Quantum Key Distribution with BB84

BY @QUANTUMCHEAP

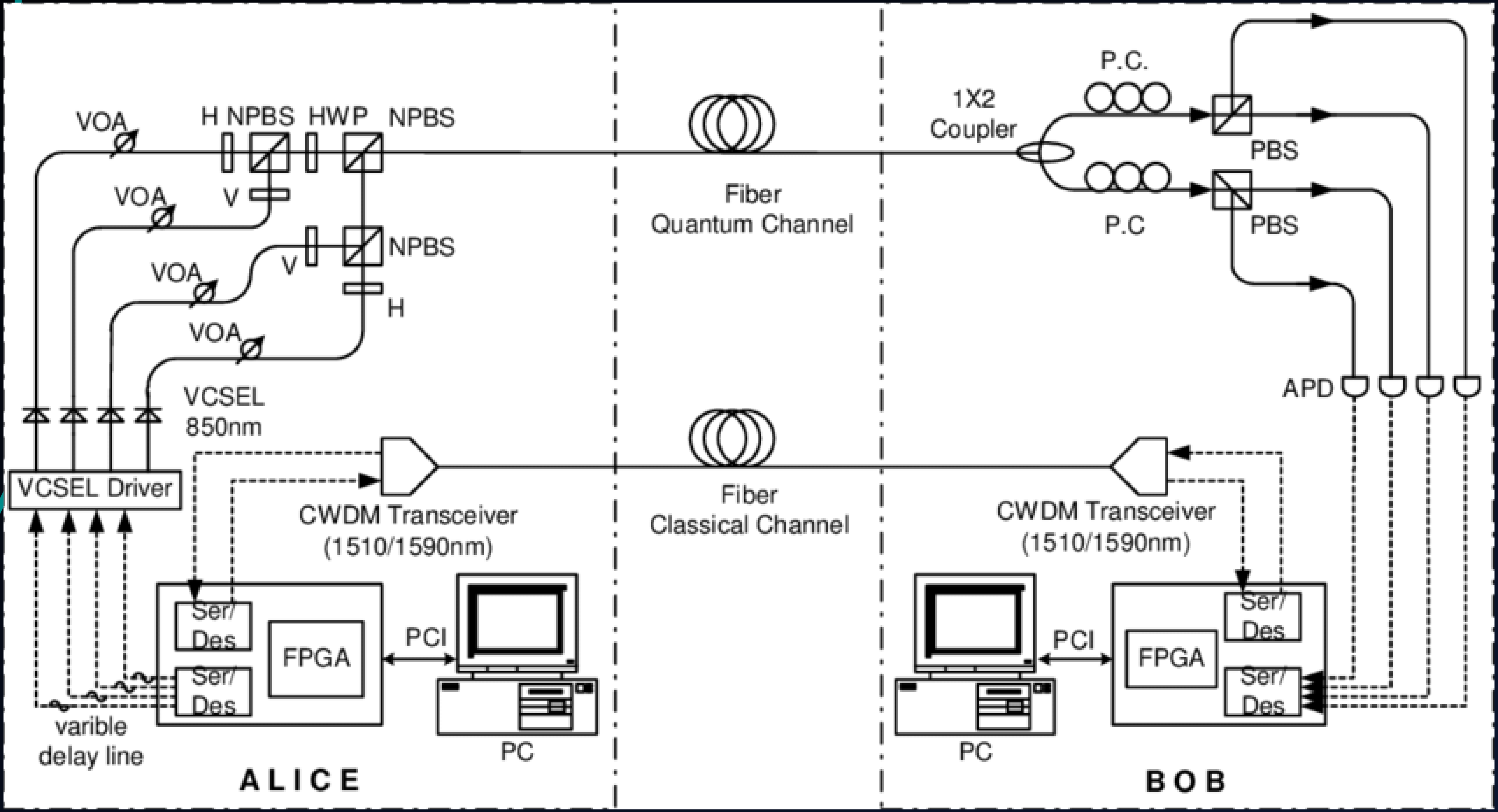
Quantum Key Distribution

- is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics
- There’s an inherent ability for the two communicators to detect the presence of an eavesdropper (since measuring a quantum system disturbs the system)

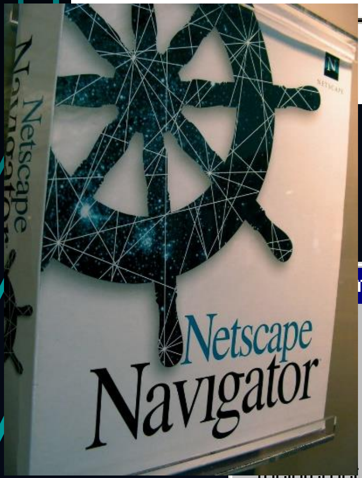
BB84

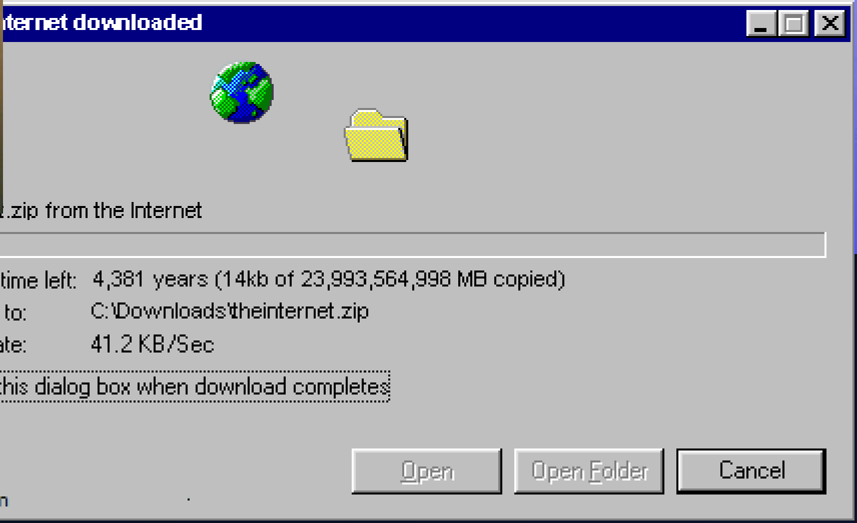
- developed by Charles Bennett and Gilles Brassard in 1984
- It is the first quantum cryptography protocol
- It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.

The Setup


VOA
H NPBS
HWP
NPBS
VOA
V
NPBS
VOA
V
H
VOA
VCSEL
850nm
VCSEL Driver
Fiber
Quantum Channel
Fiber
Classical Channel
CWDM Transceiver
(1510/1590nm)
Ser/
Des
Ser/
Des
FPGA
PCI
PC
varible
delay line
ALICE
P.C.
1X2
Coupler
PBS
P.C
PBS
APD
CWDM Transceiver
(1510/1590nm)
Ser/
Des
FPGA
Ser/
Des
PCI
PC
BOB

The Setup – Classic Channel




ternet downloaded

theinternet.zip from the Internet

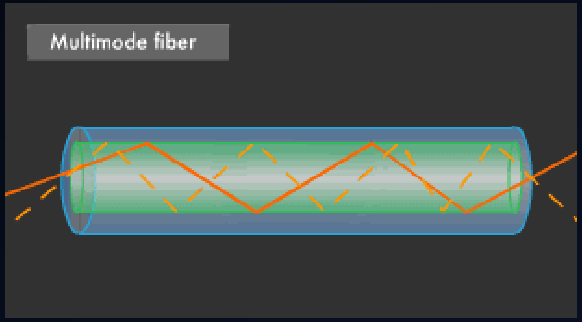
Estimated time left: 4,381 years (14kb of 23,993,564,998 MB copied)

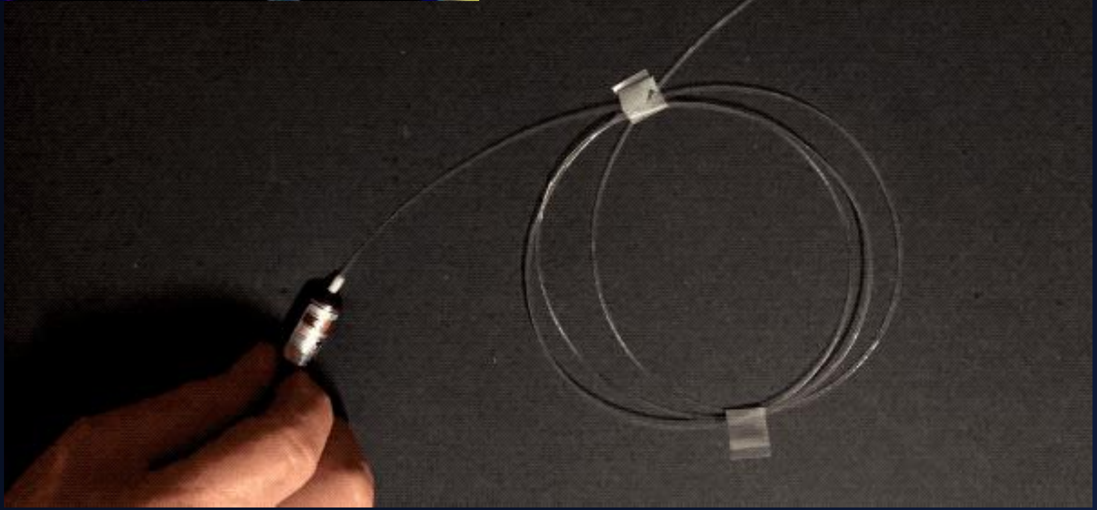
Download to: C:\Downloads\theinternet.zip

Transfer rate: 41.2 KB/Sec

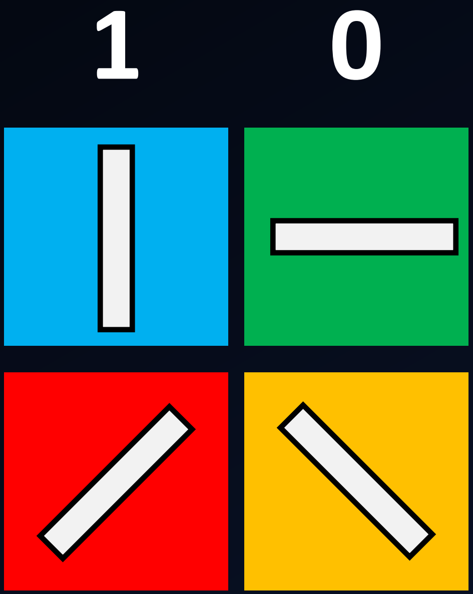
☑ Close this dialog box when download completes

