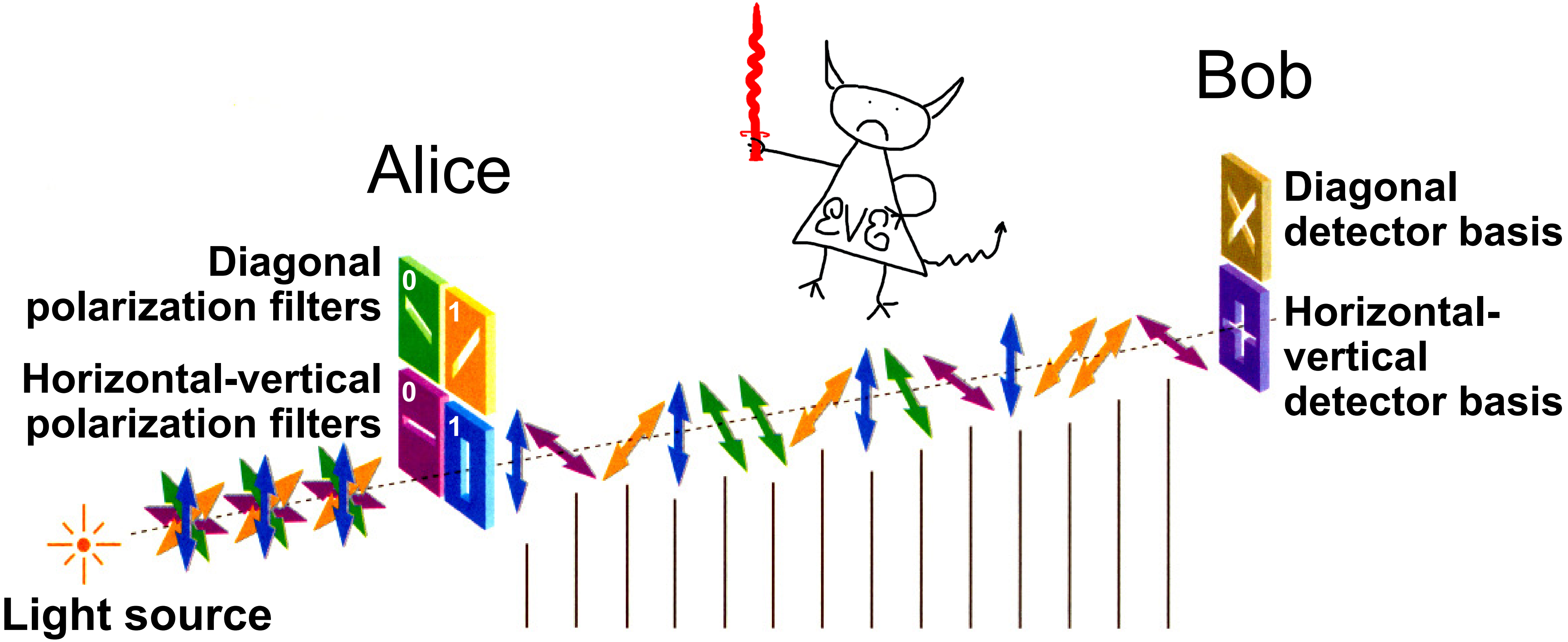
Bennett-Brassard 1984 (BB84) QKD protocol



