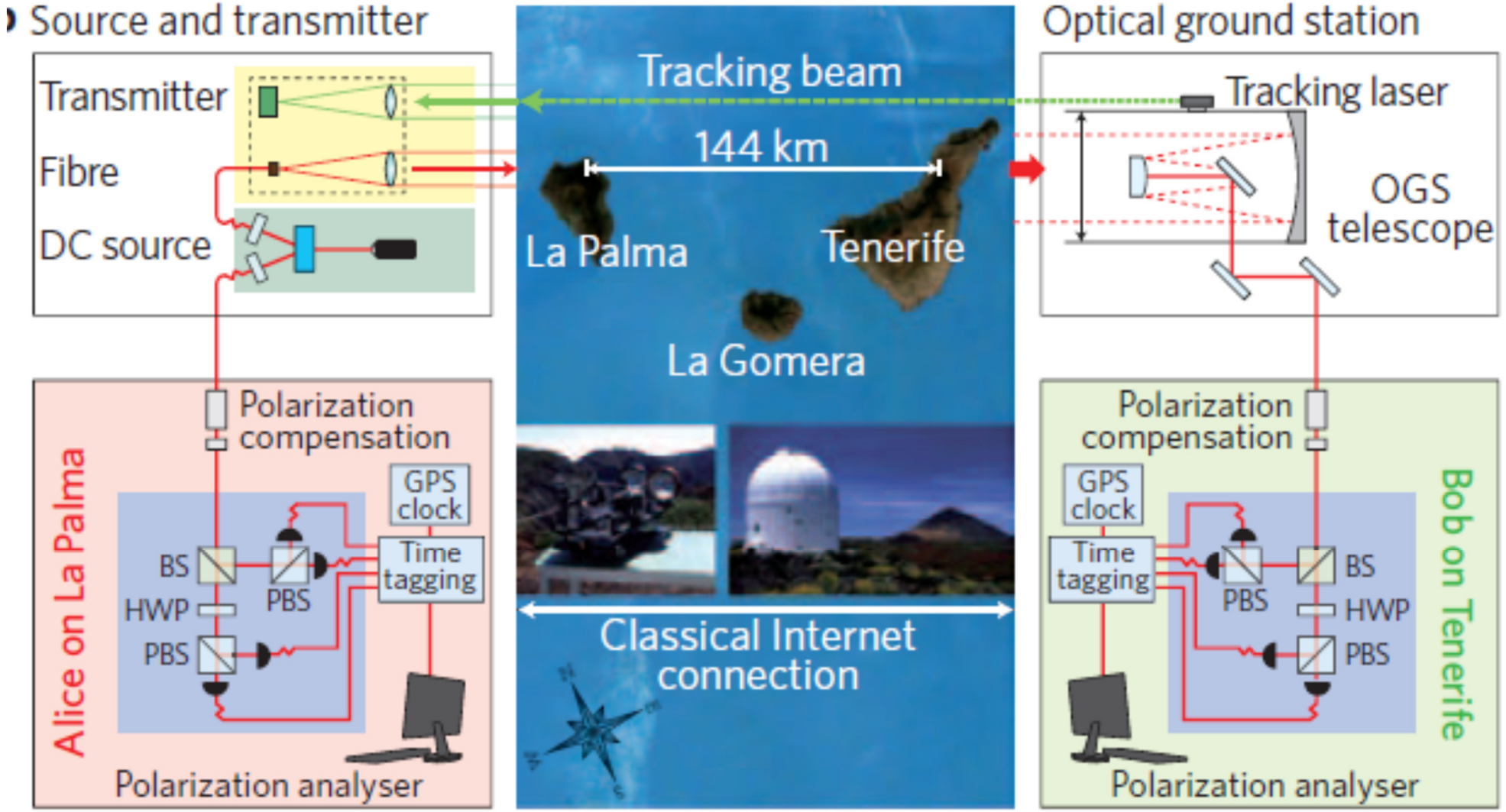

**4** After all the photons have reached Bob, he tells Alice over a public channel, perhaps by telephone or an e-mail, the sequence of filters he used for the incoming photons, but not the bit value of the photons.

**5** Alice tells Bob during the same conversation which filters he chose correctly. Those instances constitute the bits that Alice and Bob will use to form the key that they will use to encrypt messages.




Scientific American 292, 78 (2005)

# Entanglement-based Quantum Key Distribution set-up connecting the two Canary Islands La Palma and Tenerife. The optical link is 144 km long.