The Setup – Quantum Channel





The Setup – Quantum Channel



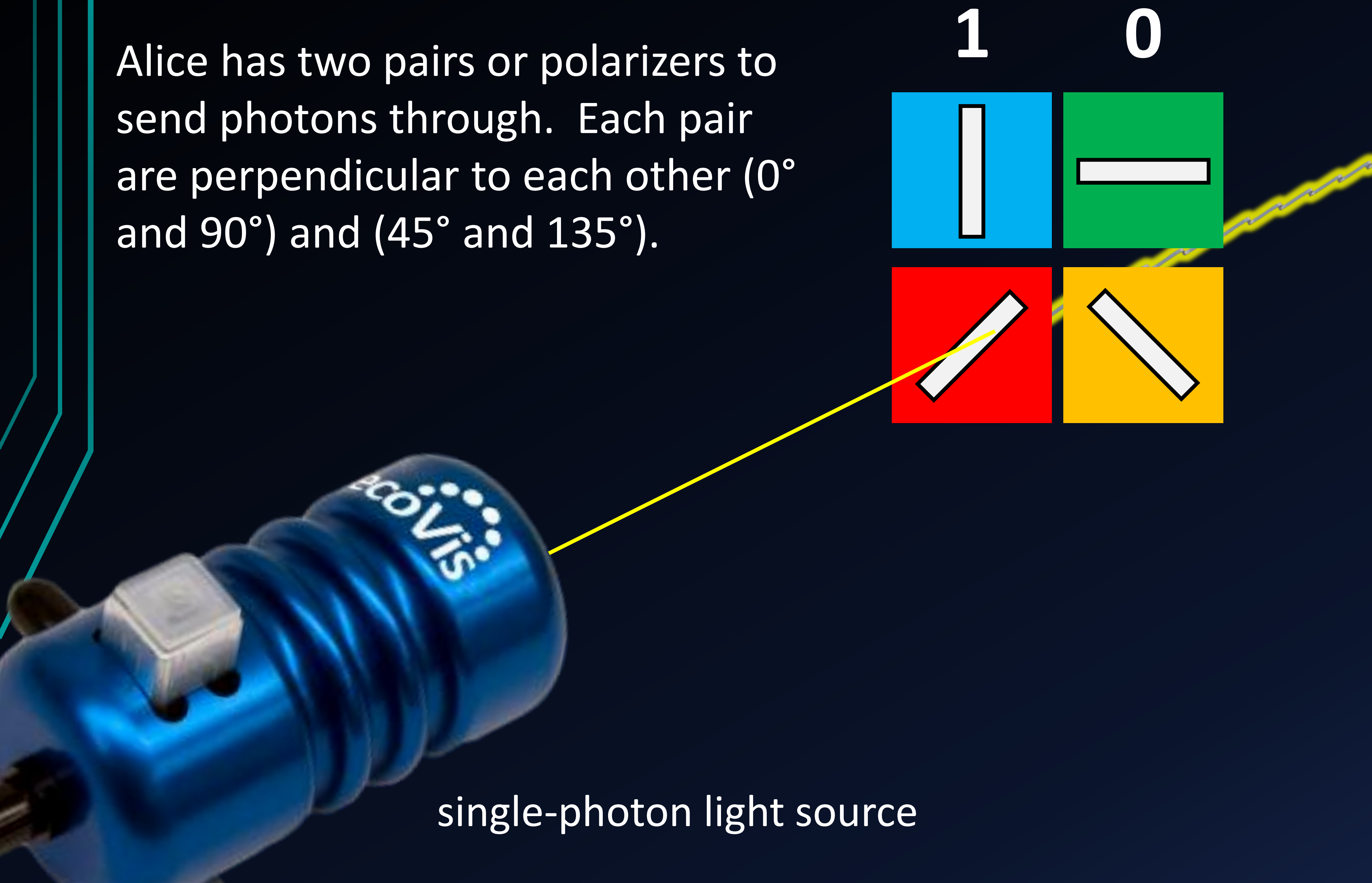
Measurement Basis

Rectilinear +

Diagonal ×

The Setup – Quantum Channel

Alice has two pairs or polarizers to send photons through. Each pair are perpendicular to each other (0° and 90°) and (45° and 135°).

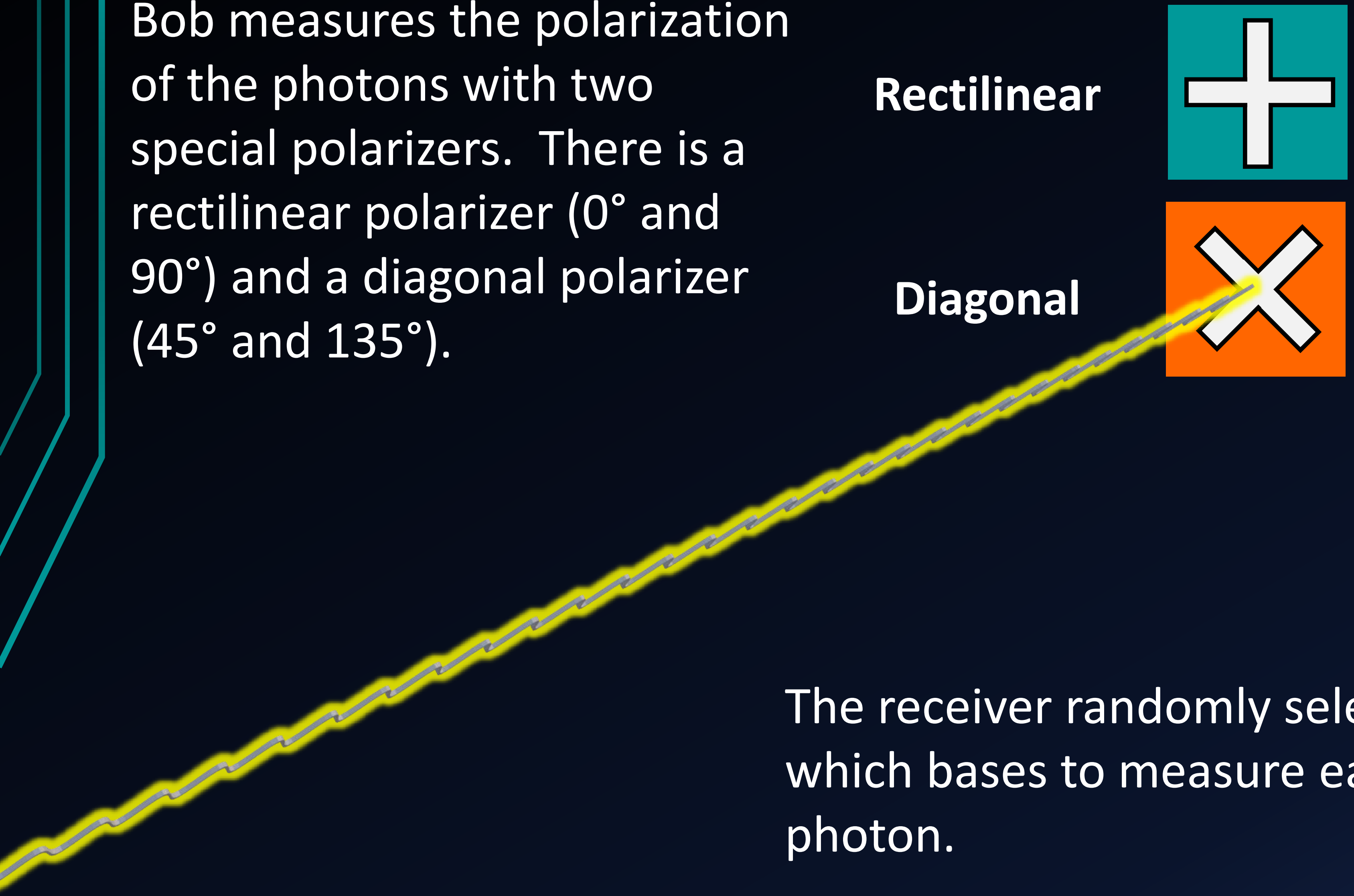


single-photon light source

The Setup – Quantum Channel

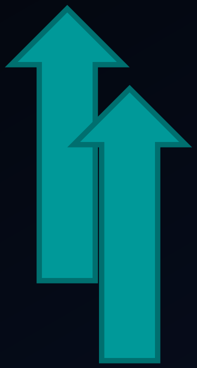
Mea

Bob measures the polarization of the photons with two special polarizers. There is a rectilinear polarizer (0° and 90°) and a diagonal polarizer (45° and 135°).

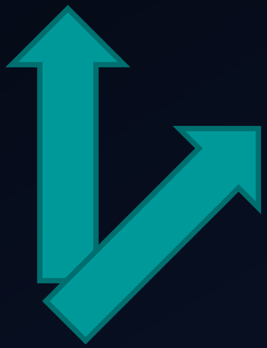


The receiver randomly selects which bases to measure each photon.