Alice

Diagonal polarization filters

Horizontal-vertical polarization filters

Light source

Bob

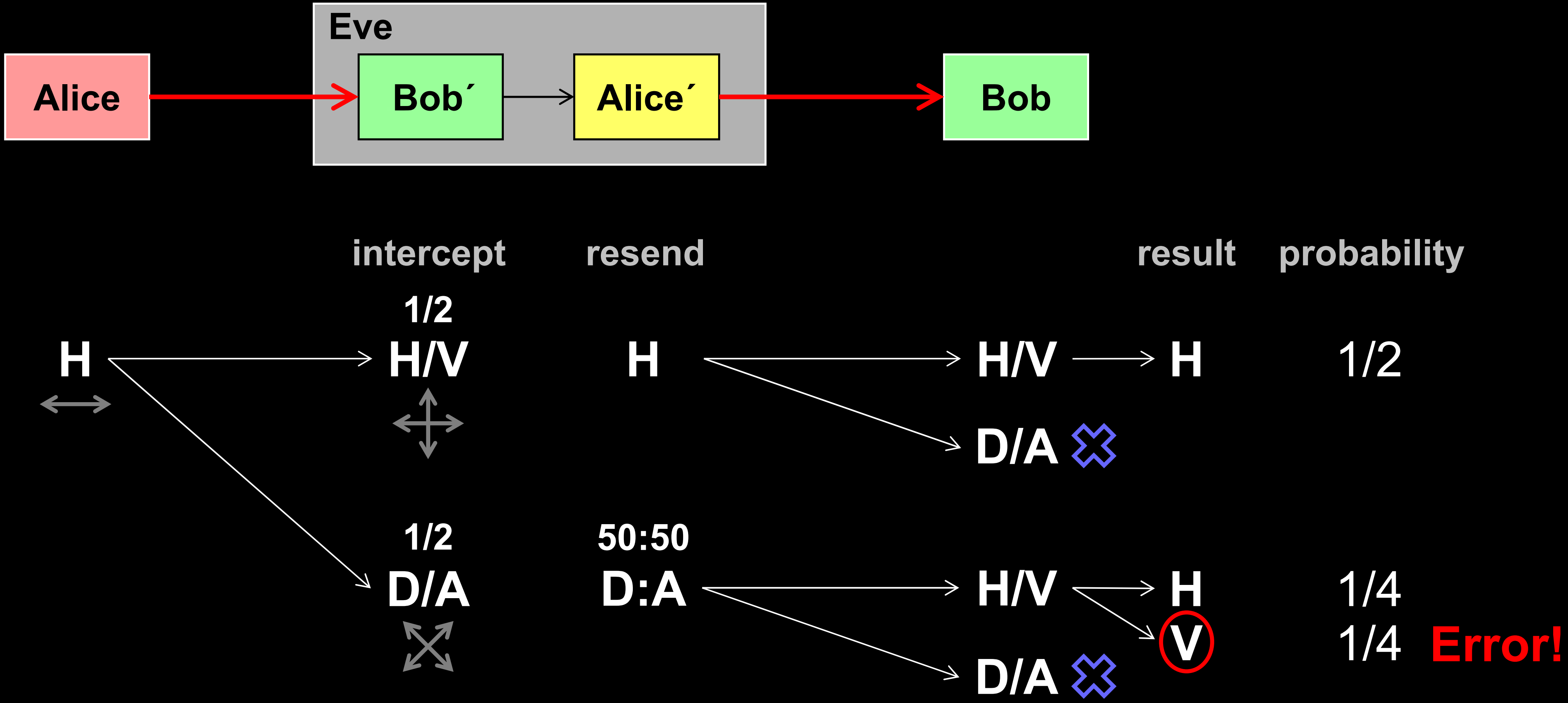
Diagonal detector basis

Horizontal-vertical detector basis

Alice’s bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob’s detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob’s measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