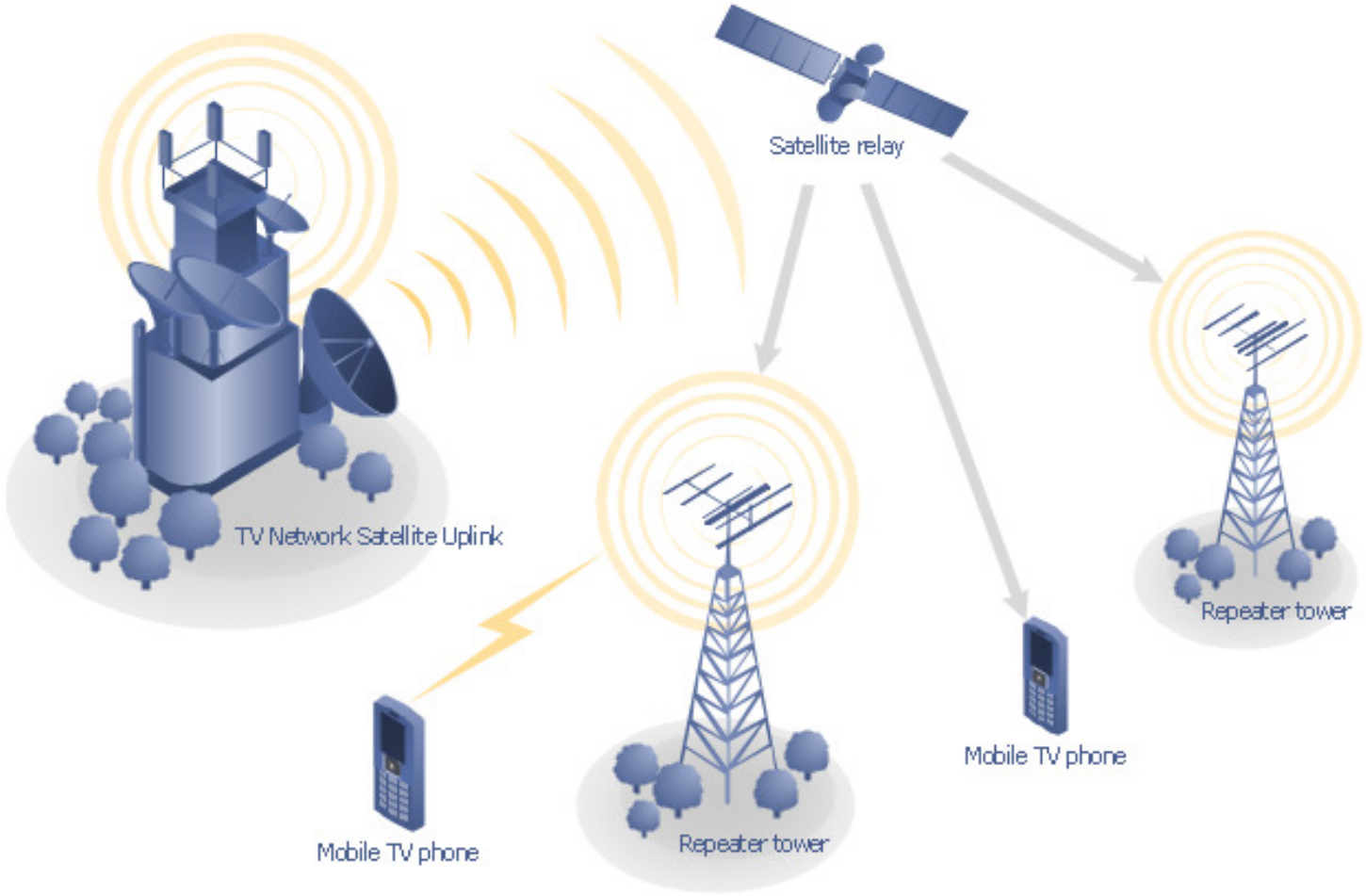



OGS, optical ground station; GPS, Global Positioning System; PBS, polarizing beamsplitter; BS, beamsplitter; HWP, half-wave plate.