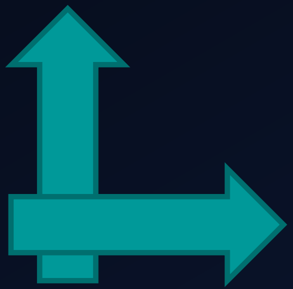
Polarization Demo



0° rotation
100%
pass-through

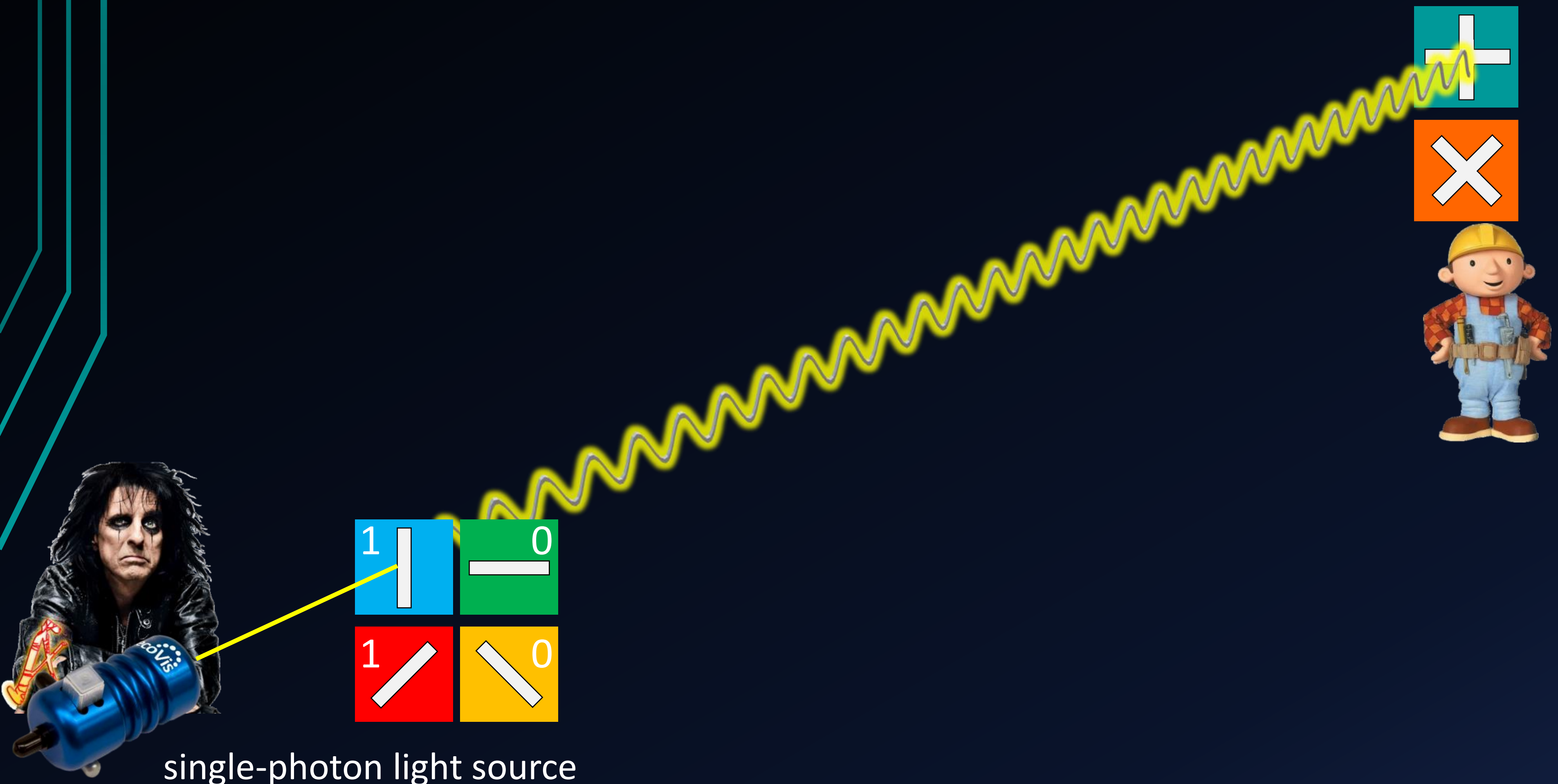


45° rotation
50%
pass-through



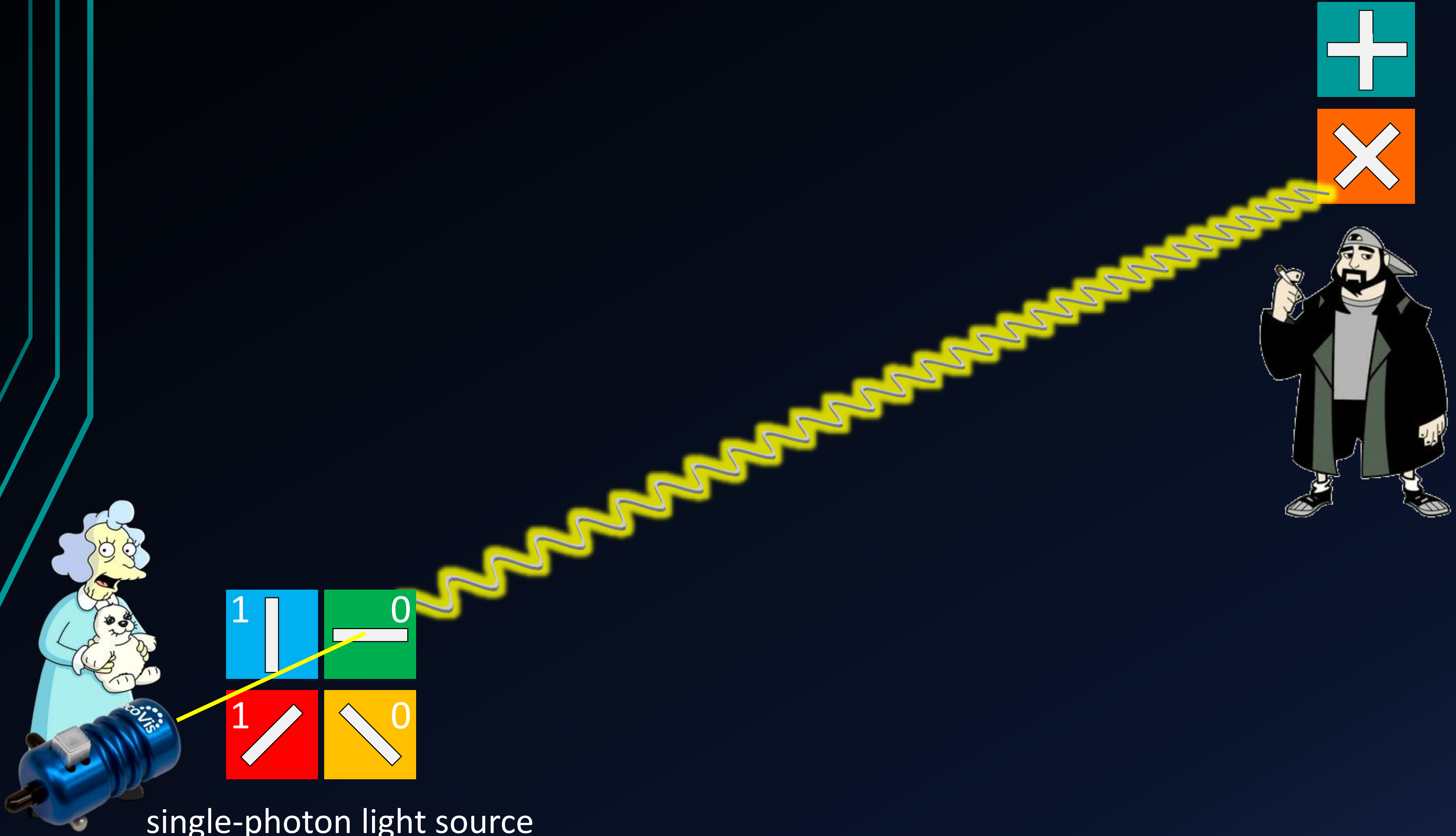
90° rotation
0%
pass-through

Photon polarization Alice sends	1 │							
Bob's random measuring basis	+							
Photon polarization Bob measures	1 │							

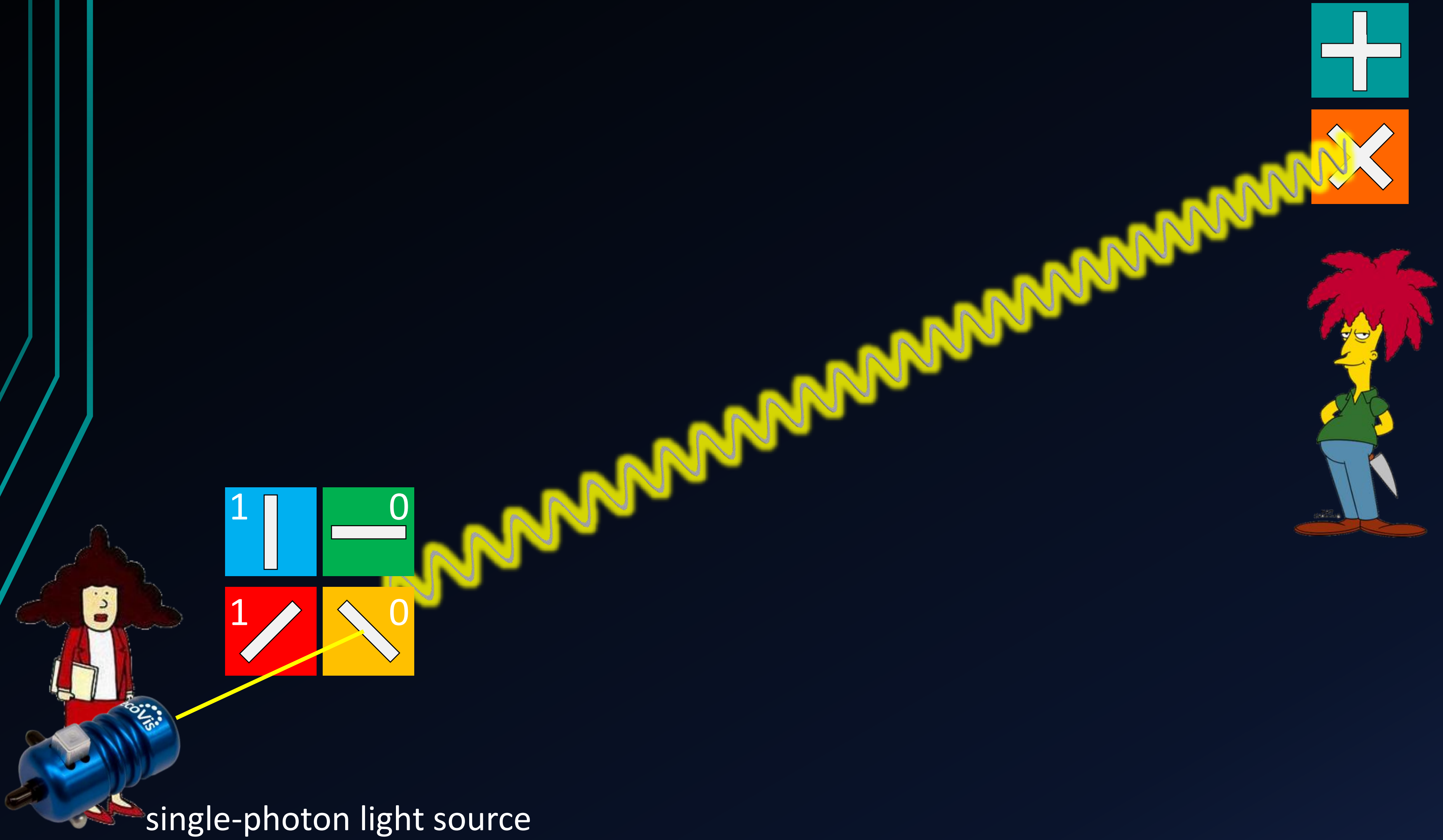


single-photon light source

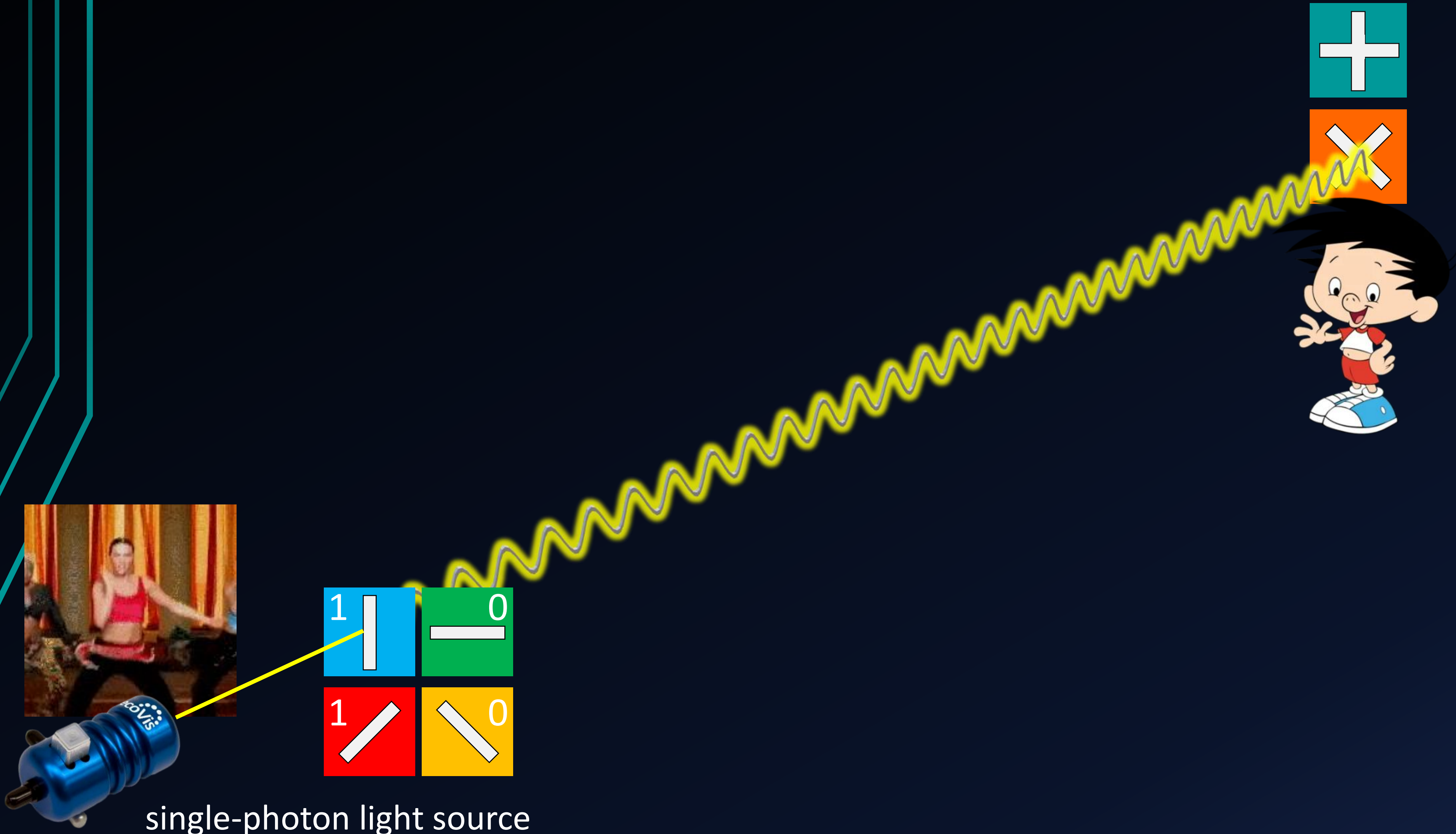
Photon polarization Alice sends	1 |	— 0						
Bob's random measuring basis	+	×						
Photon polarization Bob measures	1 |	1 /						