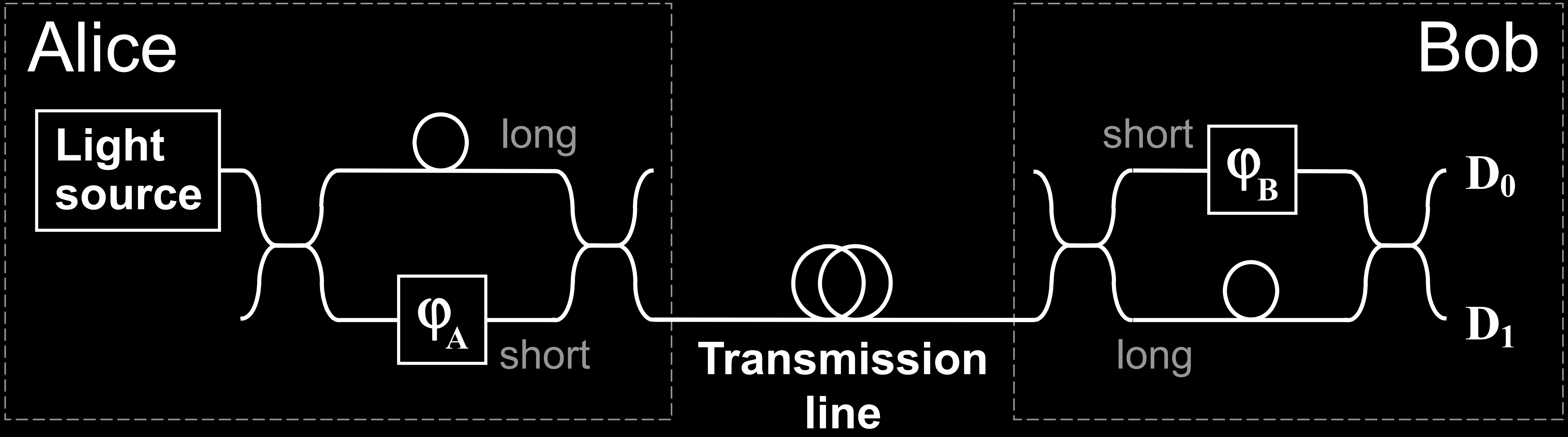
Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, “Quantum cryptography,” Physics World, March 1998

Intercept-resend attack



C. H. Bennett, G. Brassard, in *Proc. Intl. Conf. on Computers, Systems, and Signal Processing (Bangalore, India)*, p. 175 (1984)

Phase (time-bin) encoding, interferometric QKD channel



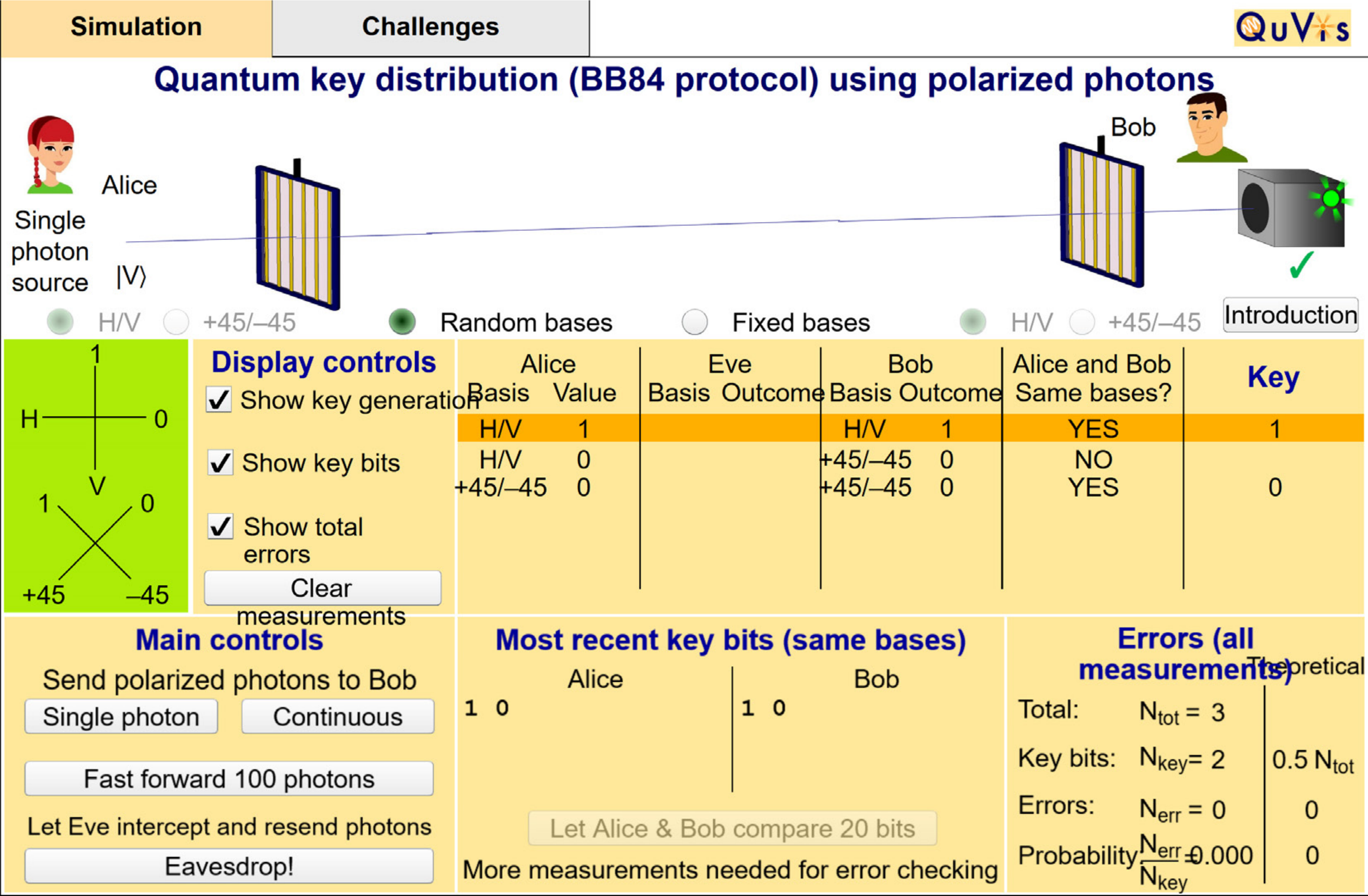
Detection basis:

