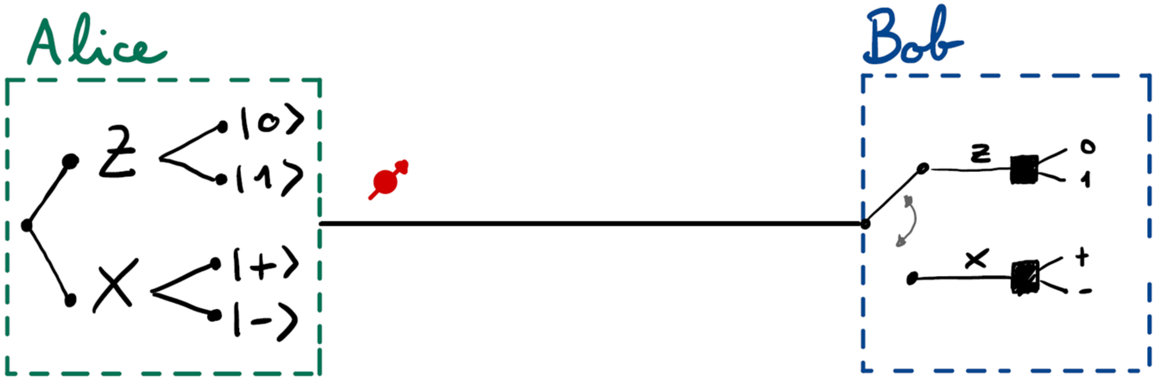
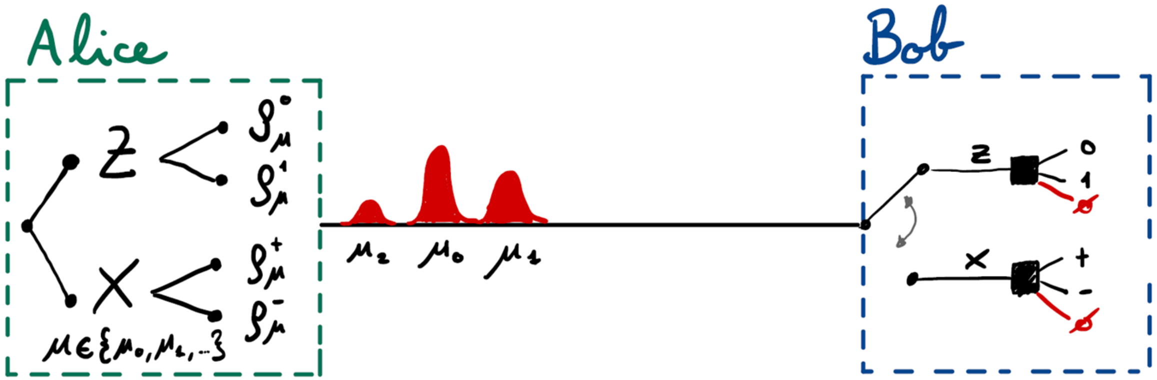




Practical implementations of Quantum Key Distribution

- Rusca Davide

- VQCC
- Summer School – 04/07/24

$$\| \rho_{R_2 E} - \rho_U \otimes \rho_E \|_1 < \varepsilon$$

atlanTTic Universida de Vigo

Financiado por la Unión Europea NextGenerationEU

Gobierno de España – Ministerio de Educación y Ciencia

Plan de Recuperación, Transformación y Resiliencia

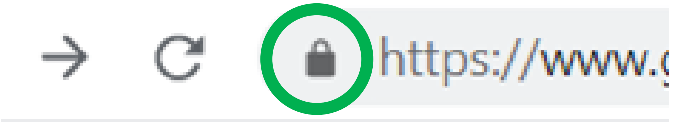
Axencia Galega de Innovación

Content

- **Introduction**
  - **What is cryptography?**
  - **What is Quantum Cryptography?**
- Single Photon Prepare and Measure QKD
- Coherent states QKD
- Implementation a simplified DS-BB84
- Implementation security of QKD
- Measurement device independent QKD

Cryptography

- Asymmetric key encryption (RSA, elliptic curves, discrete logarithms):
  - Easy to implement.
  - Only computational secure:



One Time Pad

Ciphertext $\mathbf{C} = \mathbf{M} \oplus \mathbf{K} = [1, 0, 0, 1, \dots, 1]$

Plaintext $\mathbf{M} = [0, 1, 0, 0, \dots, 1]$

Key $\mathbf{K} = [1, 1, 0, 1, \dots, 0]$

Key $\mathbf{K} = [1, 1, 0, 1, \dots, 0]$

Plaintext $\mathbf{M} = \mathbf{C} \oplus \mathbf{K} = [0, 1, 0, 0, \dots, 1]$

- Symmetric key encryption (One Time Pad)
  - Information theoretically secure

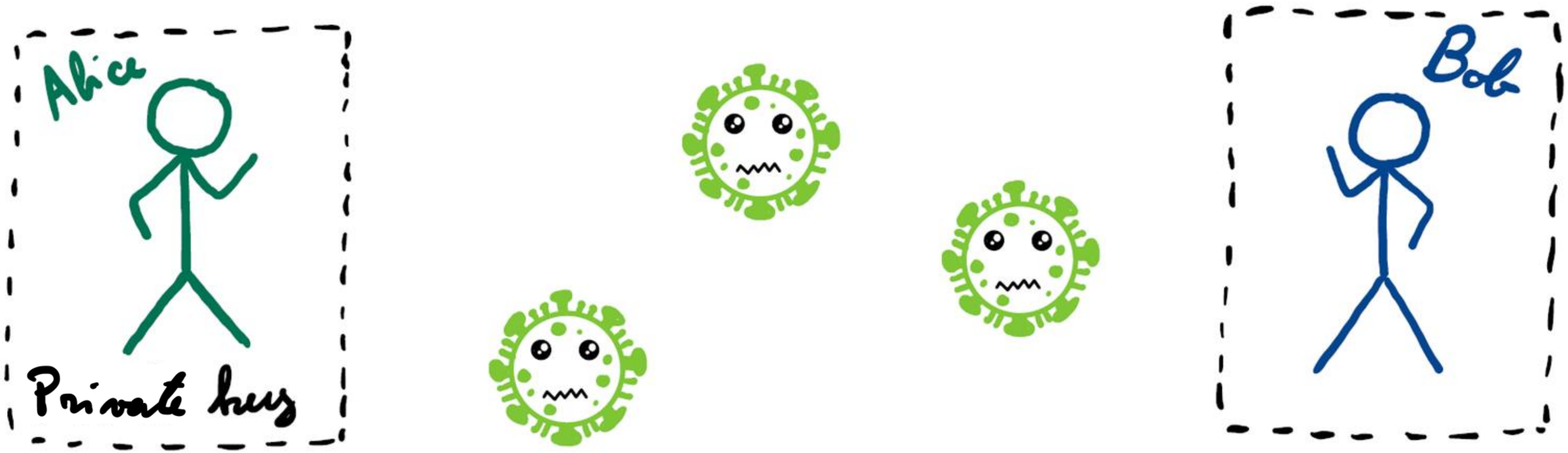
One Time Pad Requirements

- The two honest parties must share a key.

- The generated key must be completely private and random.

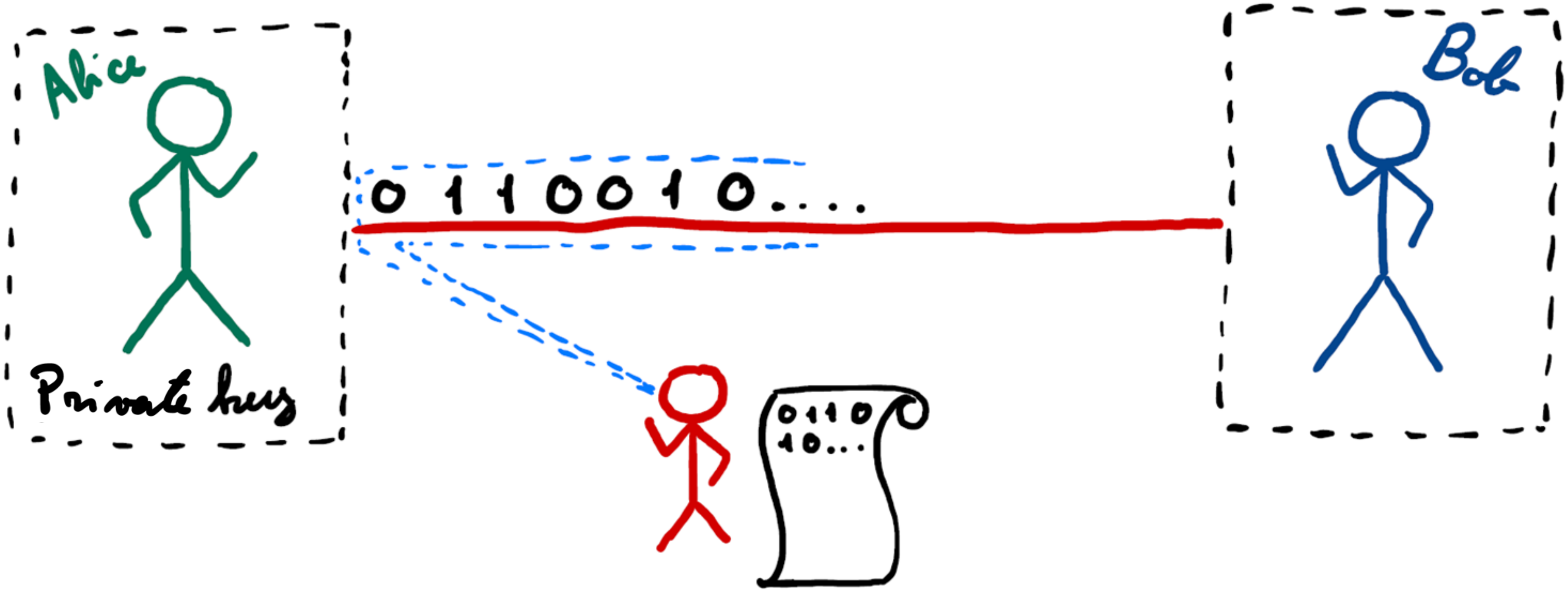
One Time Pad Requirements

- The two honest parties must share a key.
- The generated key must be completely private and random.

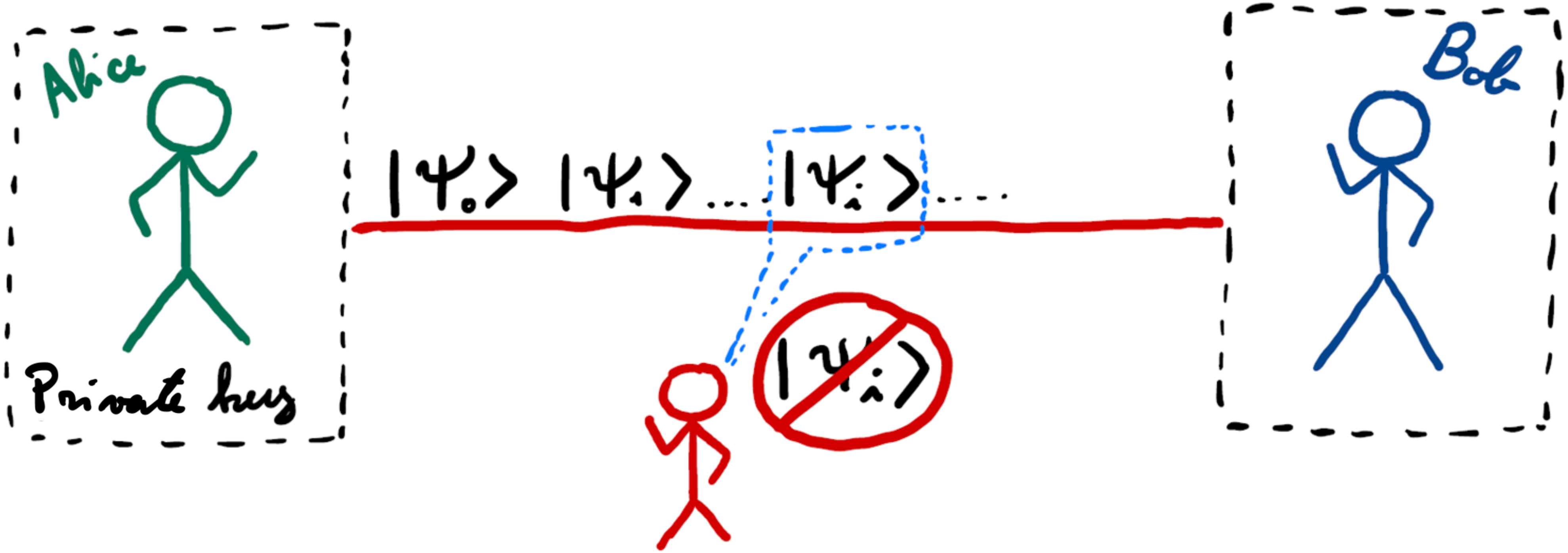


One Time Pad Requirements

- The two honest parties must share a key.
- The generated key must be completely private and random.