Photon polarization Alice sends	1 |	— 0	╲ 0					
Bob's random measuring basis	+	×	×					
Photon polarization Bob measures	1 |	1 ╱	╲ 0					

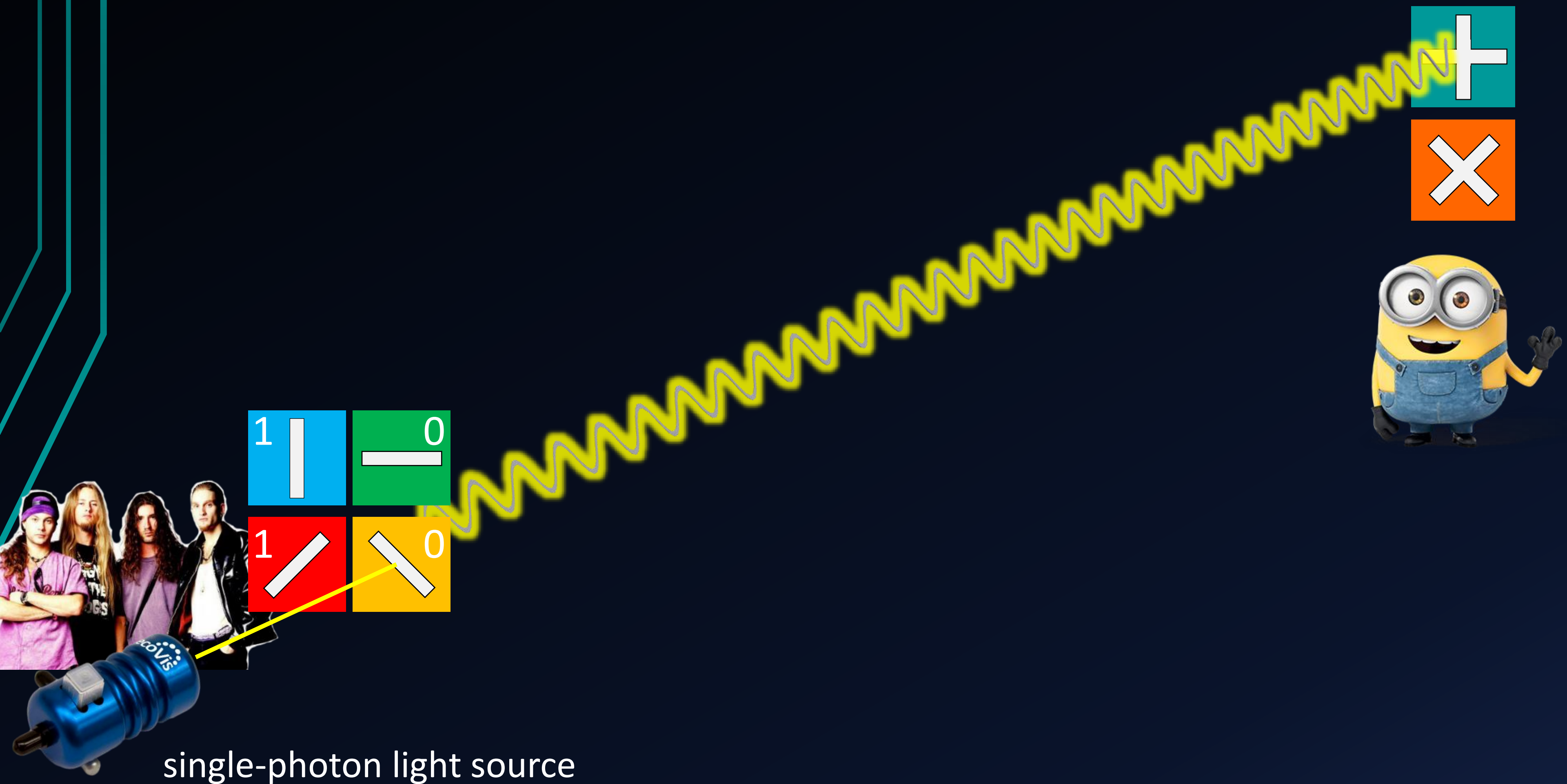


Photon polarization Alice sends	1 |	— 0	╲ 0	1 |				
Bob's random measuring basis	+	×	×	×				
Photon polarization Bob measures	1 |	1 ╱	╲ 0	1 ╱				



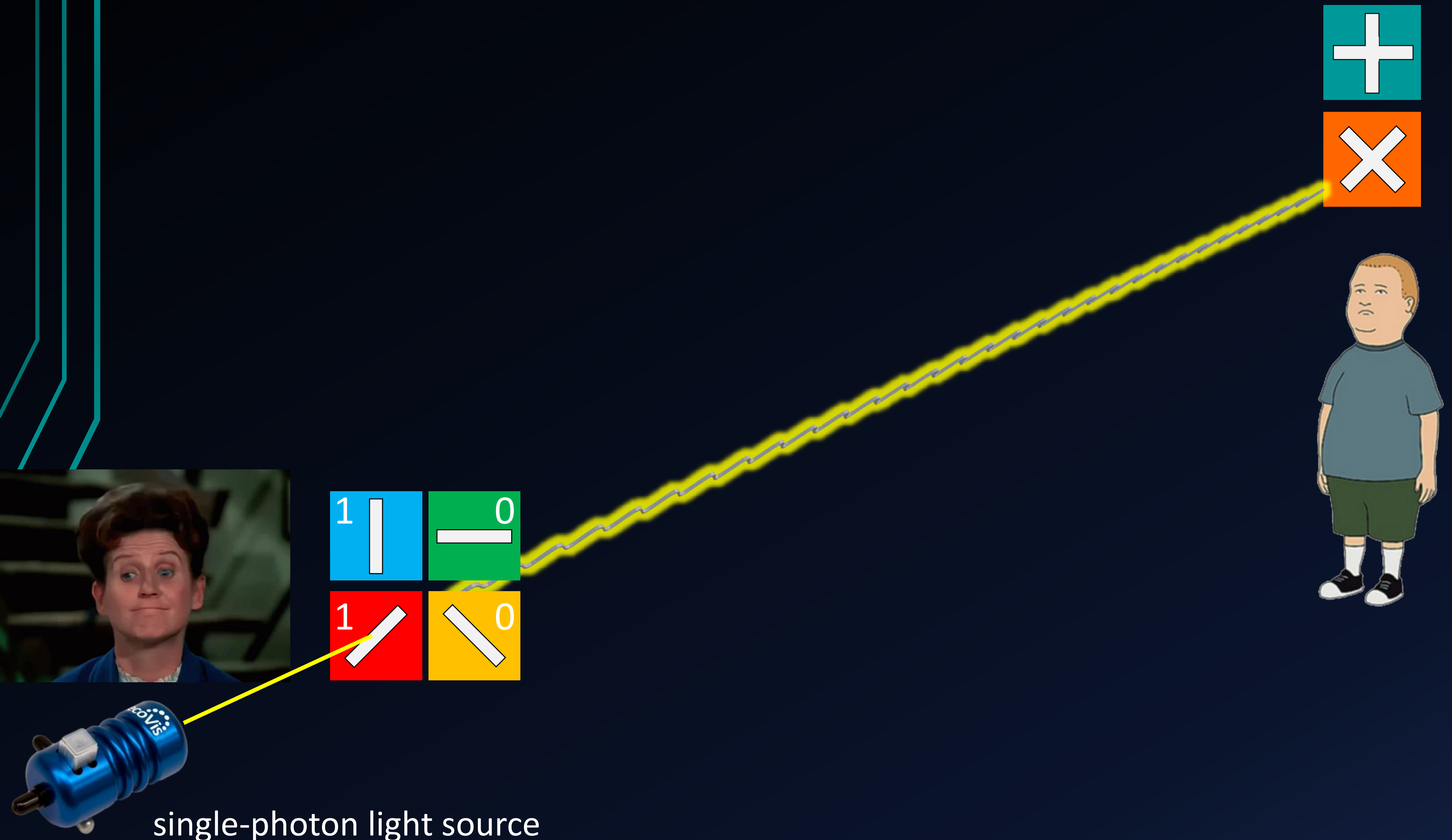
single-photon light source

Photon polarization Alice sends	1 |	0 —	0 ╲	1 |	0 ╲			
Bob's random measuring basis	+	×	×	×	+			
Photon polarization Bob measures	1 |	1 ╱	0 ╲	1 ╱	0 —			



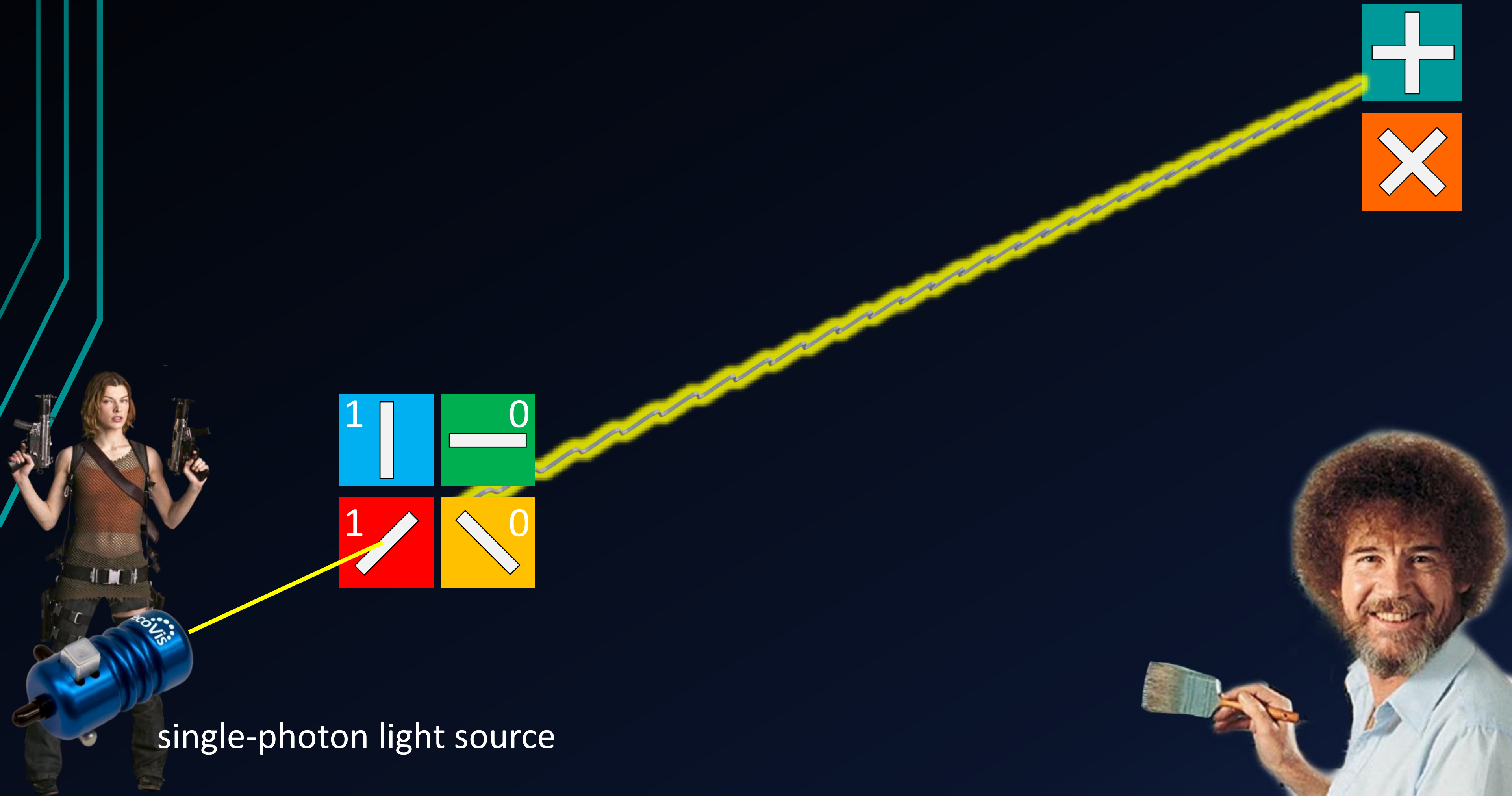
single-photon light source

Photon polarization Alice sends	1 |	0 —	0 ╲	1 |	0 ╲	1 ╱		
Bob's random measuring basis	+	×	×	×	+	×		
Photon polarization Bob measures	1 |	1 ╱	0 ╲	1 ╱	0 —	1 ╱		