$\varphi_A =$ 0 or $\pi/2$: 0

π or $3\pi/2$: 1

$\varphi_B =$ 0 : X

$\pi/2$: Z



Quantum key distribution (BB84 protocol) using polarized photons

● H/V ○ +45/–45 ● Random bases ○ Fixed bases ● H/V ○ +45/–45

Display controls

☑ Show key generation

☑ Show key bits

☑ Show total errors

Clear measurements

Alice		Eve		Bob		Alice and Bob	Key
Basis	Value	Basis	Outcome	Basis	Outcome	Same bases?	
H/V	1			H/V	1	YES	1
H/V	0			+45/–45	0	NO	
+45/–45	0			+45/–45	0	YES	0

Main controls

Send polarized photons to Bob

Single photon | Continuous

Fast forward 100 photons

Let Eve intercept and resend photons

Eavesdrop!

Most recent key bits (same bases)

Alice	Bob
1 0	1 0

Let Alice & Bob compare 20 bits

More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	$N_{tot} = 3$	
Key bits:	$N_{key} = 2$	$0.5\ N_{tot}$
Errors:	$N_{err} = 0$	0
Probability	$\frac{N_{err}}{N_{key}} = 0.000$	0

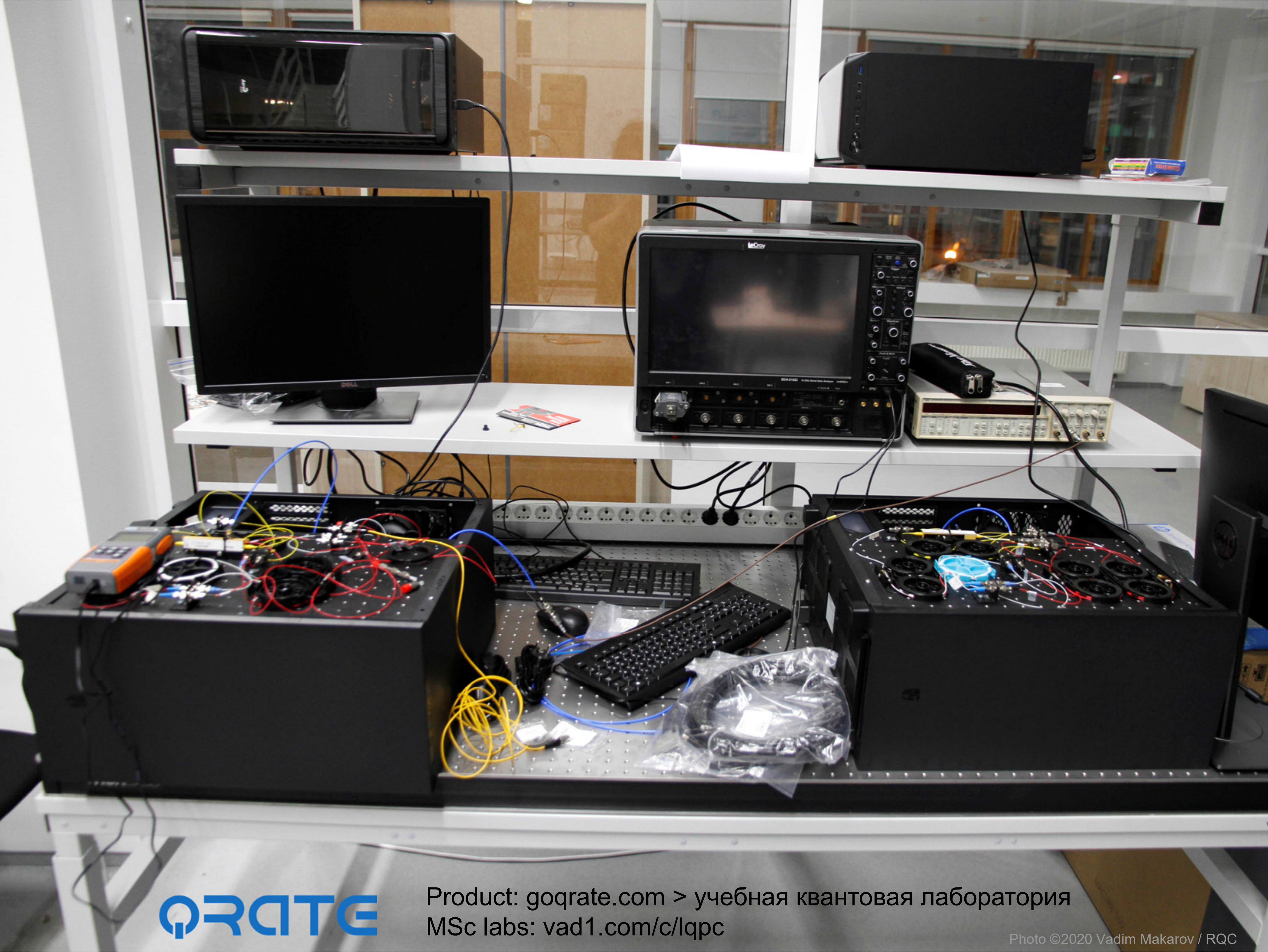
https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/BB84_photons/BB84_photons.html

Discovery

EDU-QCRY1
EDU-QCRY1/M
Quantum Cryptography Demonstration Kit

Manual

Photo ©2020 Vadim Makarov / RQC



Product: goqrate.com > учебная квантовая лаборатория
MSc labs: vad1.com/c/lqpc

Photo ©2020 Vadim Makarov / RQC

Twin-field QKD protocol

M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, Nature **557**, 400 (2018)

Twin-field *sending-or-not-sending* QKD protocol

X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A **98**, 062323 (2018)