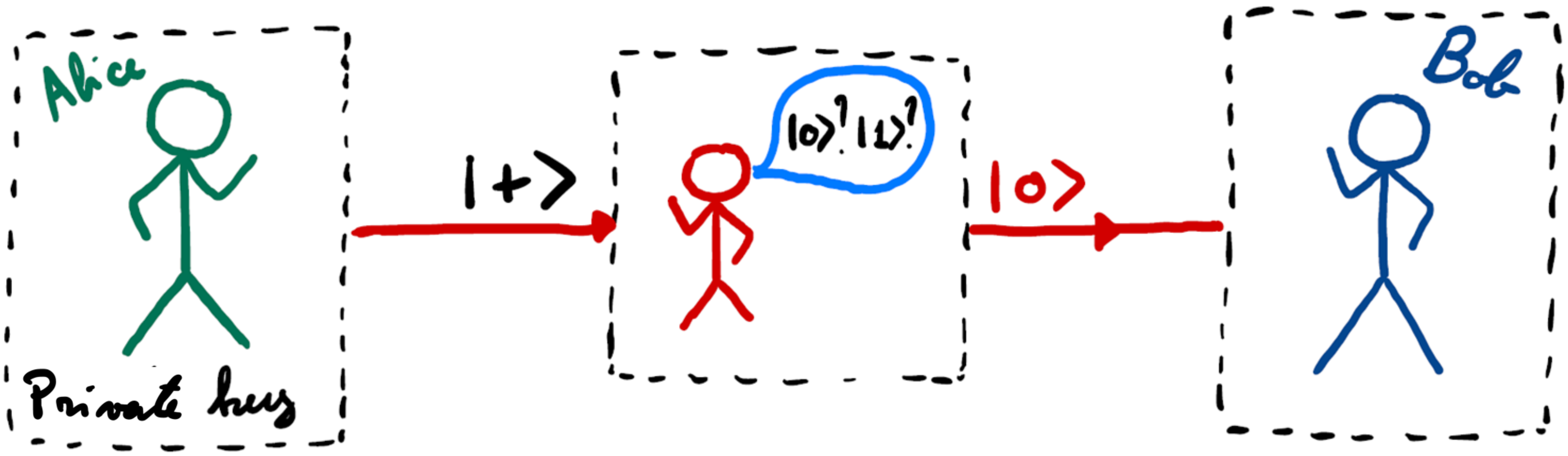


Quantum Mechanics



Quantum States cannot be copied deterministically.

Quantum Mechanics



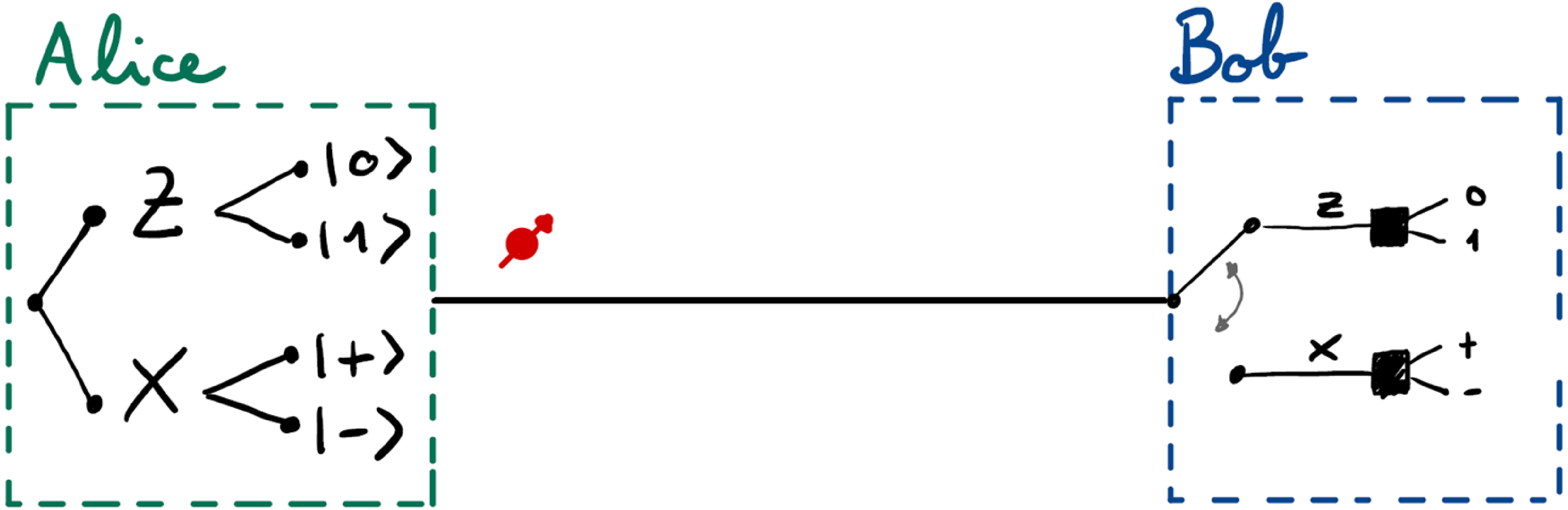
A measurement can be incompatible with the state prepared.

The result of such measurement is intrinsically probabilistic.

Content

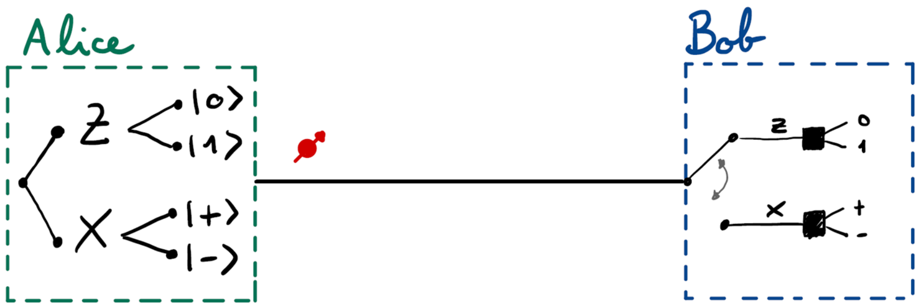
- Introduction
- **Single Photon Prepare and Measure QKD**
  - **BB84 protocol**
  - **Assumptions of QKD**
  - **Correctness and secrecy of QKD**
  - **Performance of Single Photon BB84**
- Coherent states QKD
- Implementation a simplified DS-BB84
- Implementation security of QKD
- Measurement device independent QKD

Single Photon BB84 Protocol

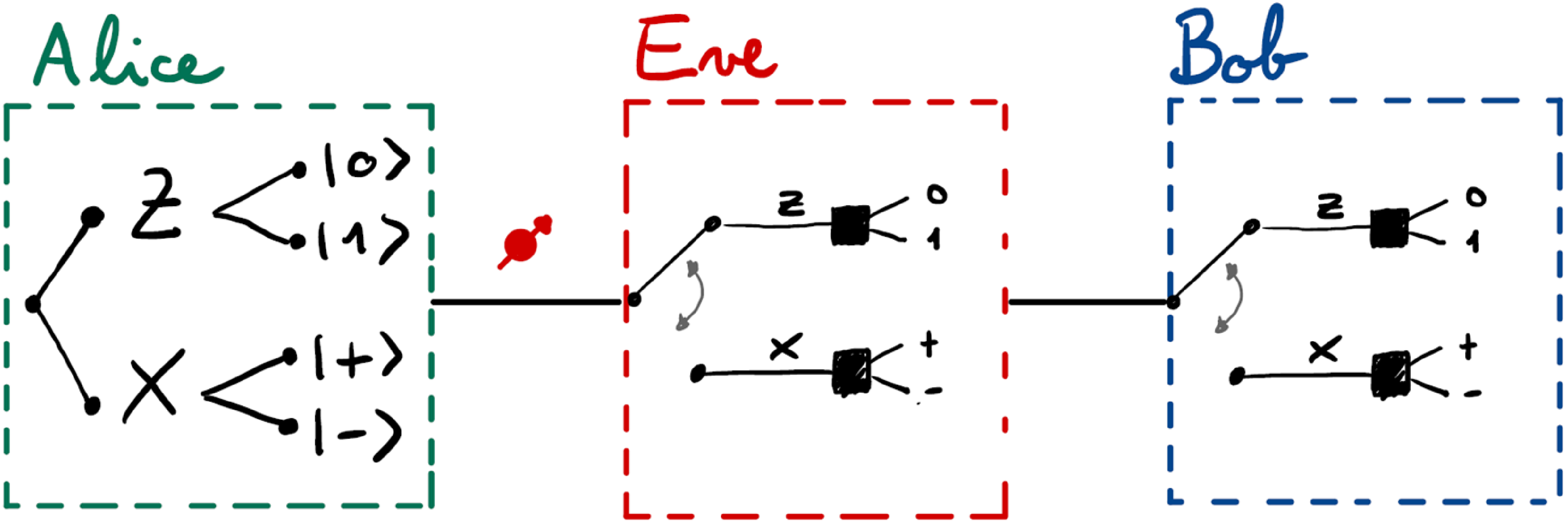


Single Photon BB84 Protocol

Bob \ Alice		Z: $\|0\rangle$	Z: $\|1\rangle$	X: $\|+\rangle$	X: $\|-\rangle$
Z	$\|0\rangle$	1	0	1/2	1/2
Z	$\|1\rangle$	0	1	1/2	1/2
X	$\|+\rangle$	1/2	1/2	1	0
X	$\|-\rangle$	1/2	1/2	0	1

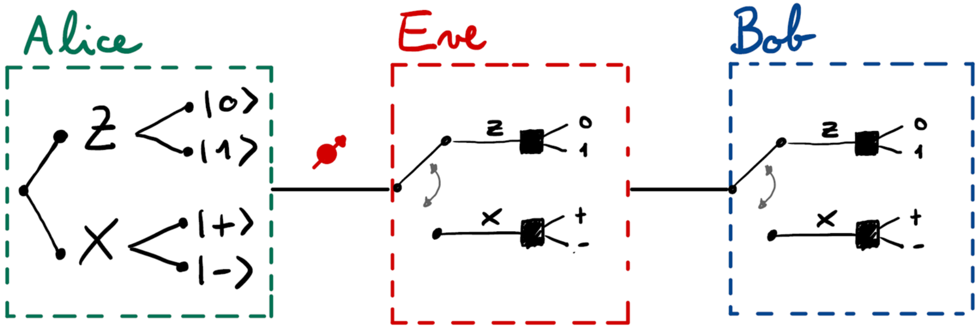


Intercept and Resend attack



Intercept and Resend attack

		Alice Z: $\|0\rangle$	Alice Z: $\|1\rangle$	Alice X: $\|+\rangle$	Alice X: $\|-\rangle$
Bob Z	$\|0\rangle$	3/4	1/4	1/2	1/2
Bob Z	$\|1\rangle$	1/4	3/4	1/2	1/2
Bob X	$\|+\rangle$	1/2	1/2	3/4	1/4
Bob X	$\|-\rangle$	1/2	1/2	1/4	3/4

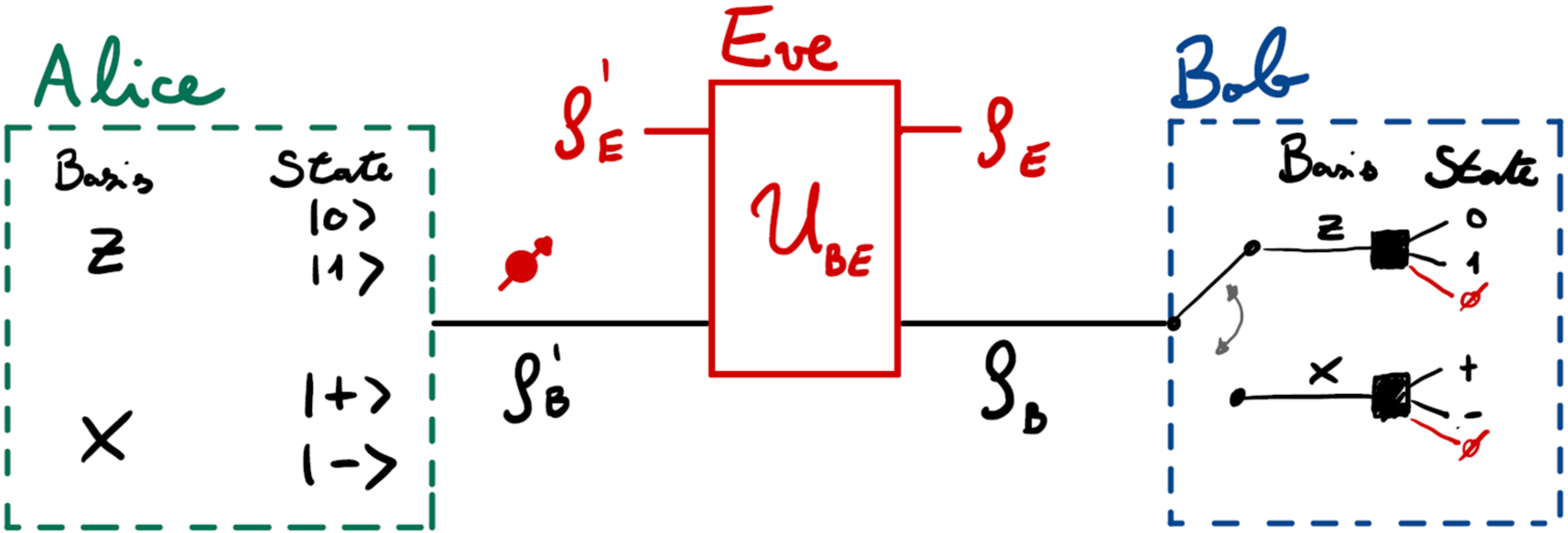


Alice and Bob can recognize that the communication has been intercepted.