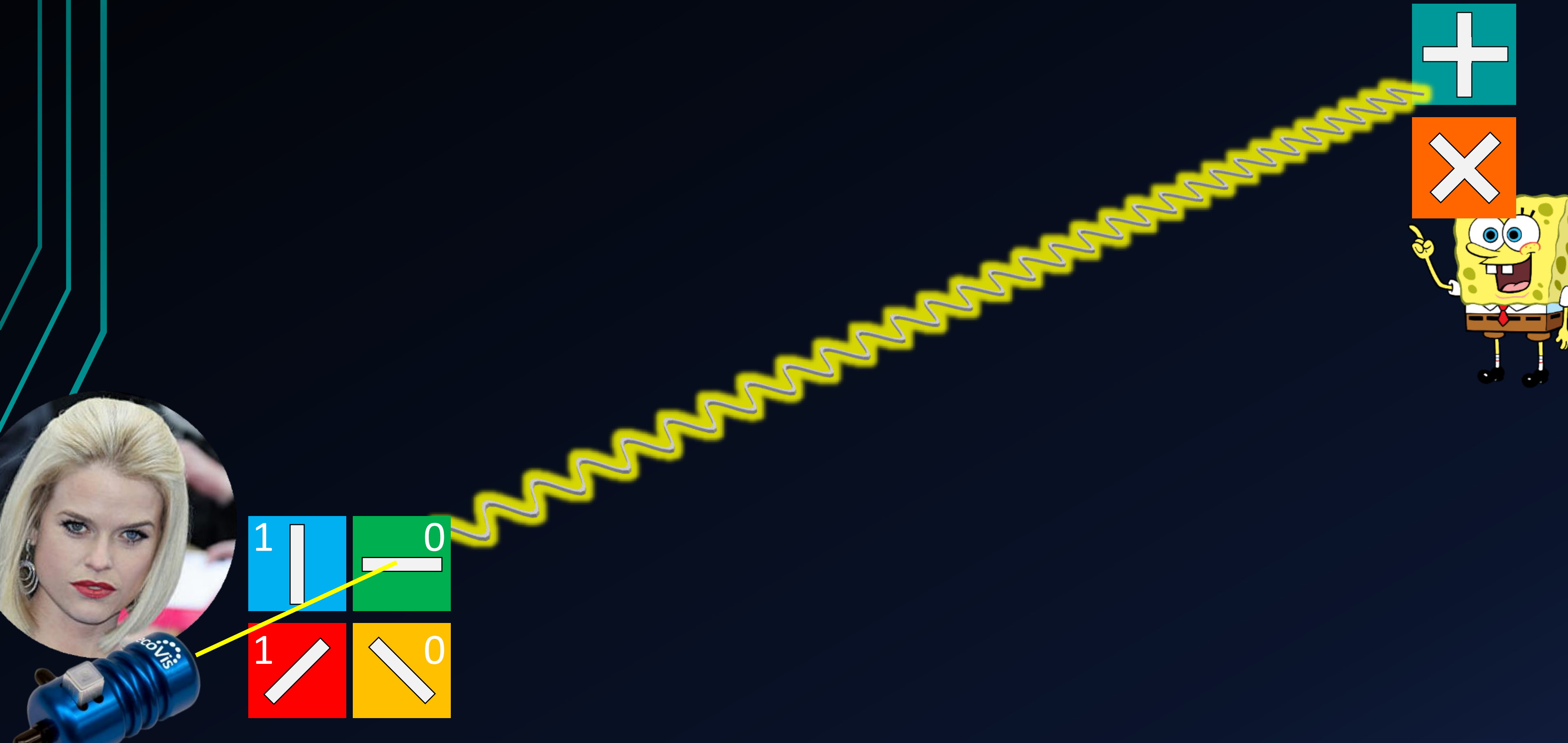


single-photon light source

Photon polarization Alice sends	1 │	— 0	╲ 0	1 │	╲ 0	1 ╱	1 ╱	
Bob's random measuring basis	✚	✕	✕	✕	✚	✕	✚	
Photon polarization Bob measures	1 │	1 ╱	╲ 0	1 ╱	— 0	1 ╱	— 0	



Photon polarization Alice sends	1 │	— 0	╲ 0	1 │	╲ 0	1 ╱	1 ╱	— 0
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	1 │	1 ╱	╲ 0	1 ╱	— 0	1 ╱	— 0	— 0



single-photon light source

Back on the classic channel…

Bob and Alice compare which basis they used to send and receive each qubit

Photon polarization Alice sends	1 |	0 —	0 ╲	1 |	0 ╲	1 ╱	1 ╱	0 —
Alice’s sending basis	+	+	×	+	×	×	×	+
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	1 |	1 ╱	0 ╲	1 ╱	0 —	1 ╱	0 —	0 —
PUBLIS DISCUSSION OF BASIS								
Shared secret key	1		0			1		0

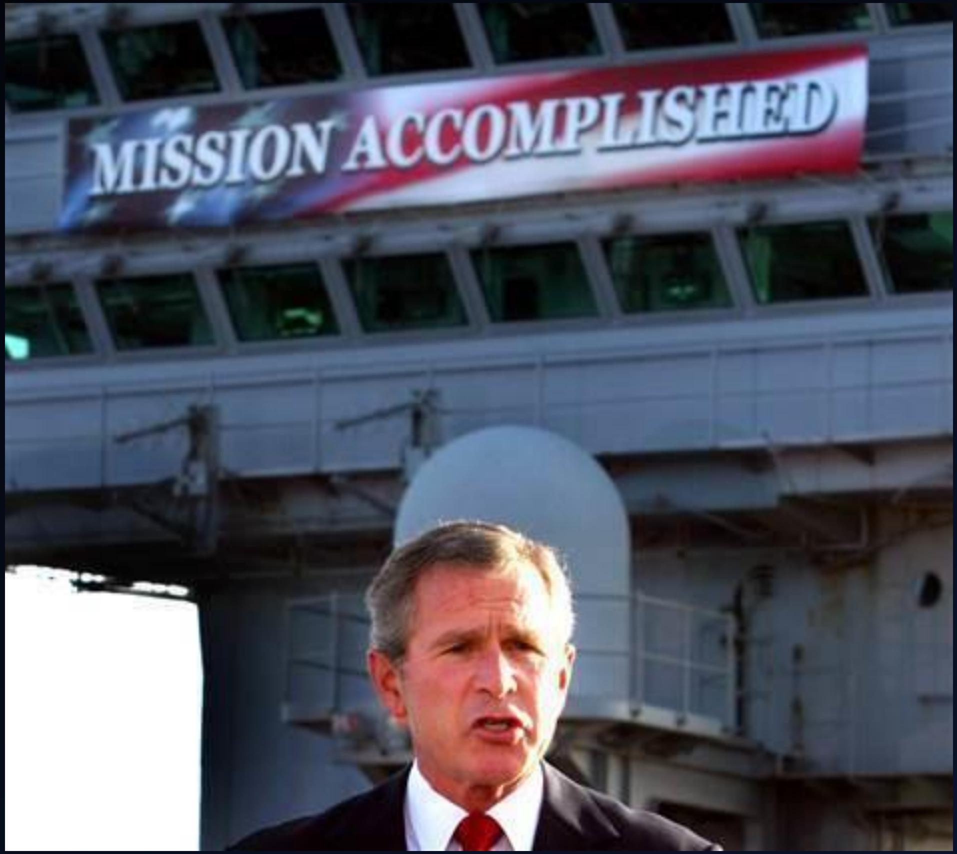
The bits corresponding to matching basises become the key!

Key = “1010”

Why Does This Work?

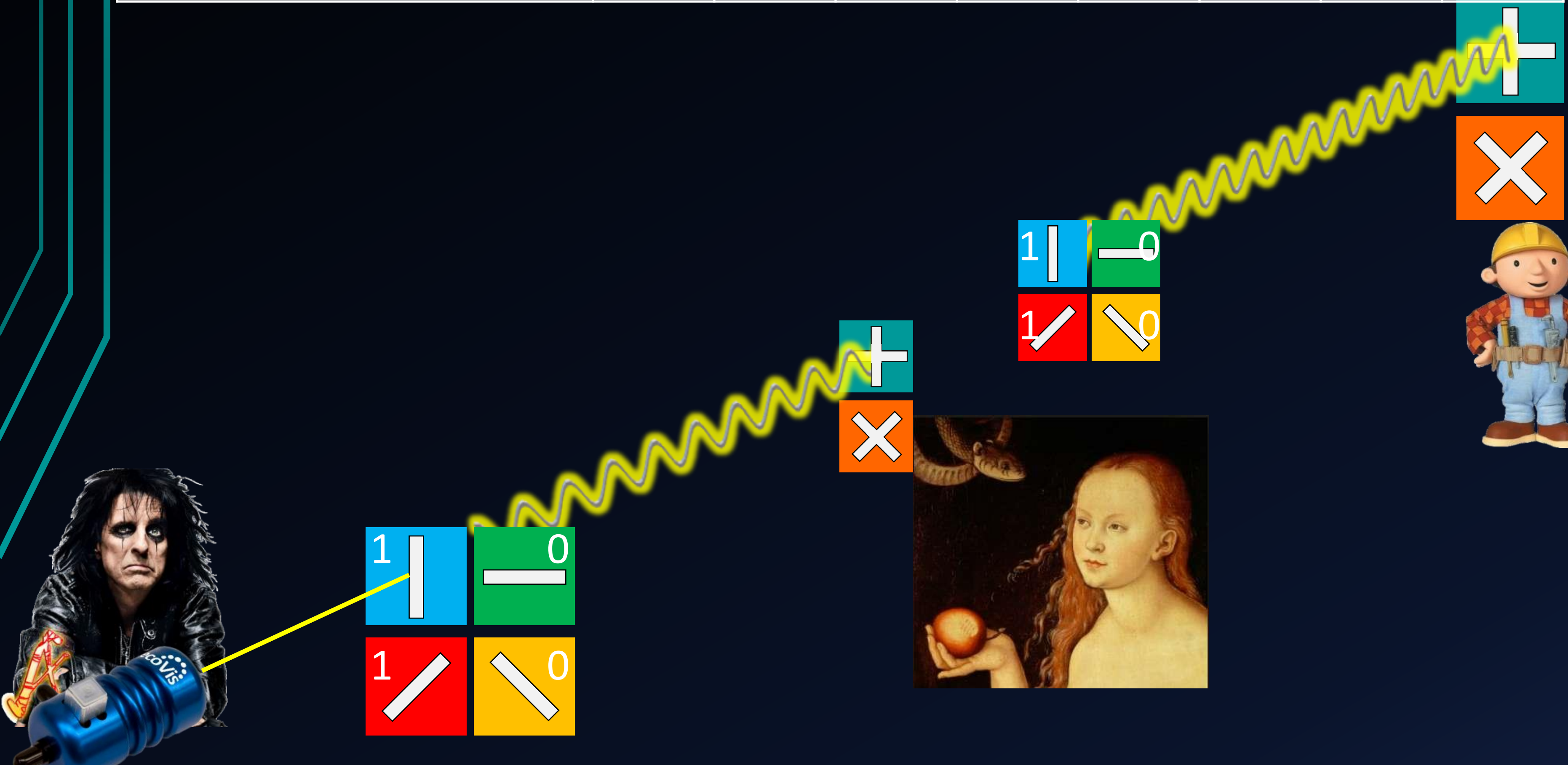
Mission accomplished?