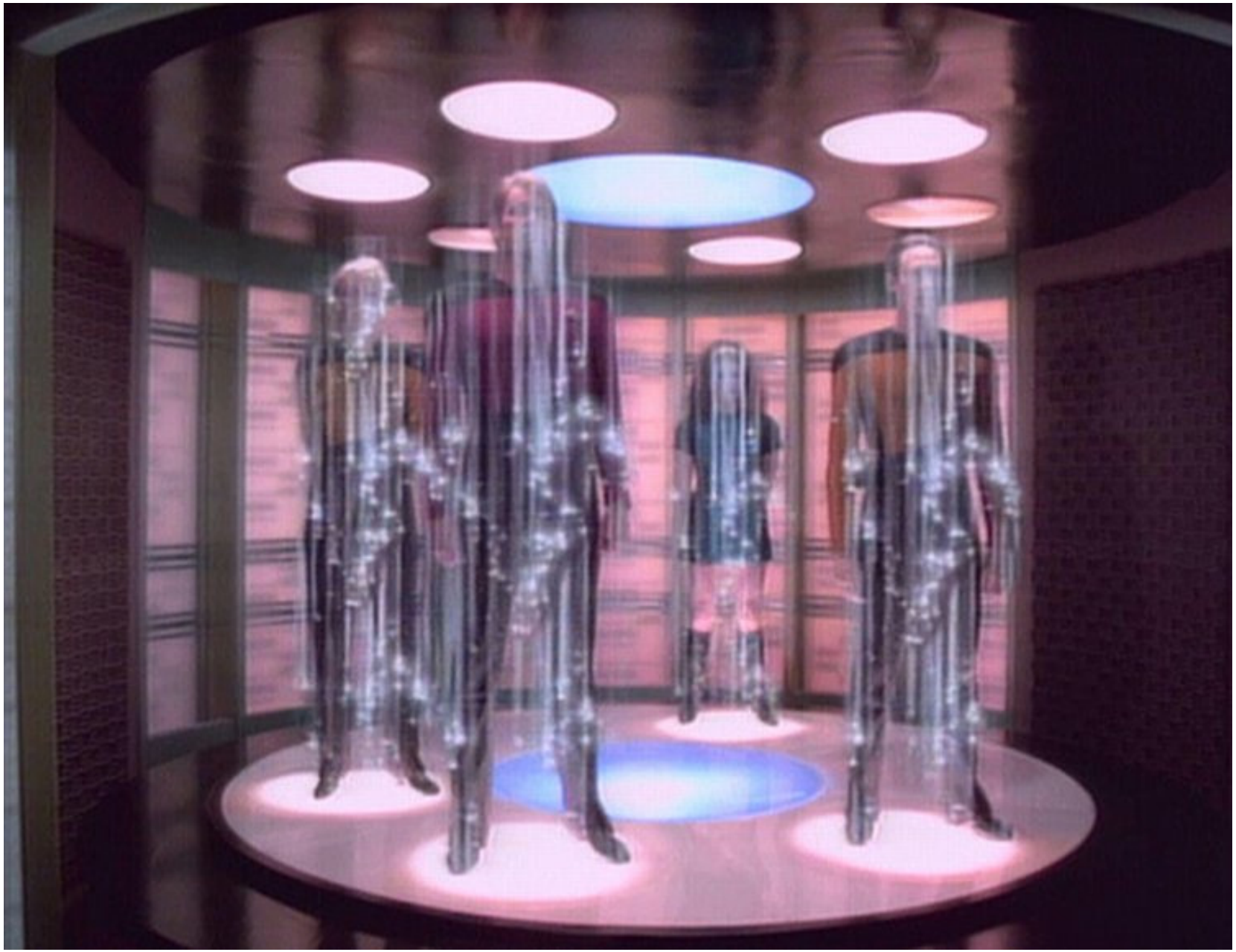
Ursin, R. et al. Nature Phys. 3, 481–486 (2007).

# Problems with quantum key distribution

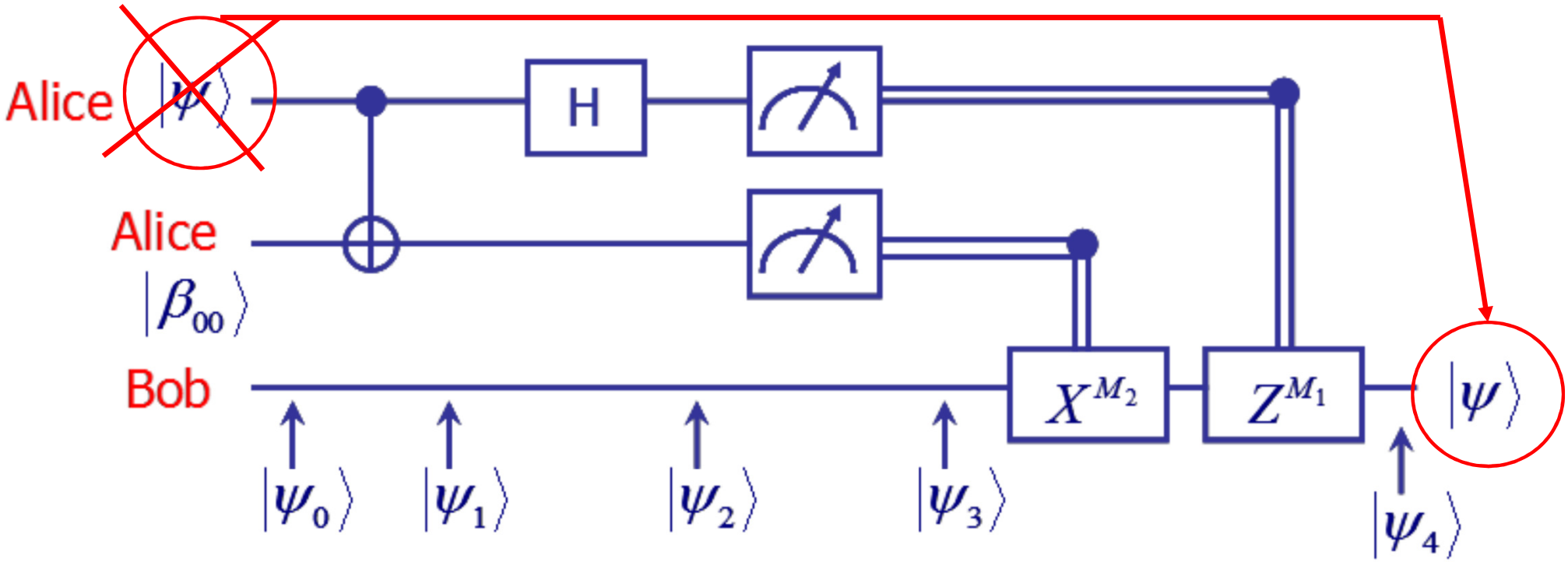
Qubits can not be copied – we can not amplify the signal or retransmit information as in the classical case.