Assumptions in QKD

- Quantum theory is correct and complete.
- Authentic communication is possible.
- Isolation of Alice’s and Bob’s labs.
- The state prepared and the measurement are characterized. (Device-dependent QKD)

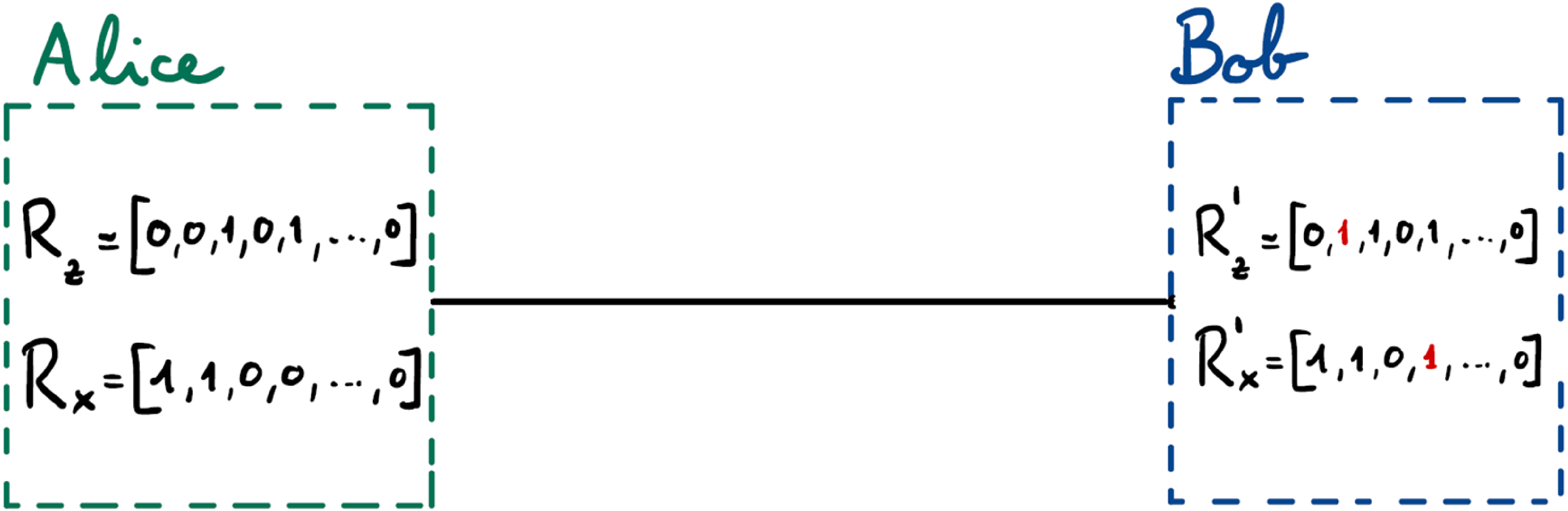
Quantum Phase



Types of attacks

- Individual attack: Eve’s attack is i.i.d. on all signal. They wait for the postprocessing phase to measure but the measurement is done on each ancilla independently
- Collective attack: Eve’s attack is still i.i.d. but all ancillas can be measured collectively.
- Coherent attack: Eve can attack all states at the same time if available. The ancilla can be measured collectively.

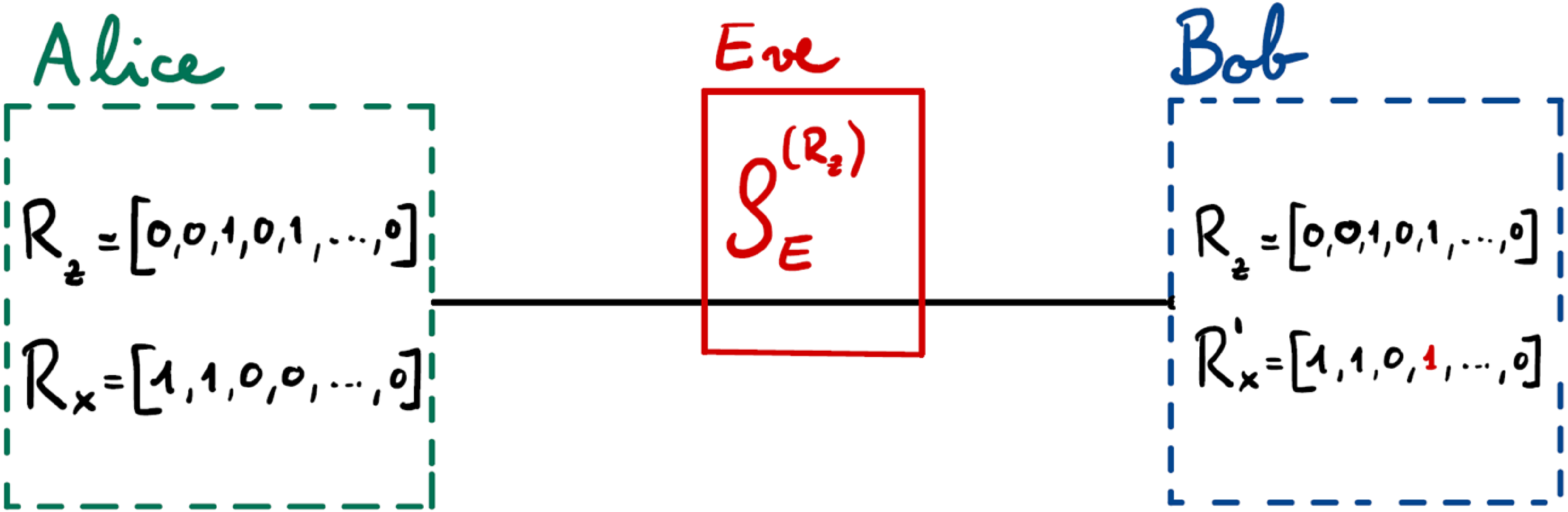
Error Correction



$$P\left(R_z^A \neq R_z^B\right) \leq \varepsilon_{corr}$$

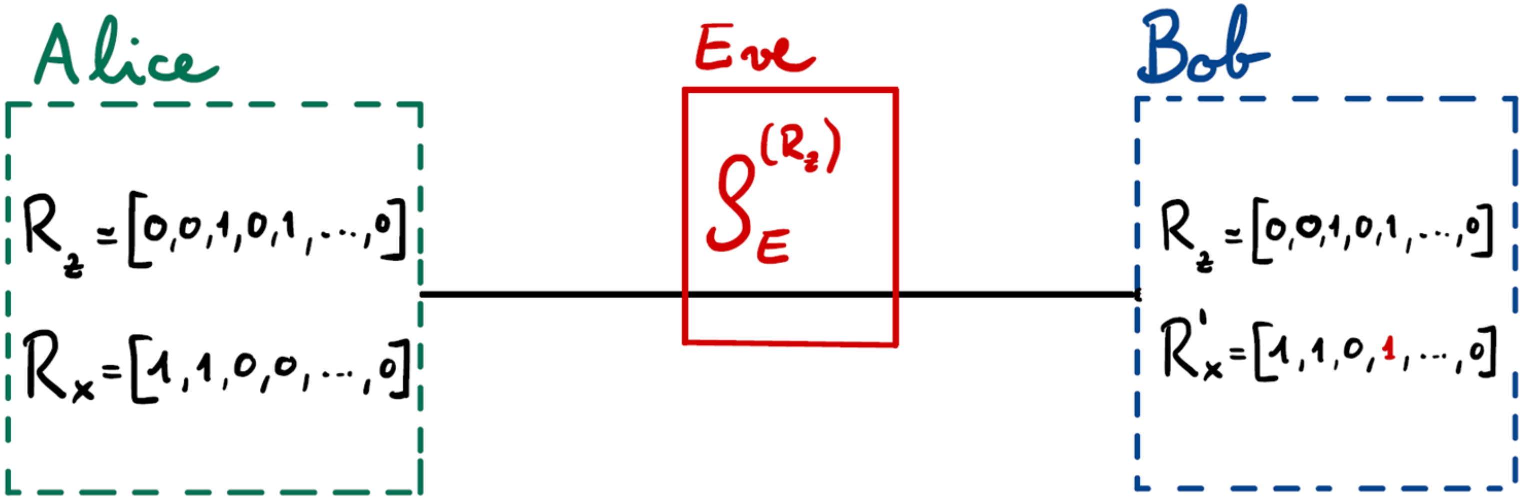
$$\delta_{leak} \geq n H(Z|Z') = n\, h(e_z)$$

Privacy Amplification



$$\rho_{R_z E} = \sum_{R_z} p(R_z)\, |R_z\rangle\langle R_z| \otimes \rho_E^{(R_z)}$$

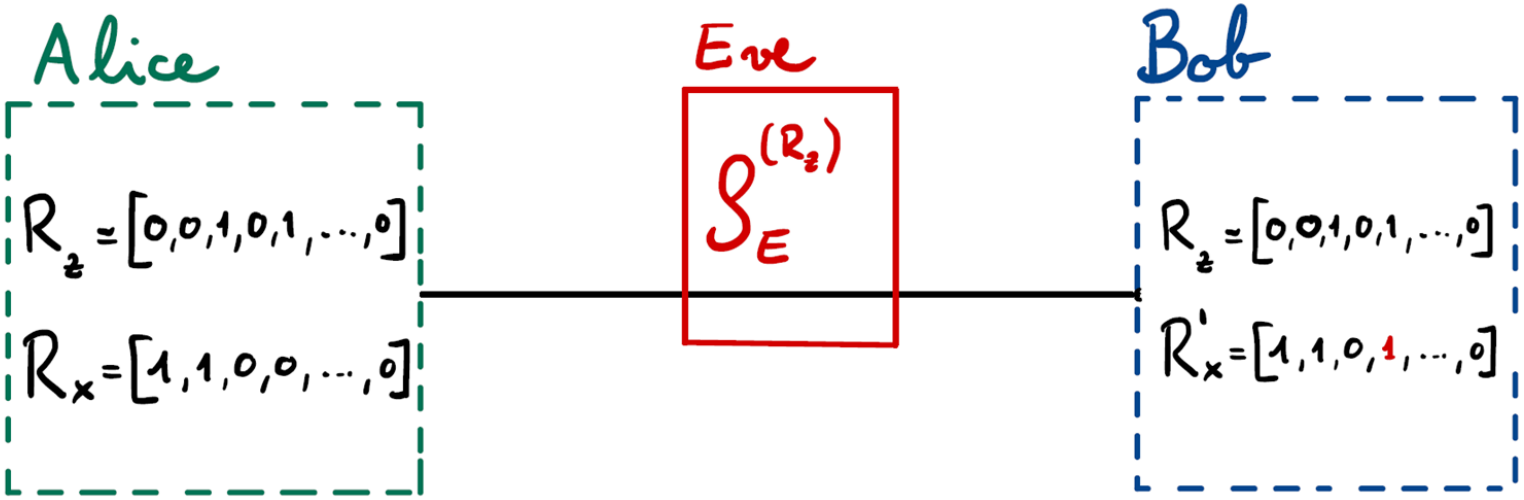
Privacy Amplification



$$P_{guess} = \max_{\{M^E\}} \sum_{R_z} p(R_z)\, \mathrm{Tr}\left(M^E \rho_E^{(R_z)}\right)$$