…or “mission accomplished”?



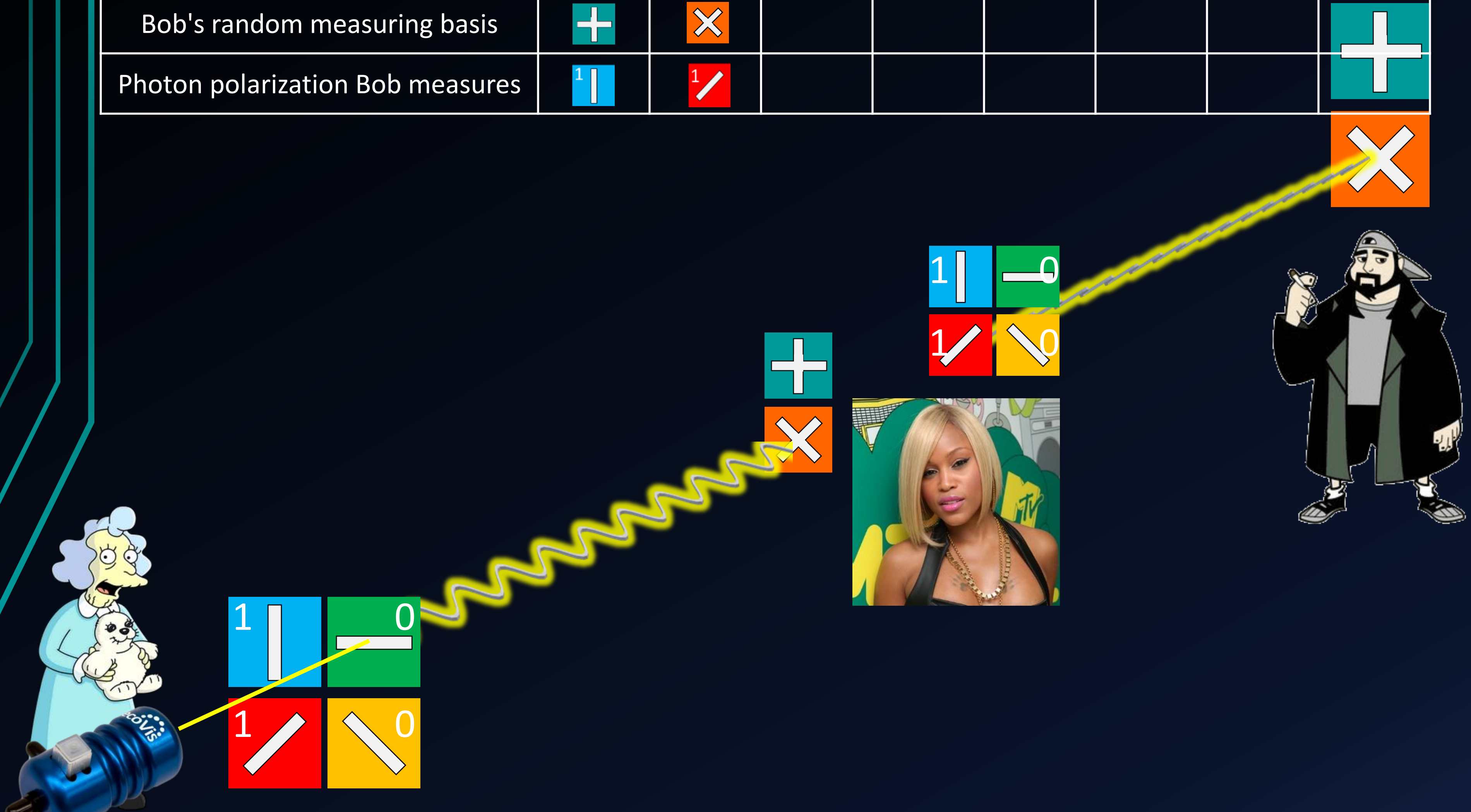
We’ve got an eavesdropper!

Photon polarization Alice sends	1 |							
Eve’s random measuring basis	+							
Polarization Eve measures and sends	1 |							
Bob's random measuring basis	+							
Photon polarization Bob measures	1 |							



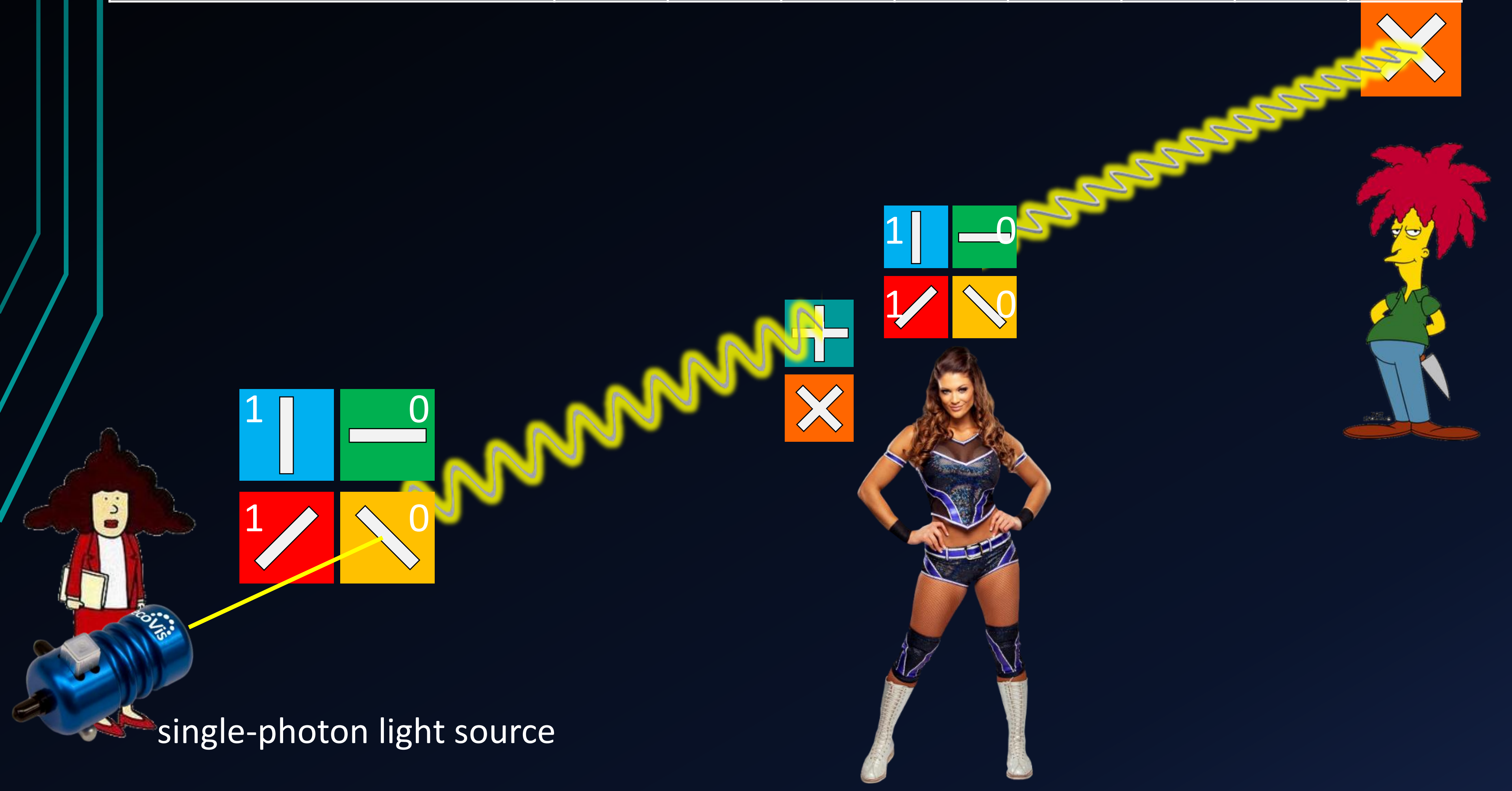
single-photon light source

Photon polarization Alice sends	1 |	— 0						
Eve’s random measuring basis	+	×						
Polarization Eve measures and sends	1 |	1 /						
Bob's random measuring basis	+	×						
Photon polarization Bob measures	1 |	1 /						

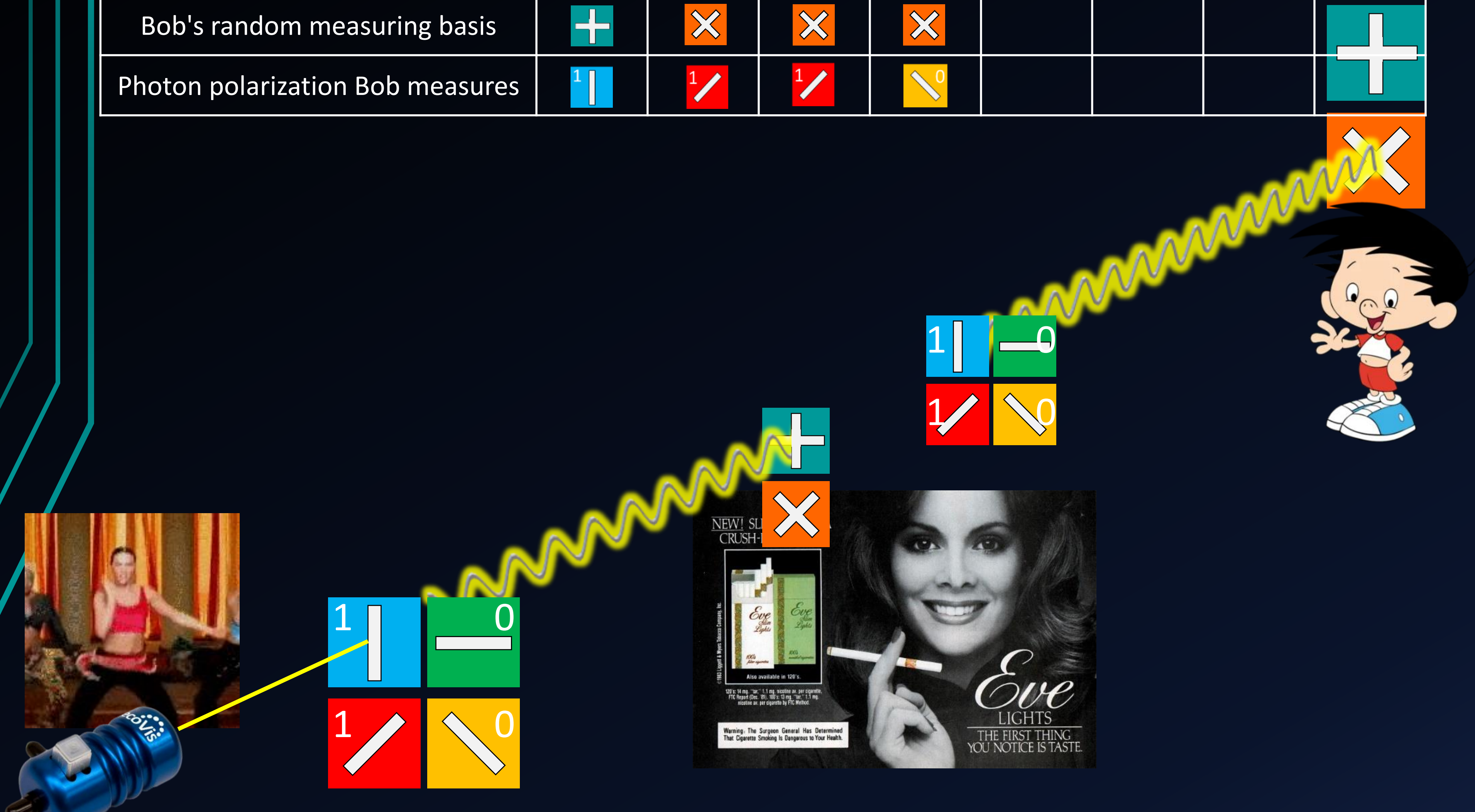


single-photon light source

Photon polarization Alice sends	1 |	— 0	\ 0					
Eve’s random measuring basis	+	×	+					
Polarization Eve measures and sends	1 |	1 /	— 0					
Bob's random measuring basis	+	×	×					
Photon polarization Bob measures	1 |	1 /	1 /					