Current distance record ~1000 km in fiber

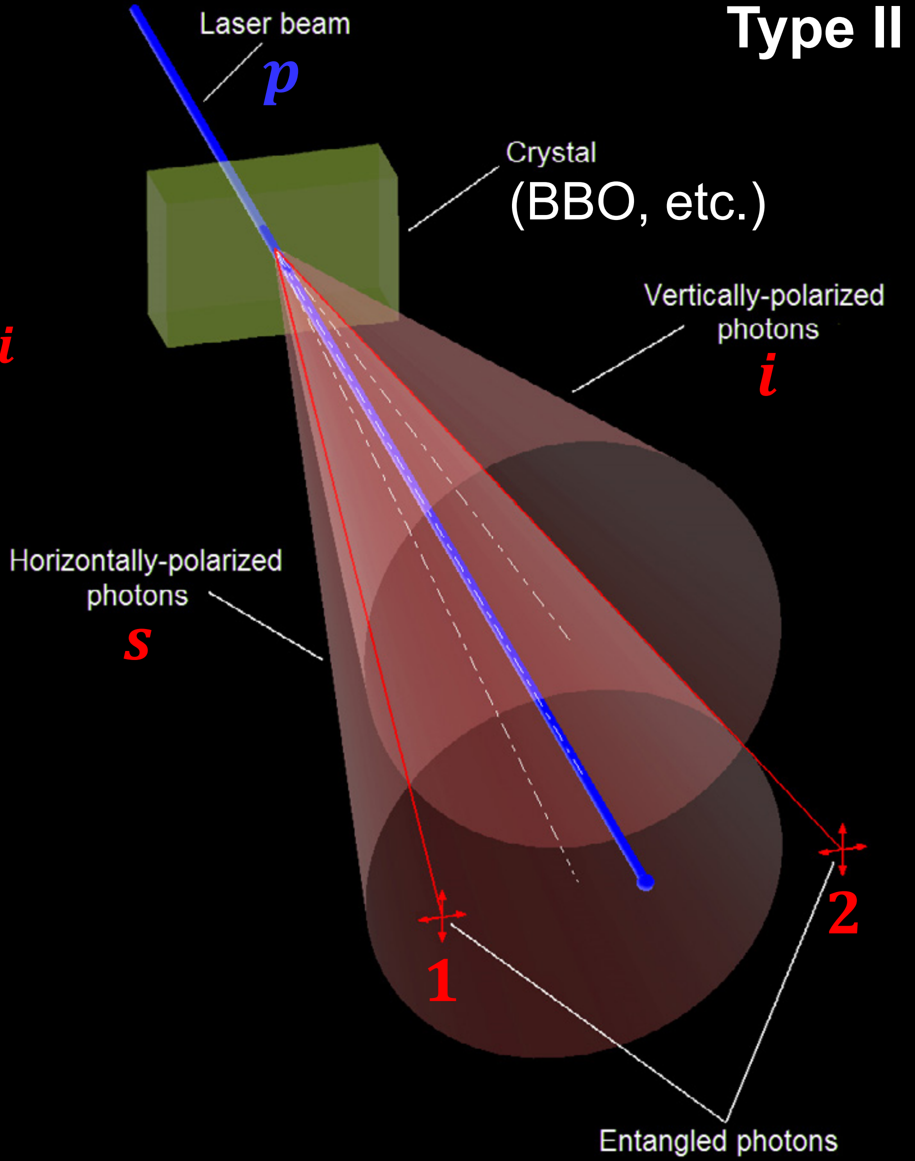
Y. Liu *et al.*, Phys. Rev. Lett. **130**, 210801 (2023)

Spontaneous parametric down-conversion

Type II

Energy conservation: $\omega_p = \omega_s + \omega_i$

Momentum conservation: $\vec{k}_p = \vec{k}_s + \vec{k}_i$

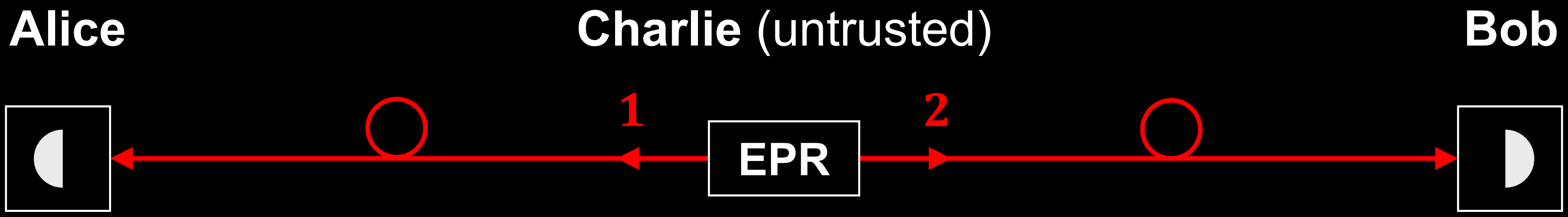


$$\begin{aligned}|\psi\rangle &= (|H_1, V_2\rangle + |V_1, H_2\rangle)/\sqrt{2}\\ &= (|D_1, A_2\rangle + |A_1, D_2\rangle)/\sqrt{2}\end{aligned}$$