$$H_{min}(\rho_{R_z E} | E) = -\log_2 P_{guess}$$

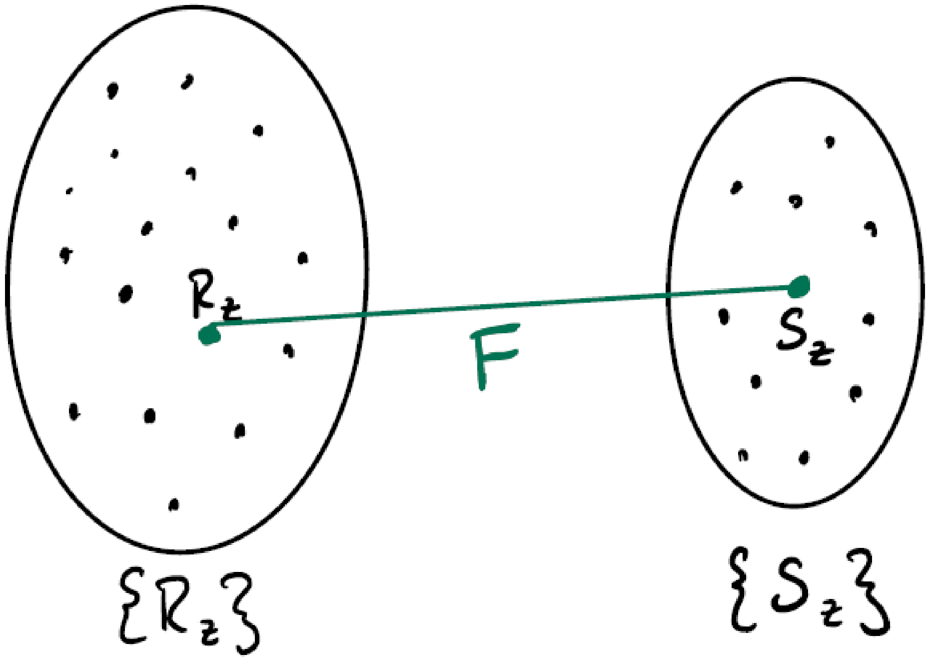
Privacy Amplification



$$\| \rho_{R_z E} - \rho_U \otimes \rho_E \|_1 < \varepsilon$$

$$F(R_z) = S_K \qquad |R_z| > |S_K| = \ell$$

Privacy Amplification



$$\ell \leq H_{min}(\rho_{R_Z E}|E) - \delta_{leak}$$

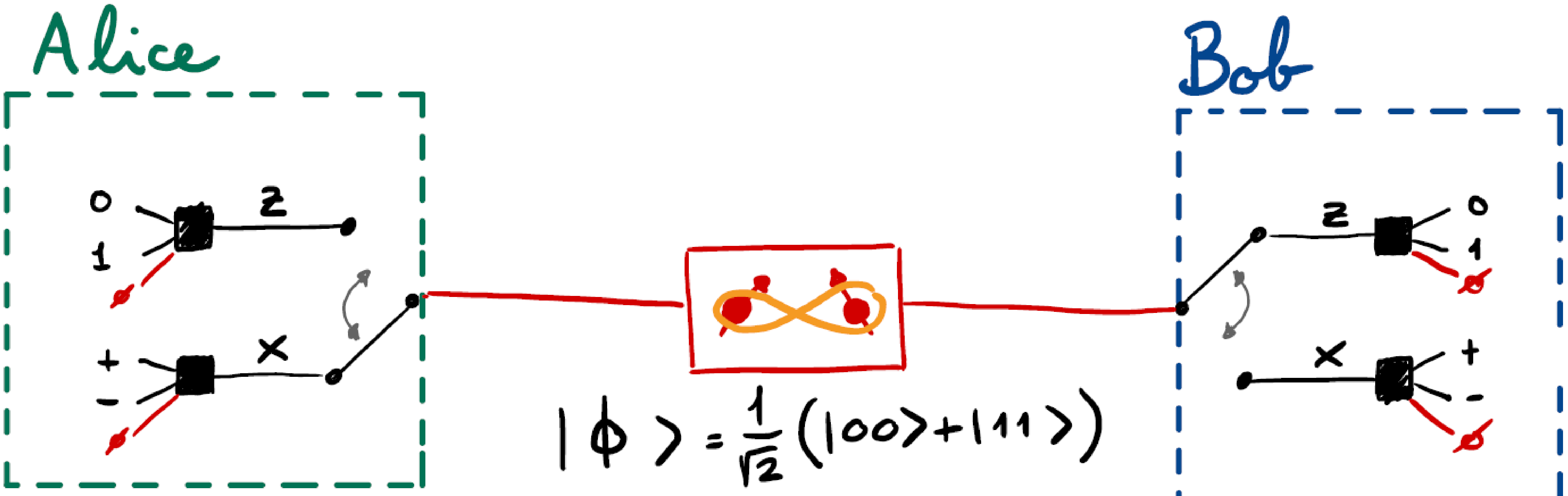
$$\ell \leq n(1 - h(e_z) - h(e_x))$$

F is a function taken from a family of 2-universal hash functions.

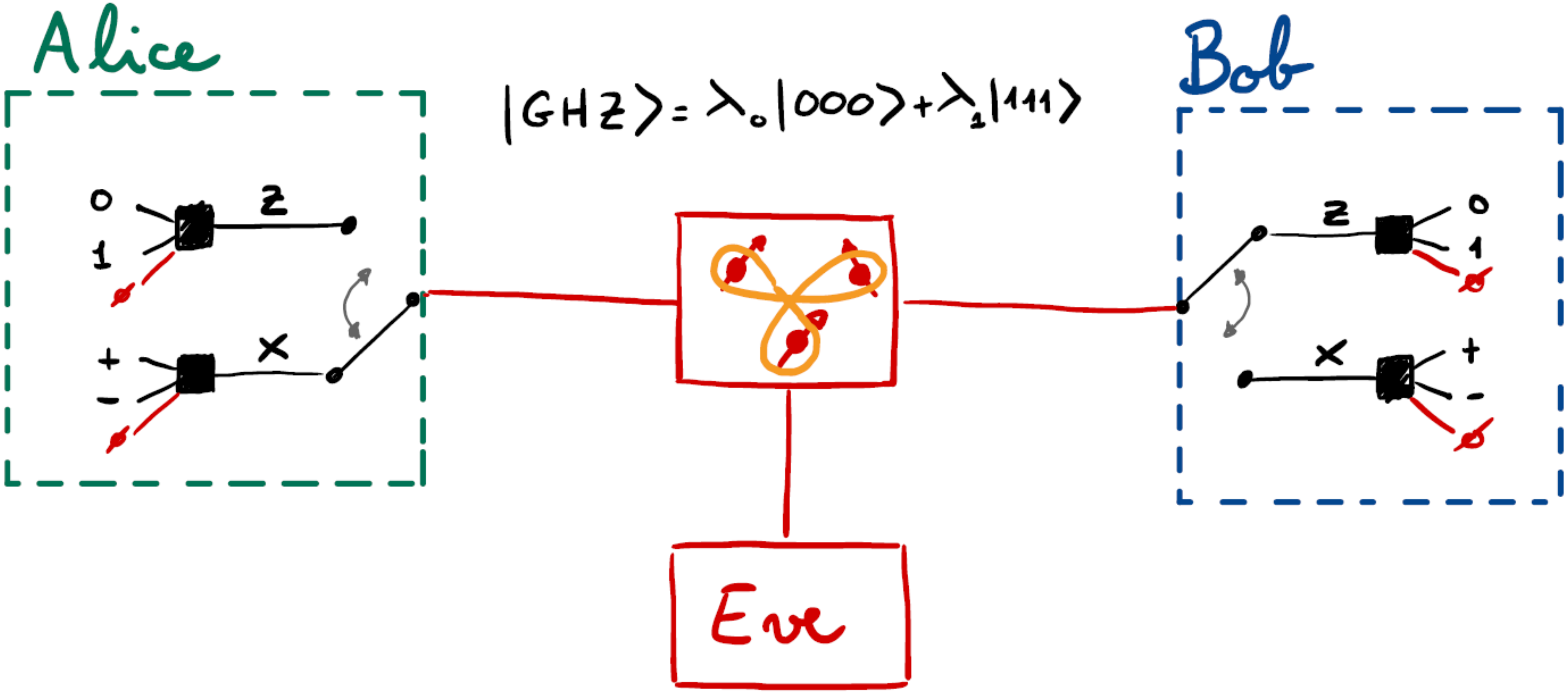
Implementation of a QKD protocol

- Prepare and measure vs Entanglement based.
- Discrete variable vs Continuous variable.
- Device dependent vs Device independent.
- Fiber link vs Free space link.

Entanglement based QKD



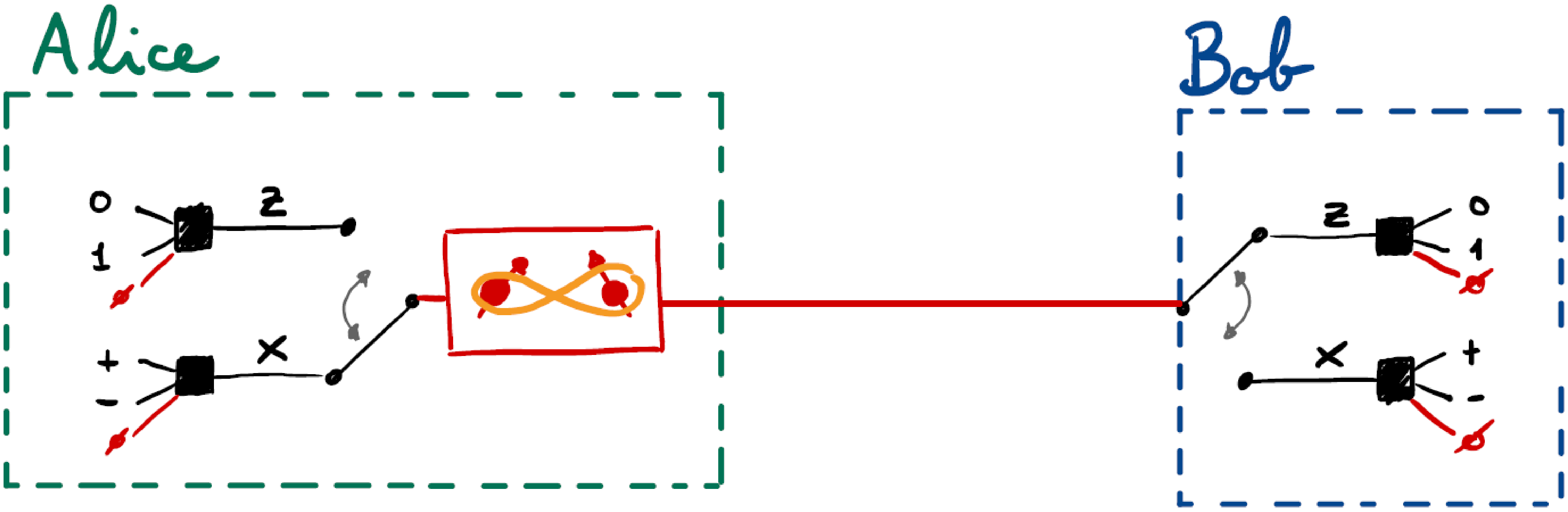
EB QKD: monogamy of entanglement



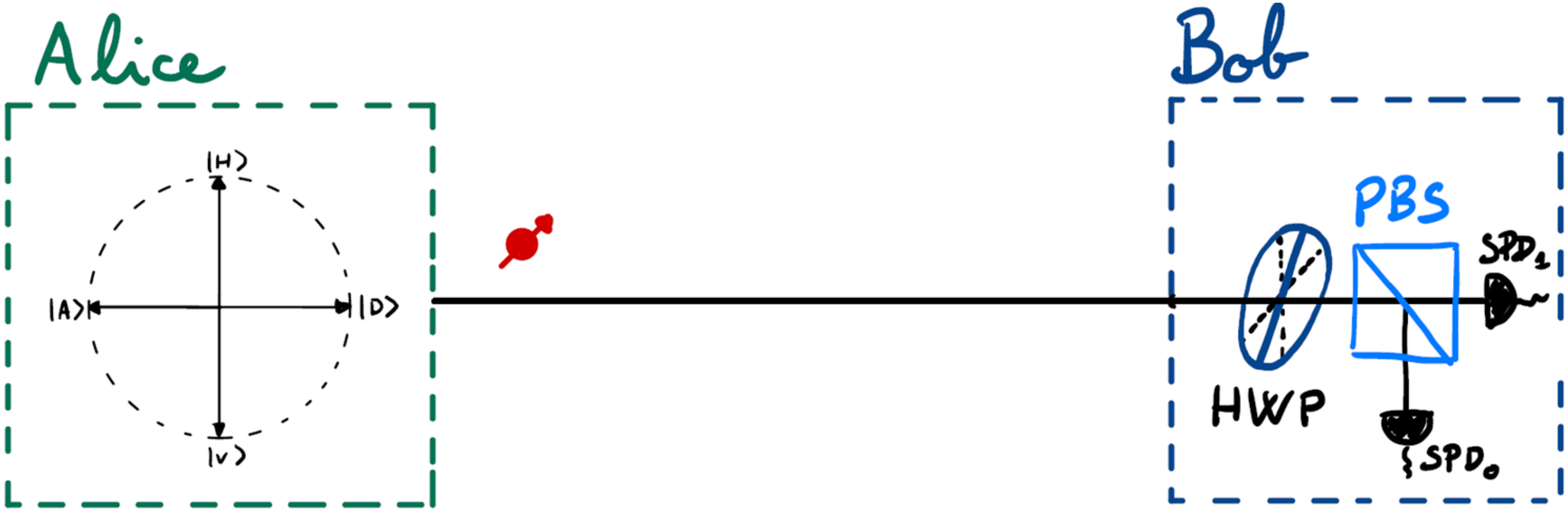
This is NOT equivalent to the previous scheme.

This property is known as monogamy of entanglement.