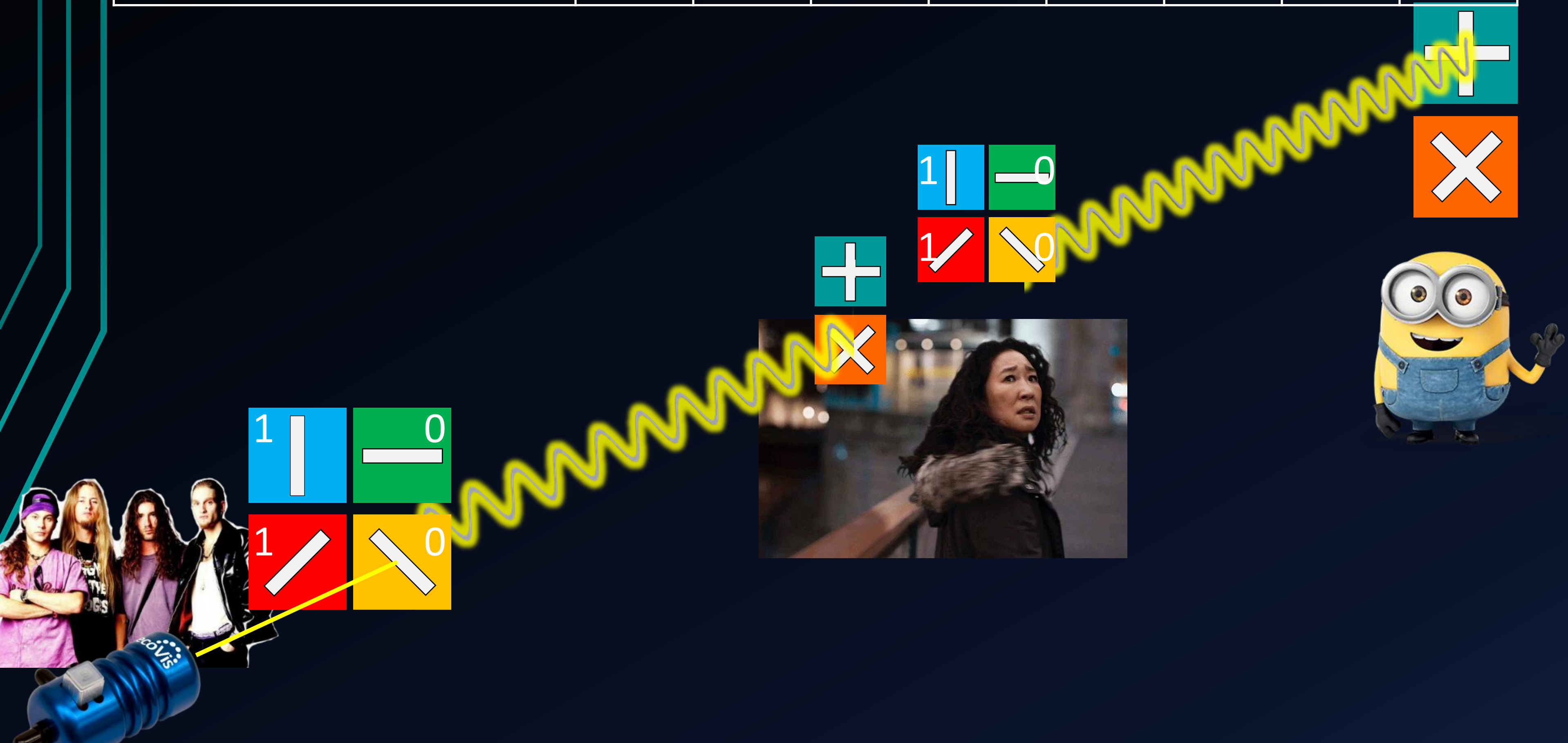


Photon polarization Alice sends	1 │	— 0	╲ 0	1 │				
Eve’s random measuring basis	+	×	+	+				
Polarization Eve measures and sends	1 │	1 ╱	— 0	1 │				
Bob's random measuring basis	+	×	×	×				
Photon polarization Bob measures	1 │	1 ╱	1 ╱	╲ 0				



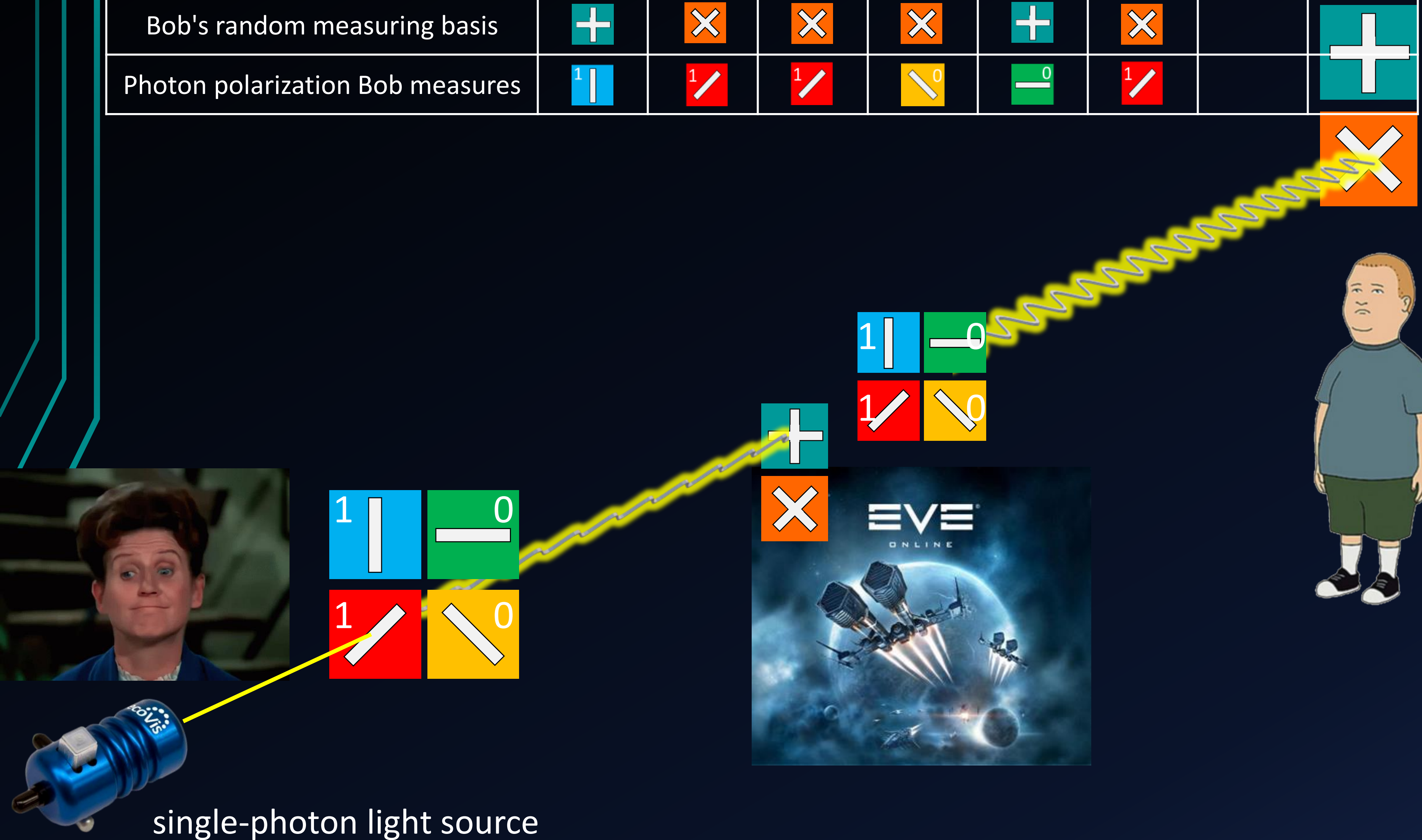
single-photon light source

Photon polarization Alice sends	1 |	— 0	╲ 0	1 |	╲ 0			
Eve’s random measuring basis	+	×	+	+	×			
Polarization Eve measures and sends	1 |	1 ╱	— 0	1 |	╲ 0			
Bob's random measuring basis	+	×	×	×	+			
Photon polarization Bob measures	1 |	1 ╱	1 ╱	╲ 0	— 0			



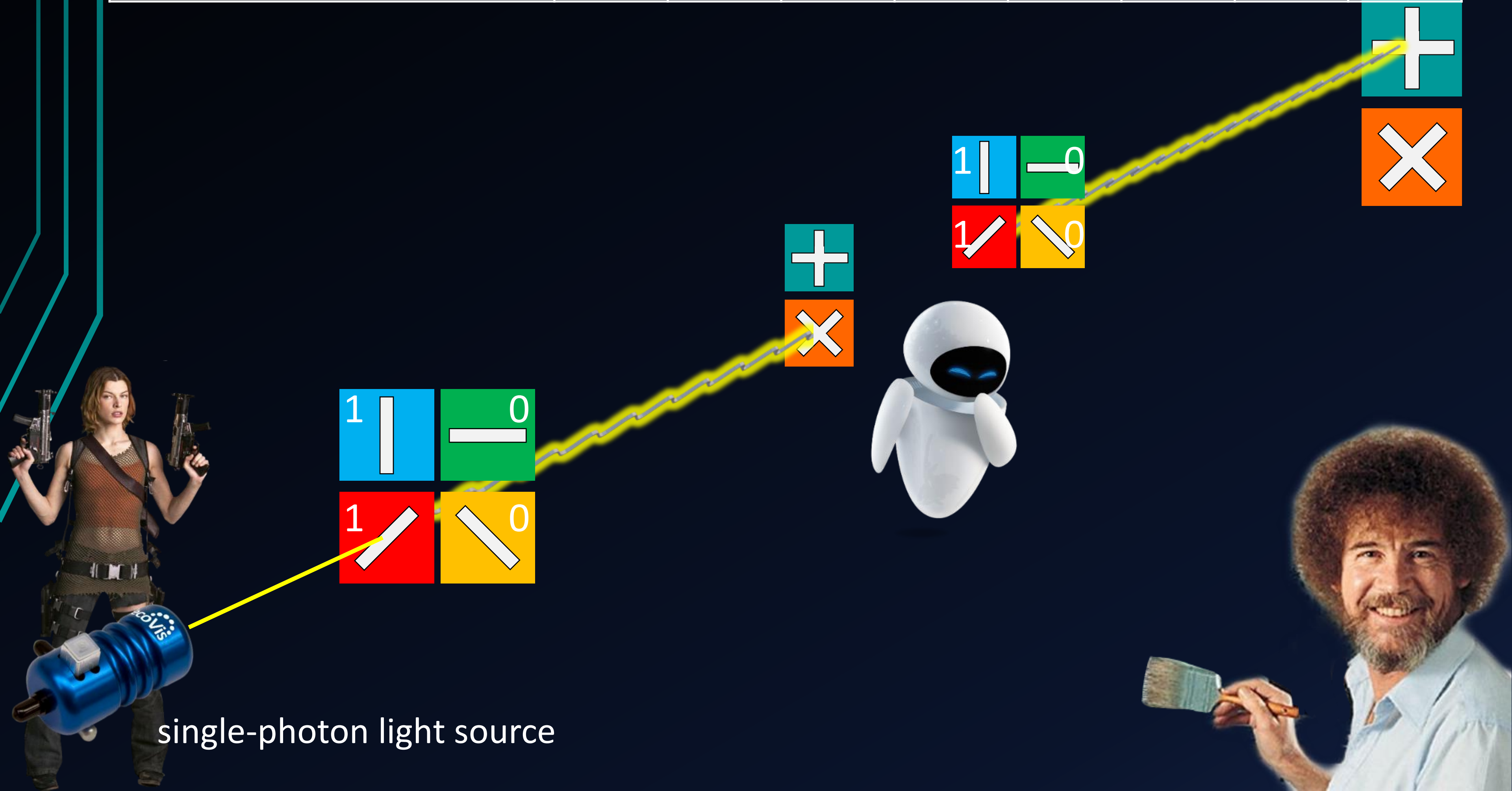
single-photon light source

Photon polarization Alice sends	1 |	0 —	0 ╲	1 |	0 ╲	1 ╱		
Eve’s random measuring basis	+	×	+	+	×	+		
Polarization Eve measures and sends	1 |	1 ╱	0 —	1 |	0 ╲	0 —		
Bob's random measuring basis	+	×	×	×	+	×		
Photon polarization Bob measures	1 |	1 ╱	1 ╱	0 ╲	0 —	1 ╱		