P. G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)

Image reprinted from: Wikipedia

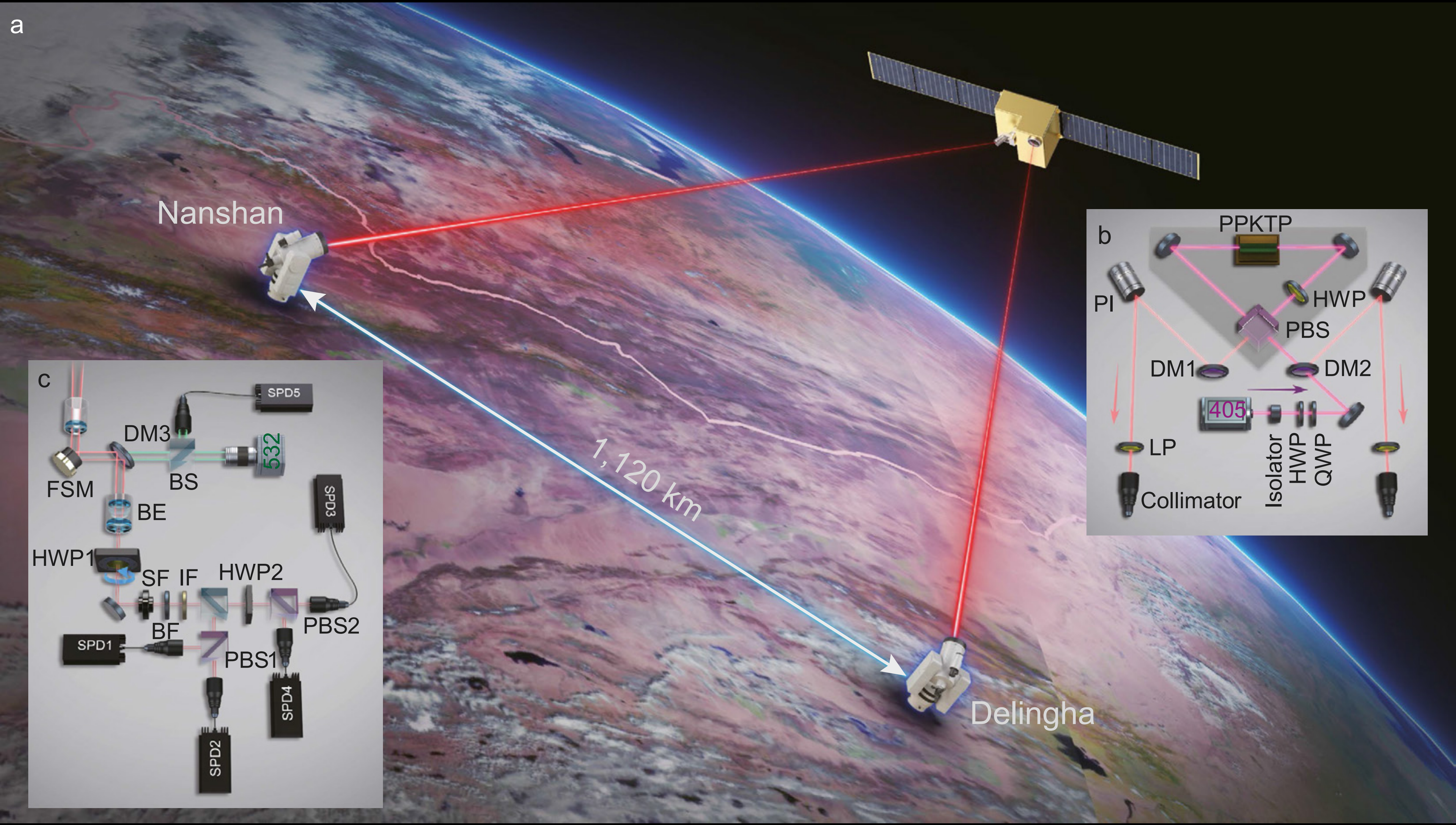
Entangled-pair QKD



$$|\psi\rangle = (|H_1, V_2\rangle + |V_1, H_2\rangle)/\sqrt{2}$$
$$= (|D_1, A_2\rangle + |A_1, D_2\rangle)/\sqrt{2}$$

A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)

Entangled-pair QKD over 1120 km



J. Yin *et al.*, Nature **582**, 501 (2020)

Quantum repeater network

1. **Entanglement swapping**

2. **Quantum memory**

3. **Error correction (entanglement distillation)**

H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998)