EB QKD = PM QKD

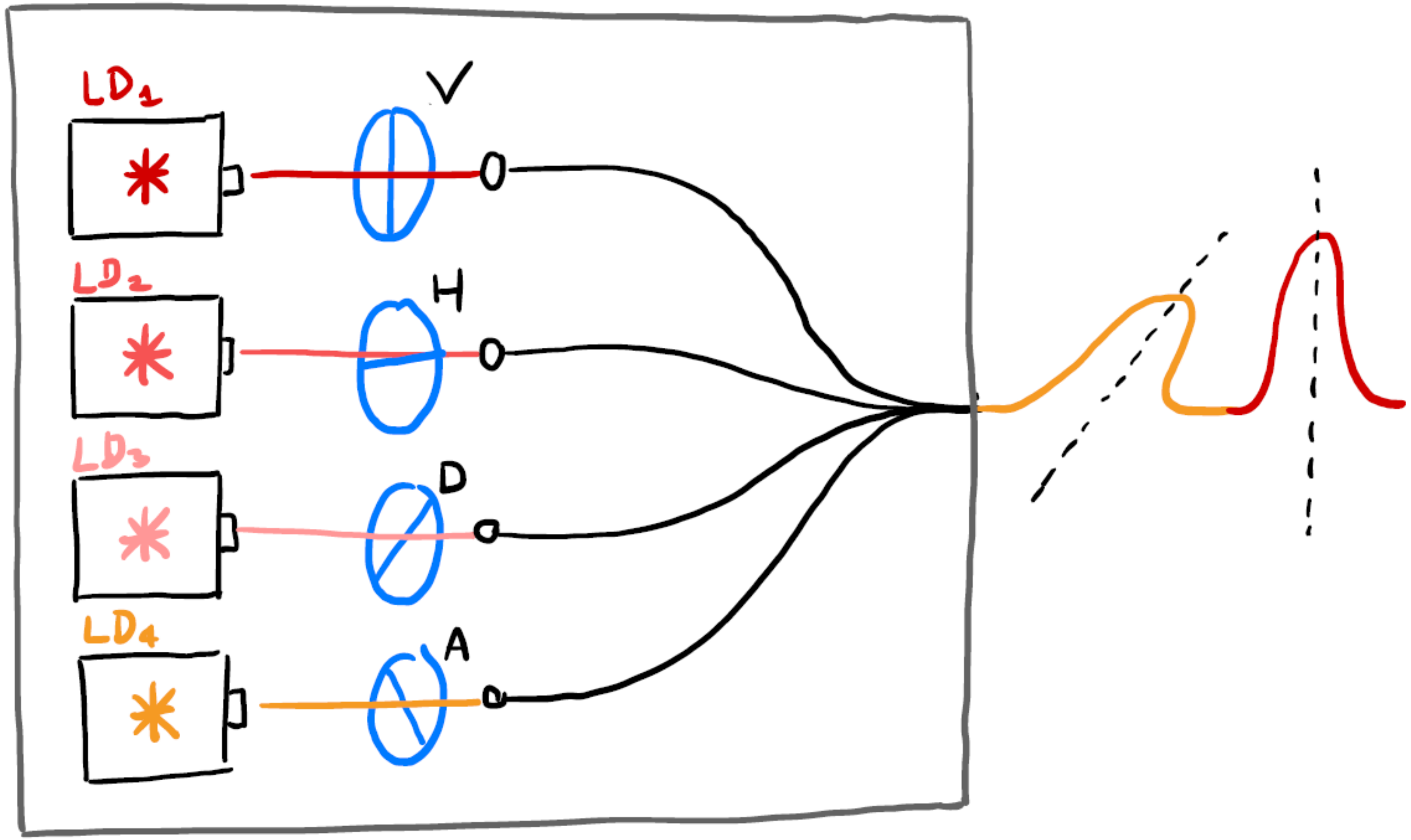


PM QKD: Polarization encoding

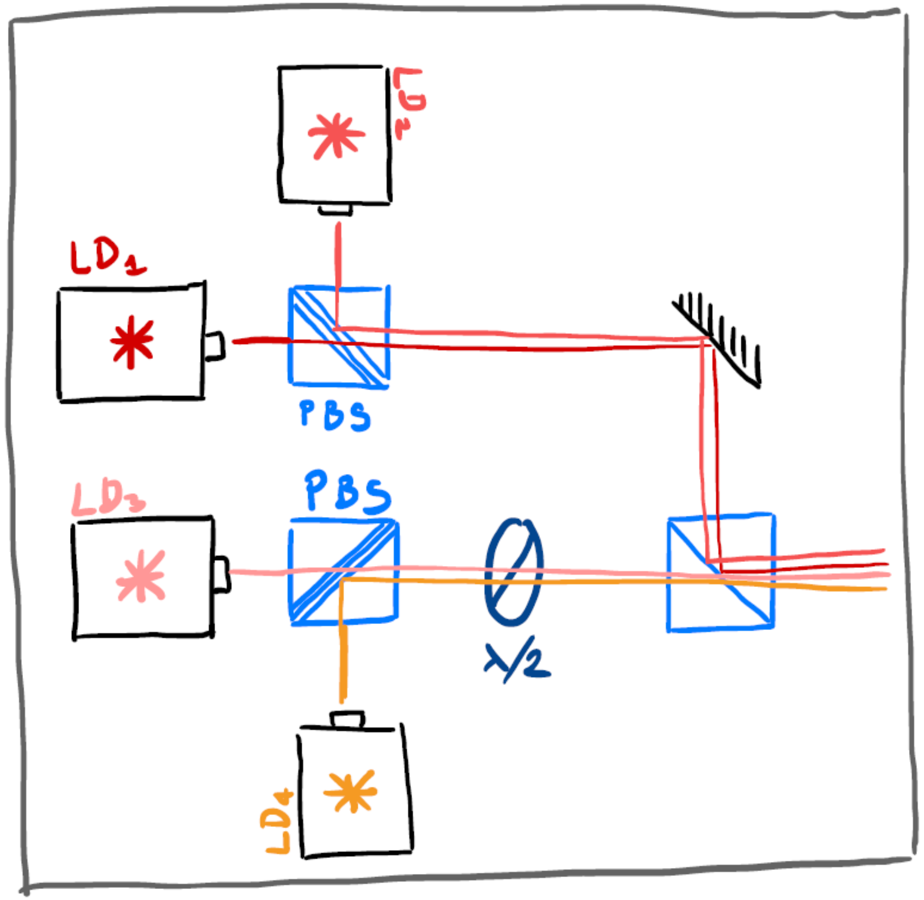


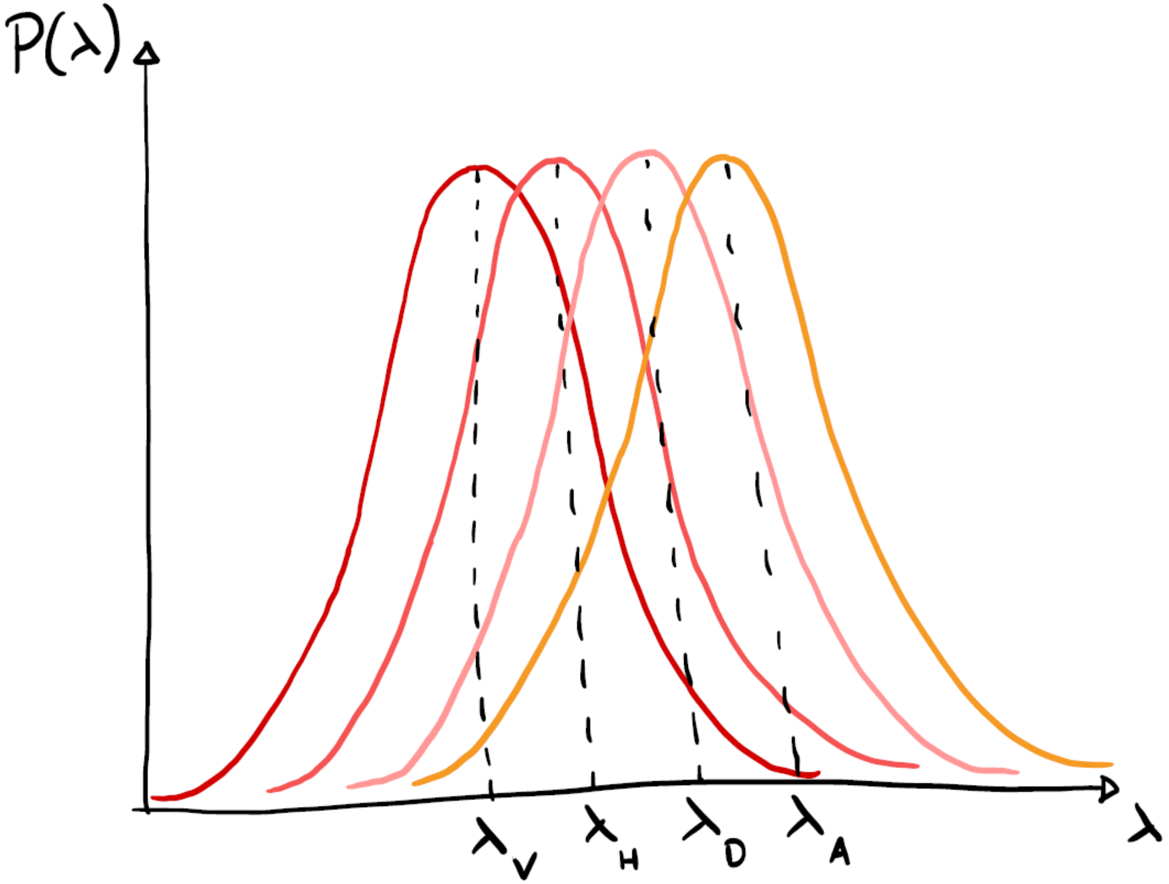
Used mostly in free space communication.
In fiber requires an active tracking of the polarization.