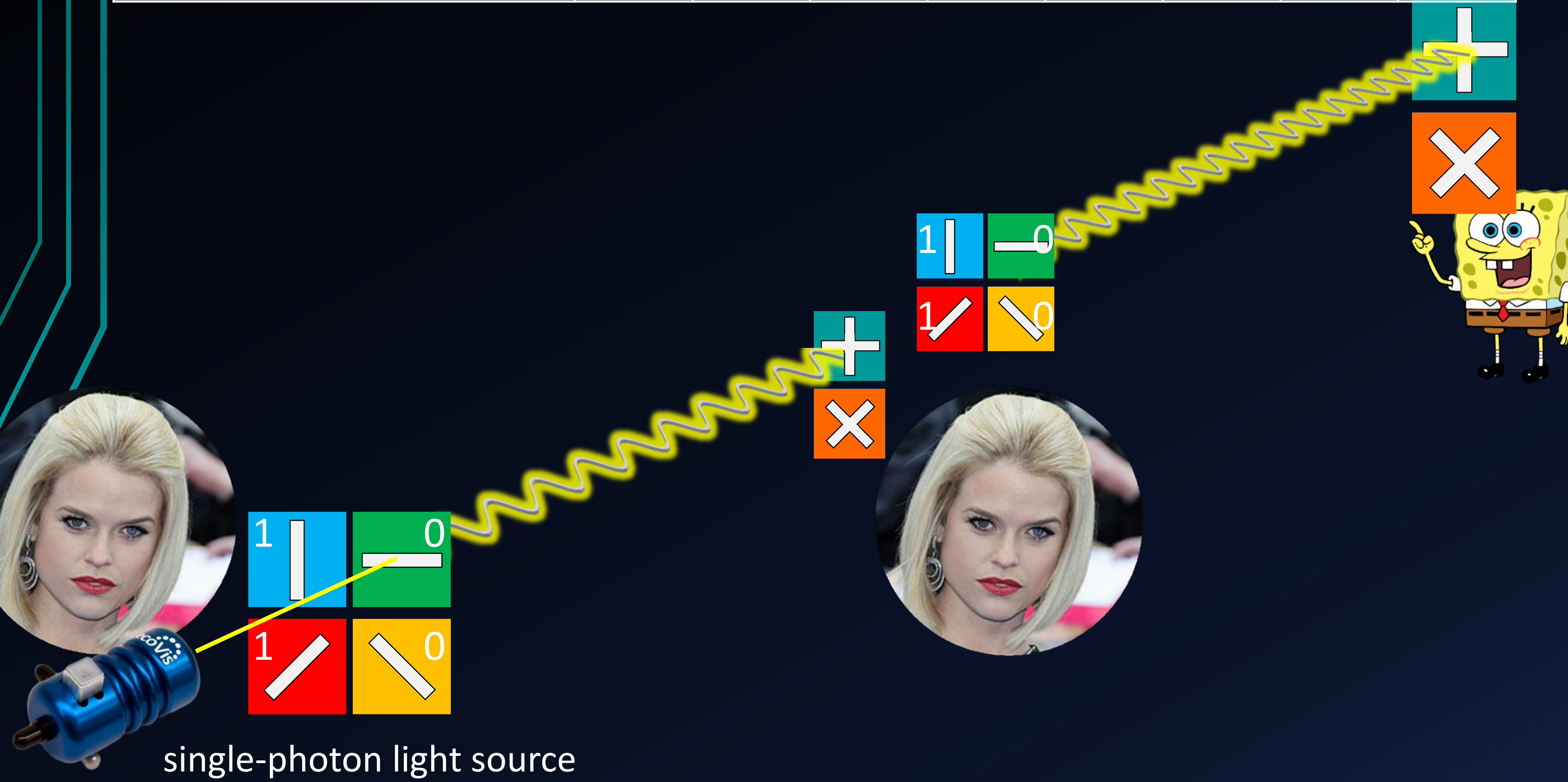


single-photon light source

Photon polarization Alice sends	1 |	— 0	\ 0	1 |	\ 0	1 /	1 /	
Eve’s random measuring basis	+	×	+	+	×	+	×	
Polarization Eve measures and sends	1 |	1 /	— 0	1 |	\ 0	— 0	1 /	
Bob's random measuring basis	+	×	×	×	+	×	+	
Photon polarization Bob measures	1 |	1 /	1 /	\ 0	— 0	1 /	1 |	



Photon polarization Alice sends	1 |	— 0	╲ 0	1 |	╲ 0	1 ╱	1 ╱	— 0
Eve’s random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	1 |	1 ╱	— 0	1 |	╲ 0	— 0	1 ╱	— 0
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	1 |	1 ╱	1 ╱	╲ 0	— 0	1 ╱	1 |	— 0



Back on the classic channel…

Photon polarization Alice sends	1 |	0 —	0 ╲	1 |	0 ╲	1 ╱	1 ╱	0 —
Alice's sending basis	+	+	×	+	×	×	×	+
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	1 |	1 ╱	0 —	1 |	0 ╲	0 —	1 ╱	0 —
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	1 |	1 ╱	1 ╱	0 ╲	0 —	1 ╱	1 |	0 —
PUBLIS DISCUSSION OF BASIS								
Shared secret key	1		1			1		0
Errors in key	✓		✗			✓		✓

What do we do now?

- (Assuming Alice chooses randomly) the probability Eve chooses the incorrect basis is 50%.
- If Bob measures Eve's photon in the same basis that Alice sent, he gets a random result, i.e., an incorrect result with probability of 50%.
- So, the probability an intercepted photon generates an error in the key string is then 50% × 50% = **25%**

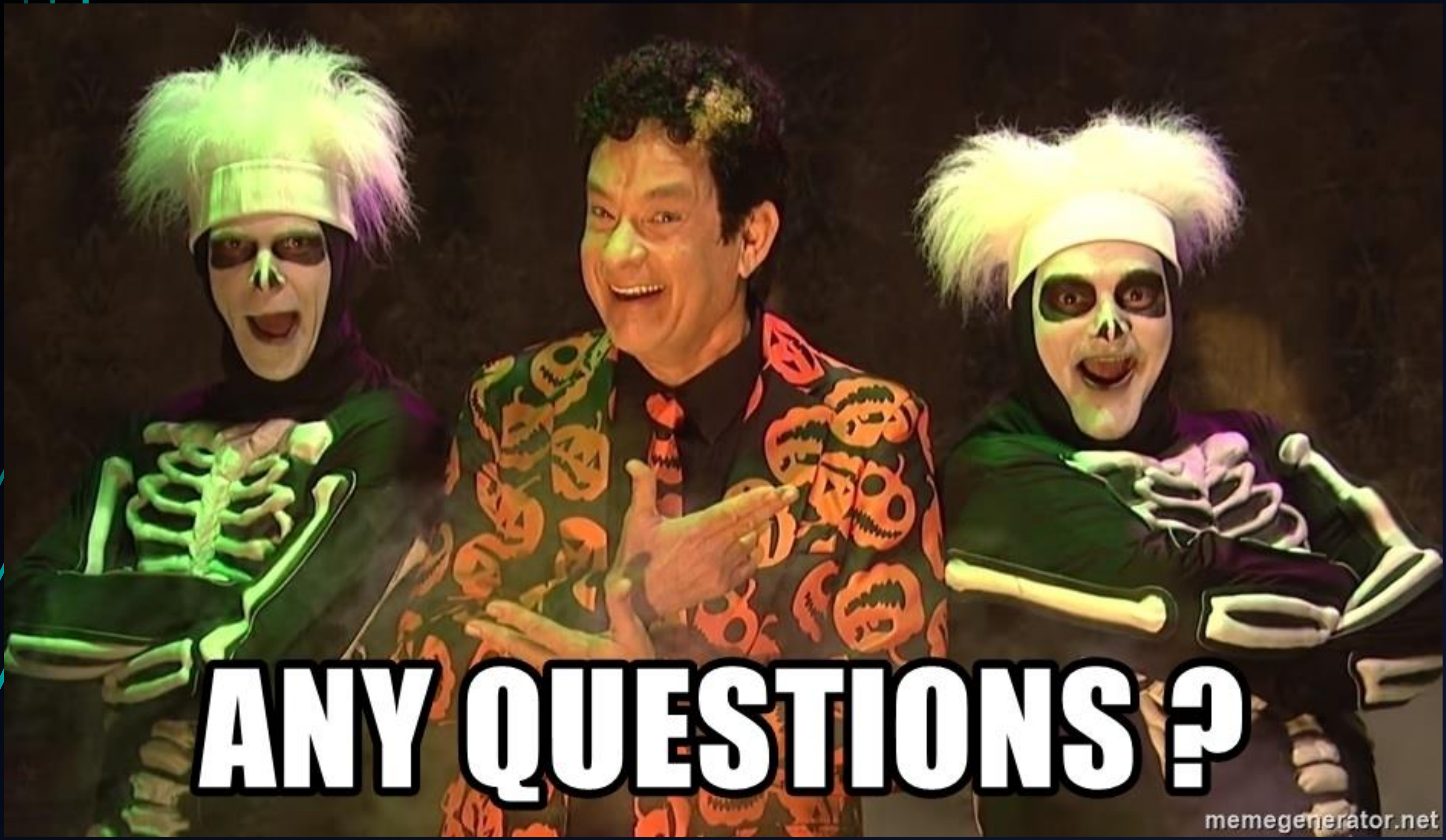
Alice and Bob will then publicly compare n of their key bits. The probability of finding mis-matched bits and the eavesdropper is

$$P = 1 - (\frac{3}{4})^n$$

So, to detect an eavesdropper with probability 99.9999999%, Alice and Bob would only need to compare **72** bits.

The Steps

- Alice sends a bunch of qubits
  - Random bits with random polarizations
- Bob measures the qubits
  - With either rectilinear (+) or diagonal (X) basis
- Bob and Alice find out which qubits were measured correctly by publicly comparing each others' basiseseses
  - The bits with matching basis become the key
- They publicly compare a set of those bits
  - if they match, the remaining bits become the key
  - If they don't match, there may have been an eavesdropper. So they start all over again.



ANY QUESTIONS ?
memegenerator.net