# If you can not copy – teleport!



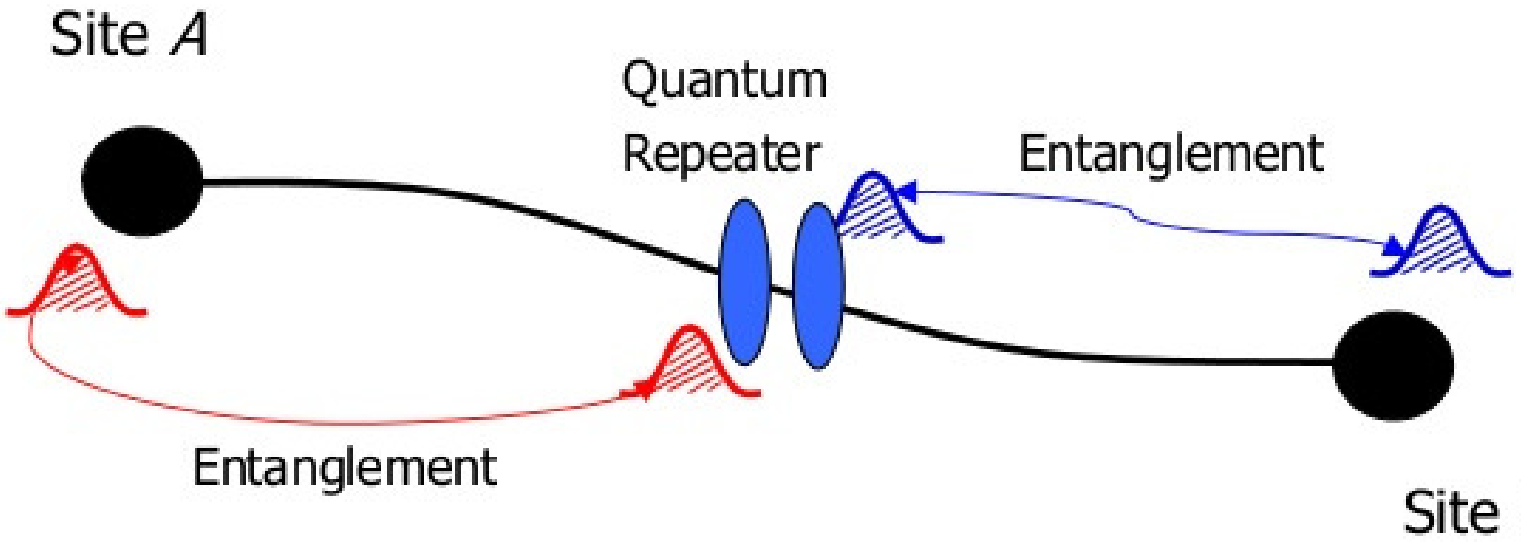
## Teleportation scheme




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

# Quantum Networks

Enable ultra-secure communication over fiber network or free space




**Requirements**

- **Light-matter interface**
- **Quantum memory**
- **Elementary quantum gates**

"The quantum internet", H. J. Kimble, *Nature* **453**, 1023 (2008)

DISTRIBUTION STATEMENT A – Unclassified, Unlimited Distribution

AFRL



Quantum repeater is essentially a small quantum computer!

# Quantum internet ?


Quantum repeater is essentially a small quantum computer –
So need to be able to implement small-scale quantum computing for quantum communications too!

http://www.idquantique.com/
http://www.magiqtech.com