PM QKD: Polarization encoding

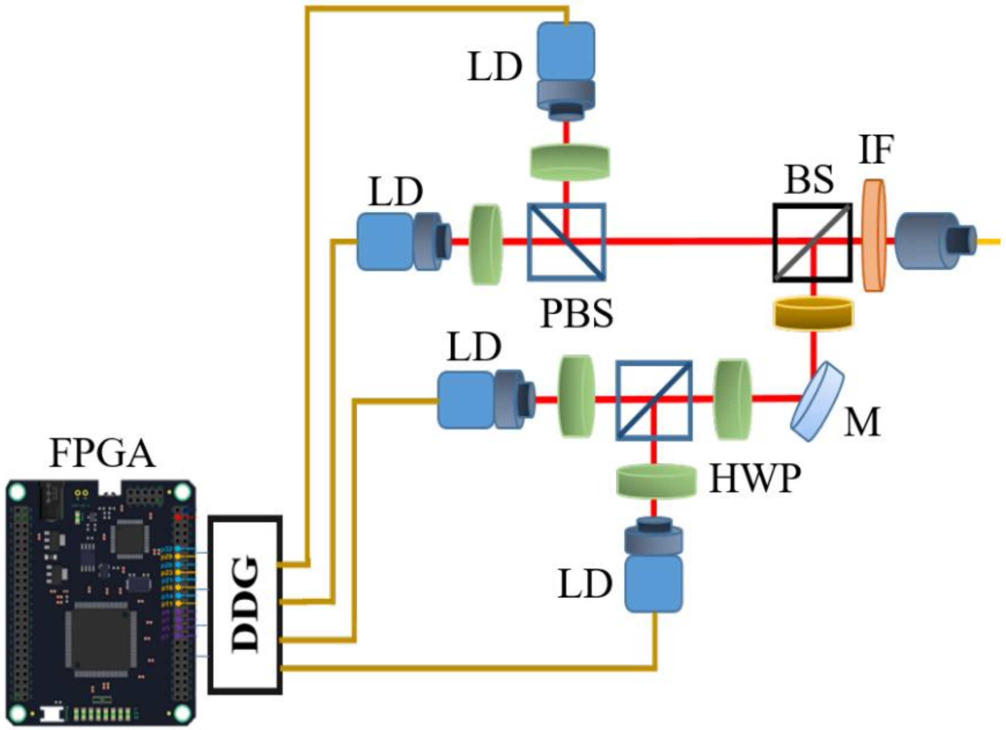


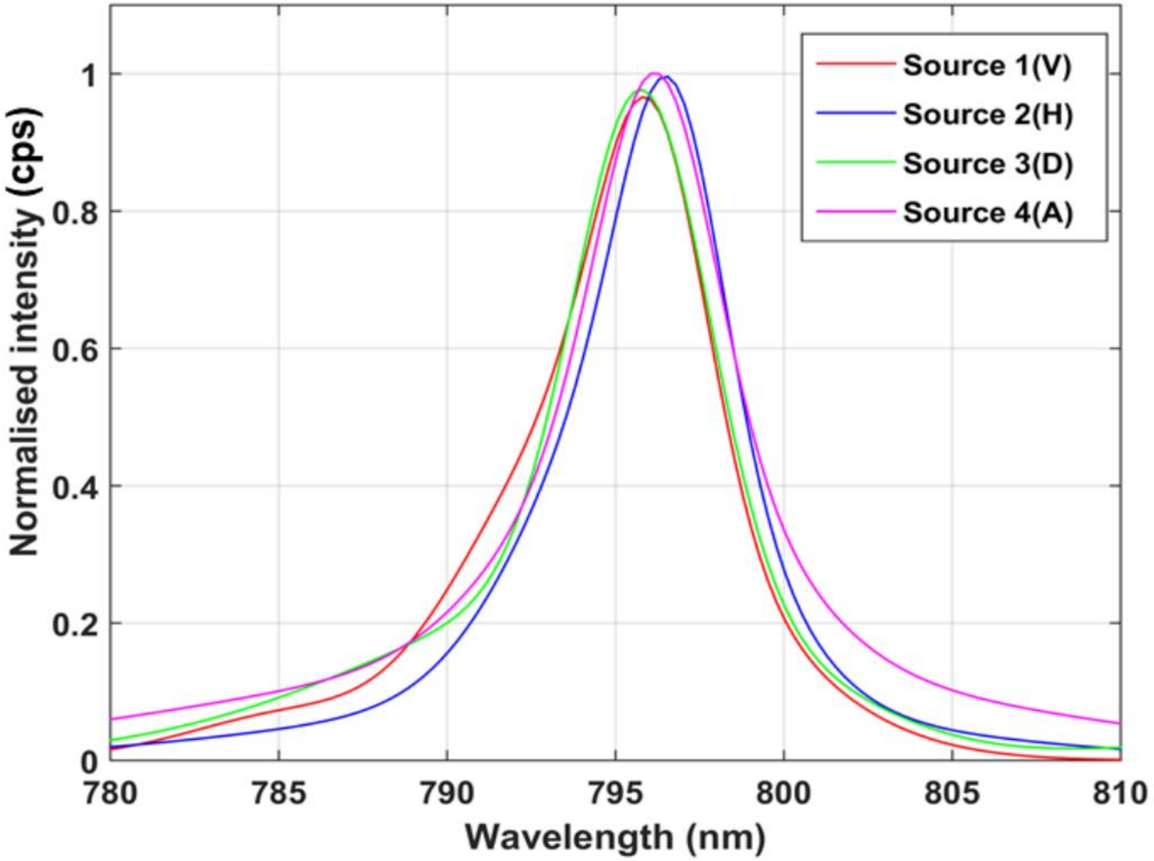
PM QKD: Polarization encoding





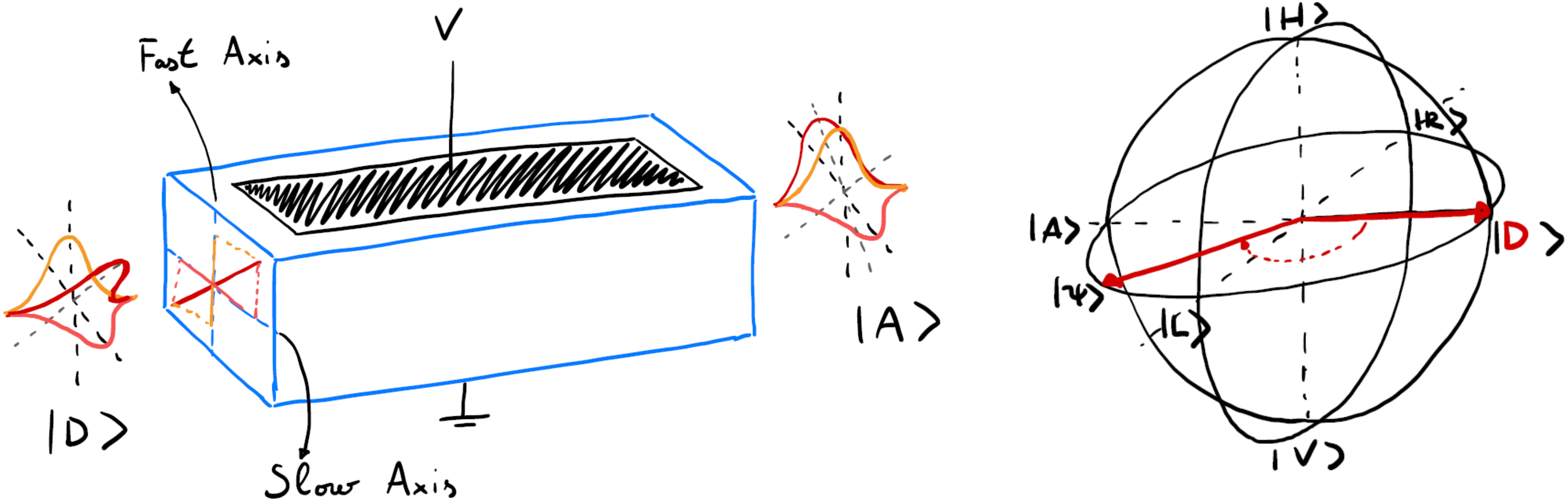
PM QKD: Polarization encoding



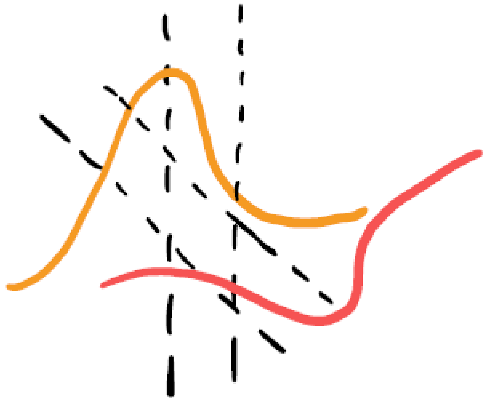


A. Biswas et al., arXiv:2106.10500v3

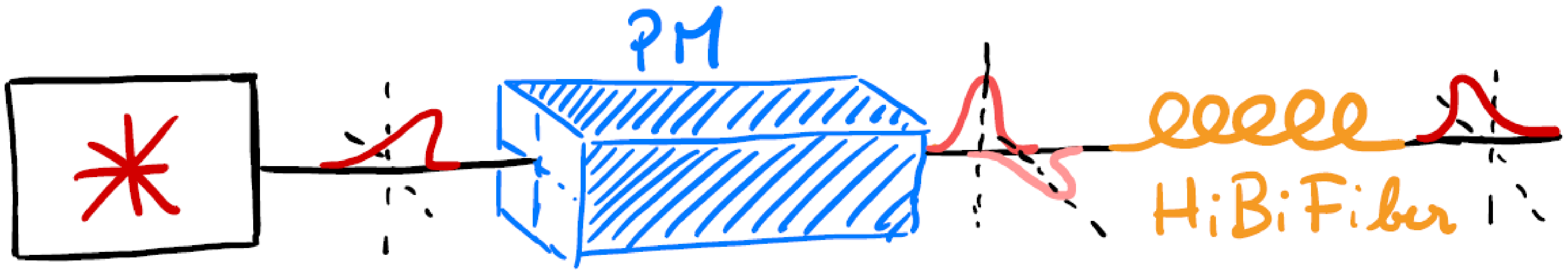
PM QKD: Polarization encoding



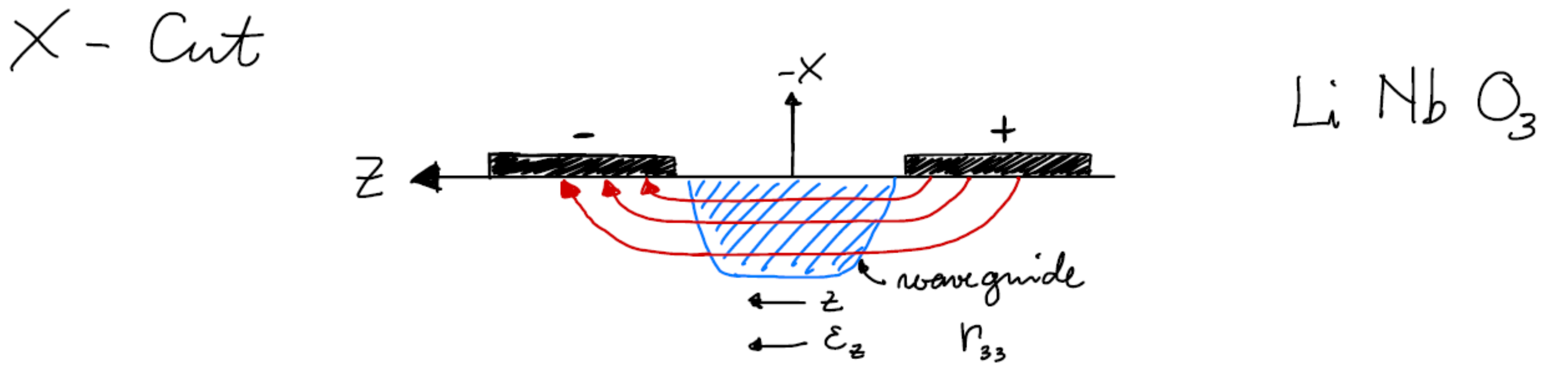
PM QKD: Polarization encoding

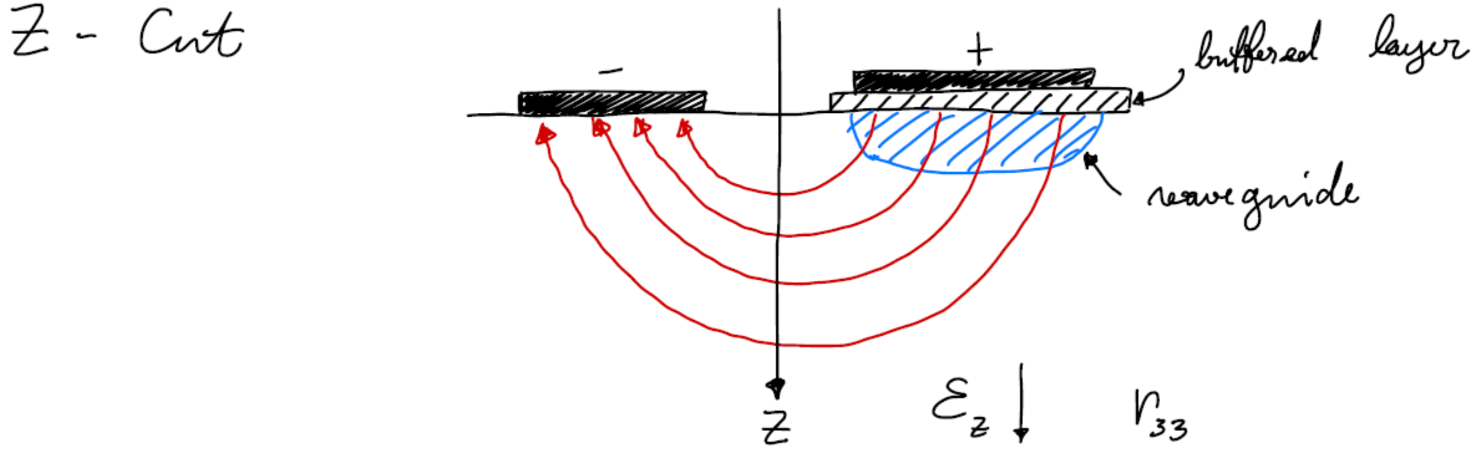


High birefringence can lead to polarization mode dispersion

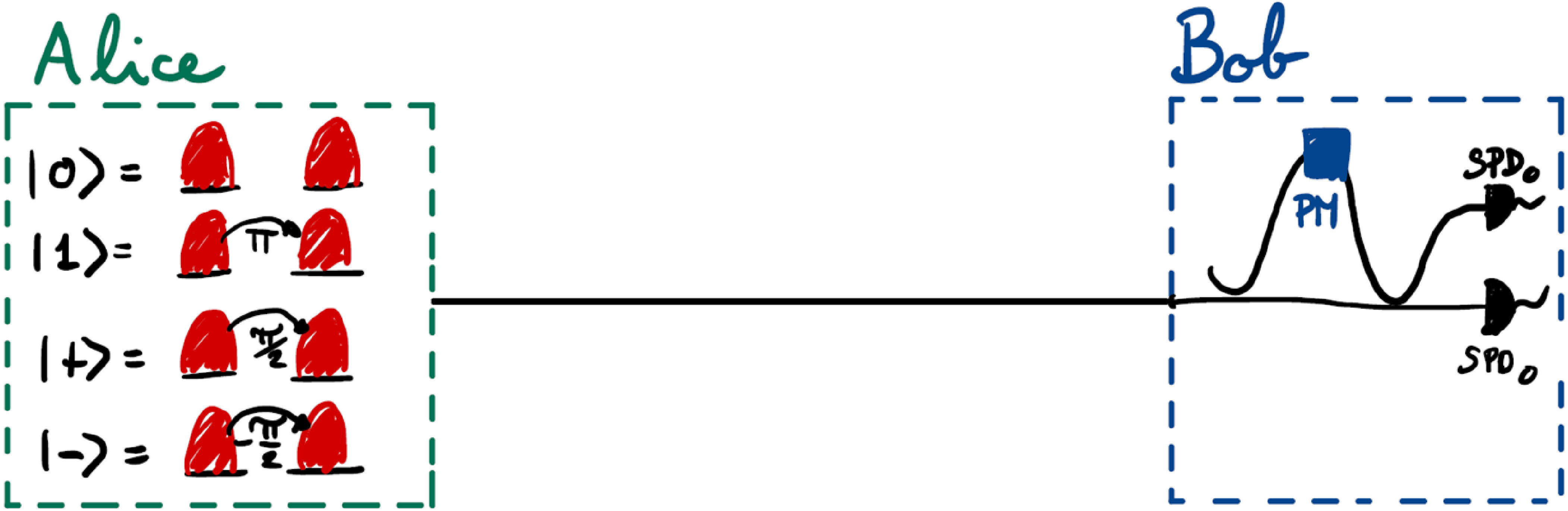


PM QKD: Polarization encoding



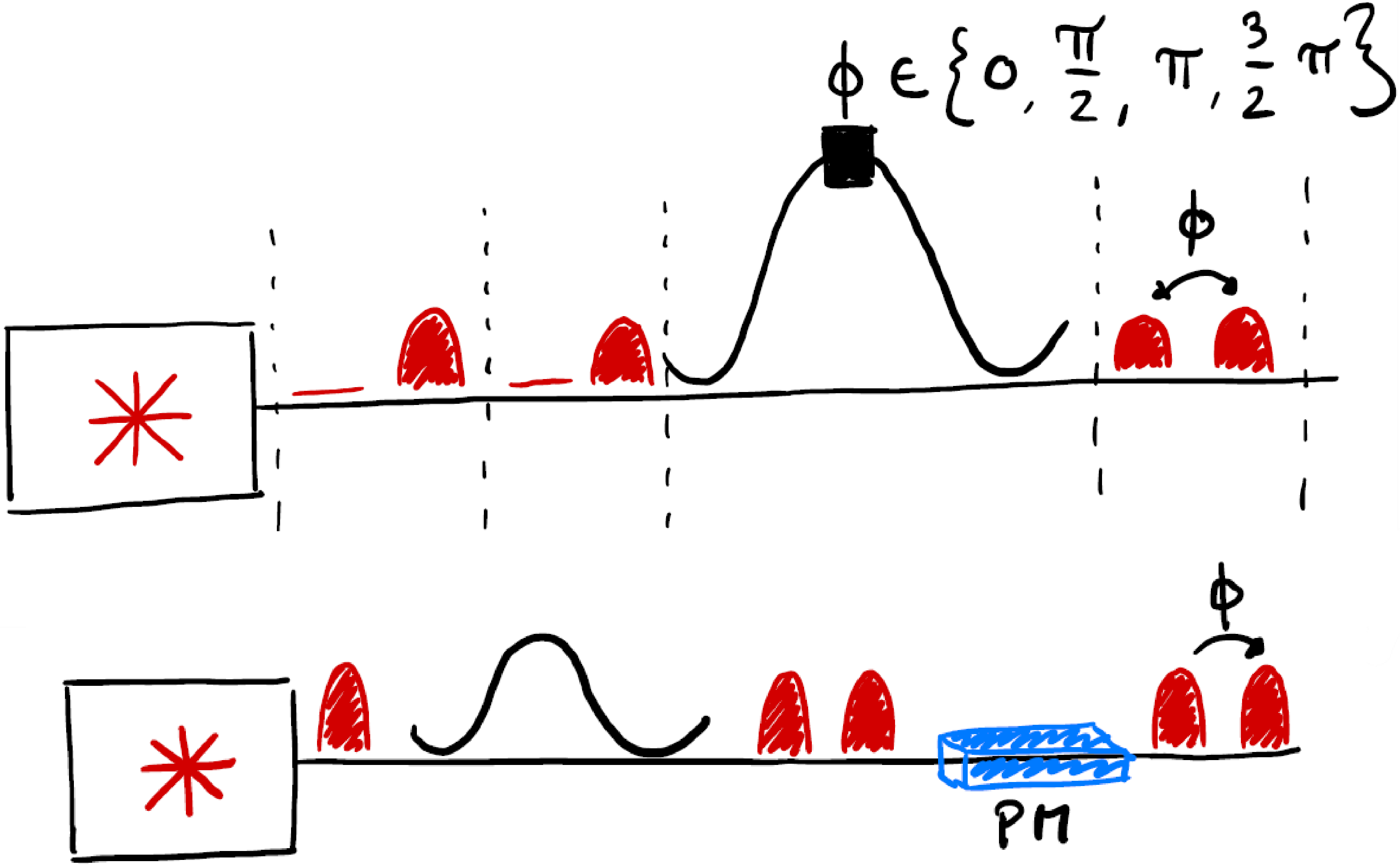


Protocol Implementation: phase

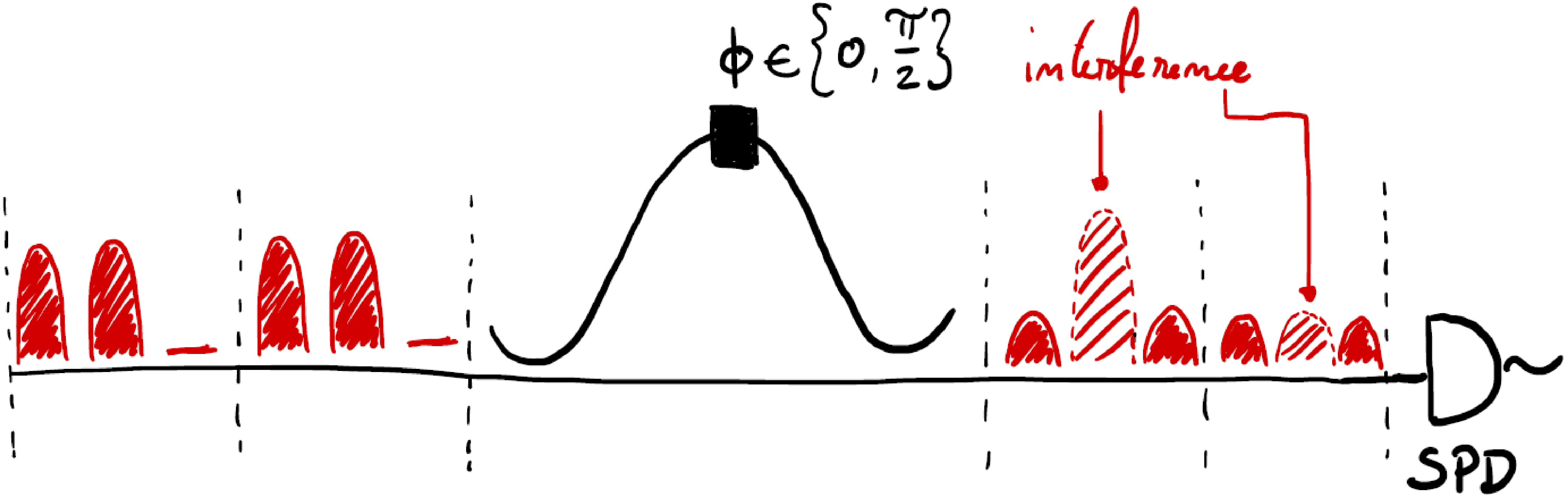


The polarization stabilization is not an issue.
Bob must stabilize the interferometer.

Protocol Implementation: phase

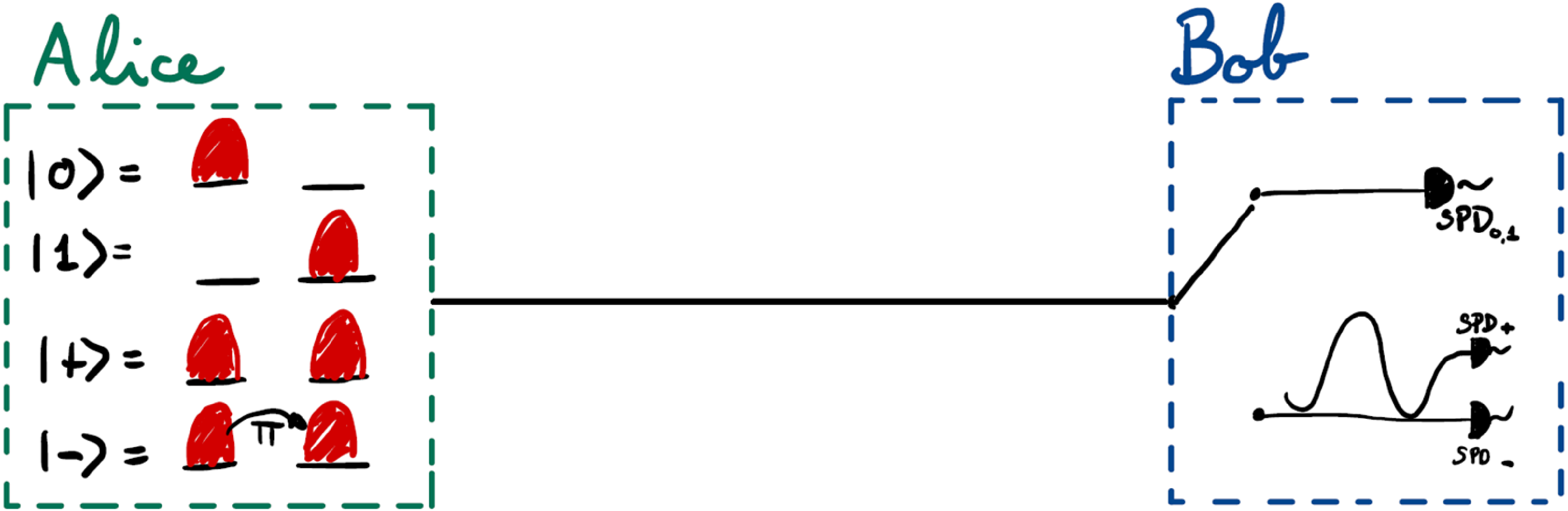


Protocol Implementation: phase



3dB loss intrinsic to the measurement

Protocol Implementation: time-bin/phase

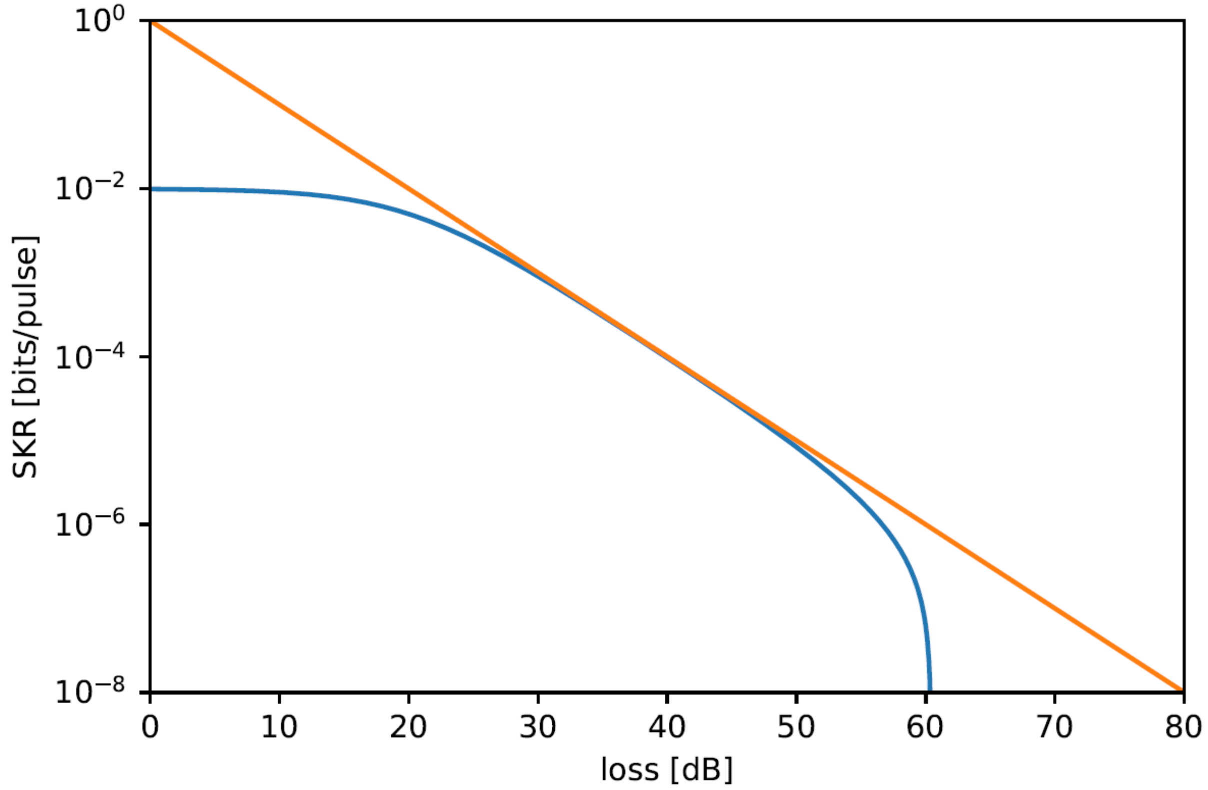


The interferometer needs only one phase.

Protocol Implementation: time-bin/phase

Michelson interferometer with Farady mirrors to avoid polarization dependence

Protocol Implementation and performance

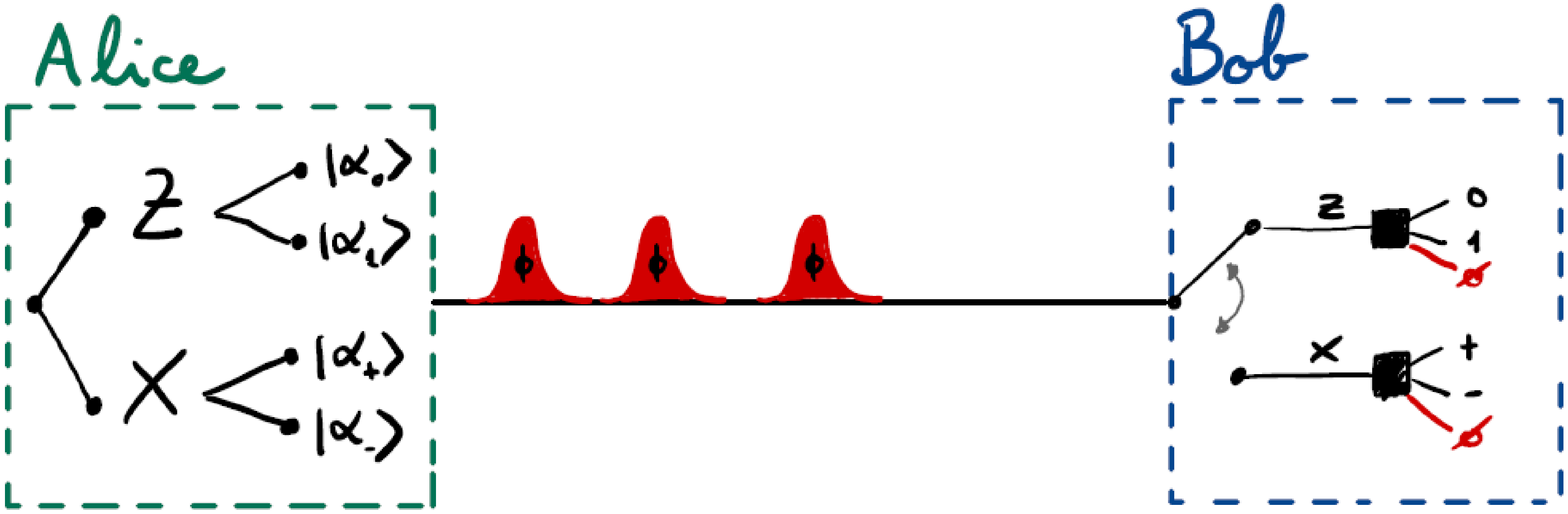


- Ideal BB84 scaling is proportional to the loss and the sifting probability.
- Fiber loss are exponential with respect to the distance (≈ 0.2 dB/km)
- Free space transmission in vacuum has a quadratic scale.
- Detectors have an efficiency, dark counts and saturation

Content

- Introduction
- Single Photon Prepare and Measure QKD
- **Coherent states QKD**
  - **Coherent state BB84**
  - **Photon number splitting attack**
  - **Decoy state method for QKD**
- Implementation a simplified DS-BB84
- Implementation security of QKD
- Conclusion and Outlooks

Coherent State BB84



$$|\alpha_0\rangle = |\alpha\rangle \otimes |0\rangle$$

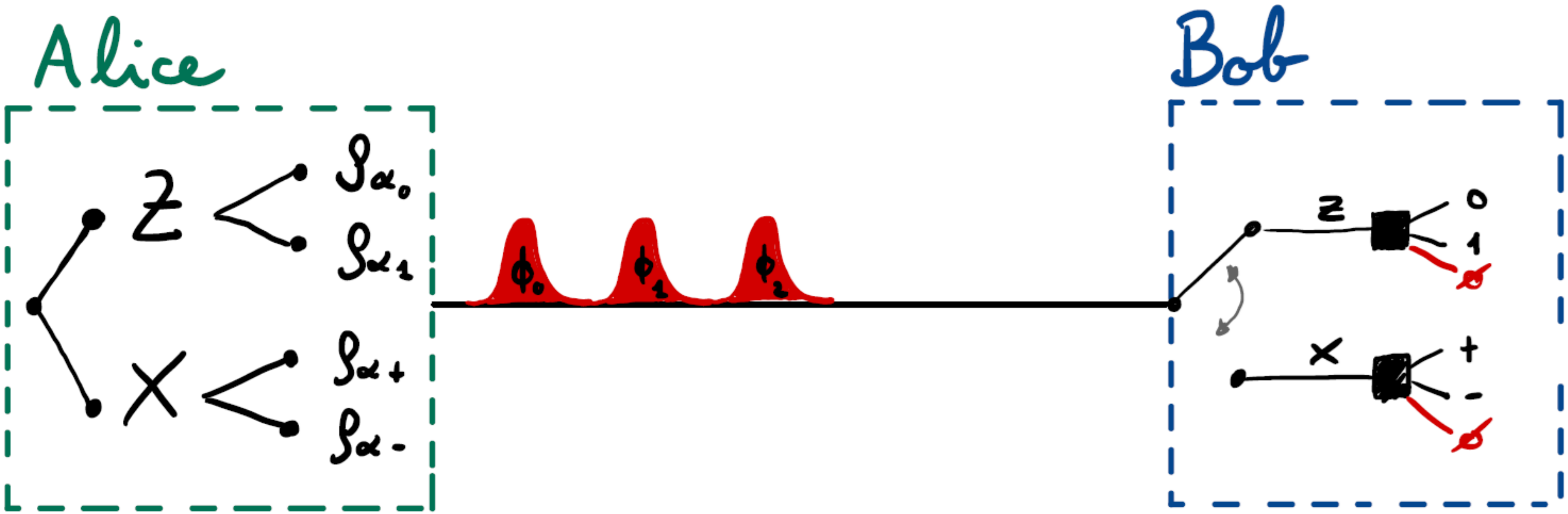
$$|\alpha_1\rangle = |0\rangle \otimes |\alpha\rangle$$

$$|\alpha_+\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle$$

$$|\alpha_-\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|-\frac{\alpha}{\sqrt{2}}\right\rangle$$

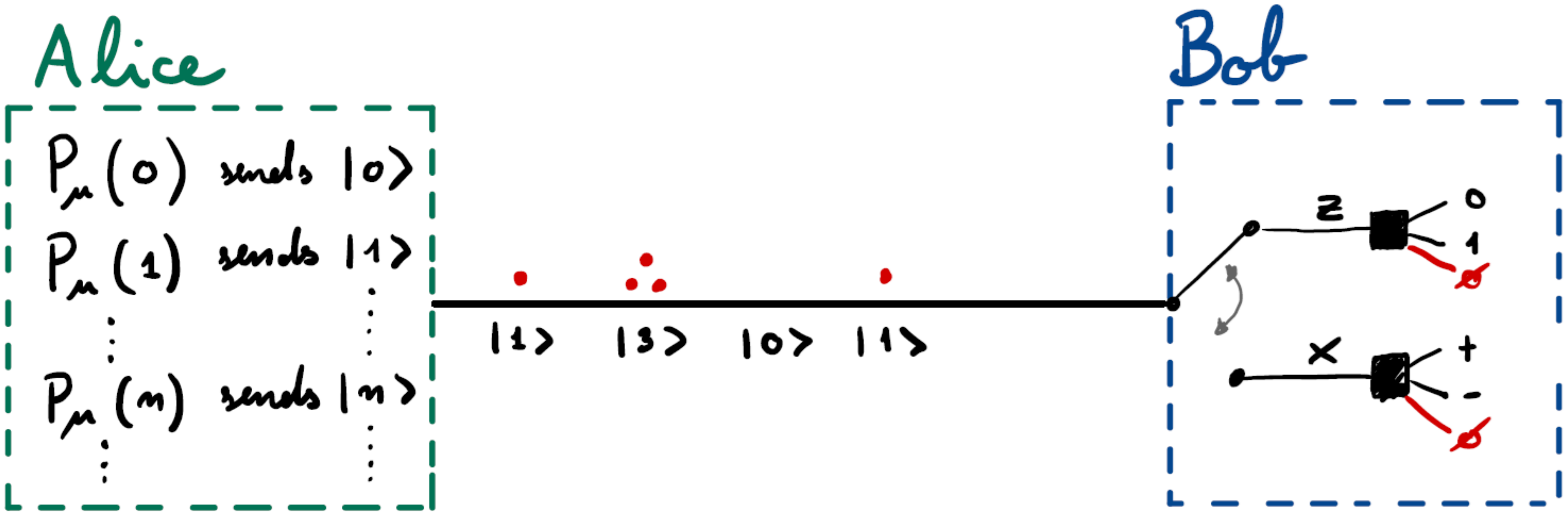
$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

Phase Randomization



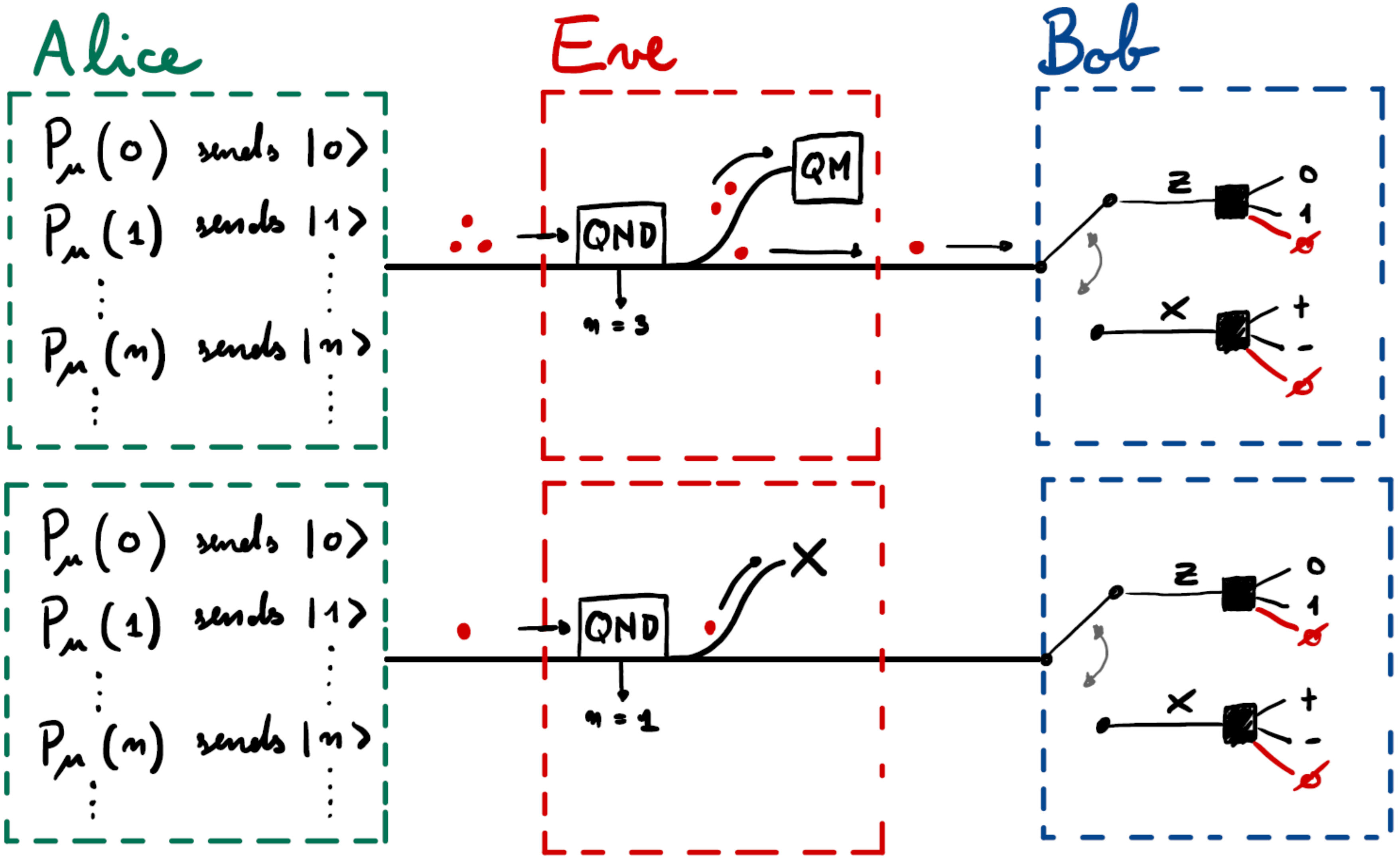
$$\rho_\alpha = \frac{1}{2\pi}\int_{-\infty}^{+\infty} d\phi \, |e^{-i\phi}\alpha\rangle\langle e^{-i\phi}\alpha| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|$$

Phase Randomization



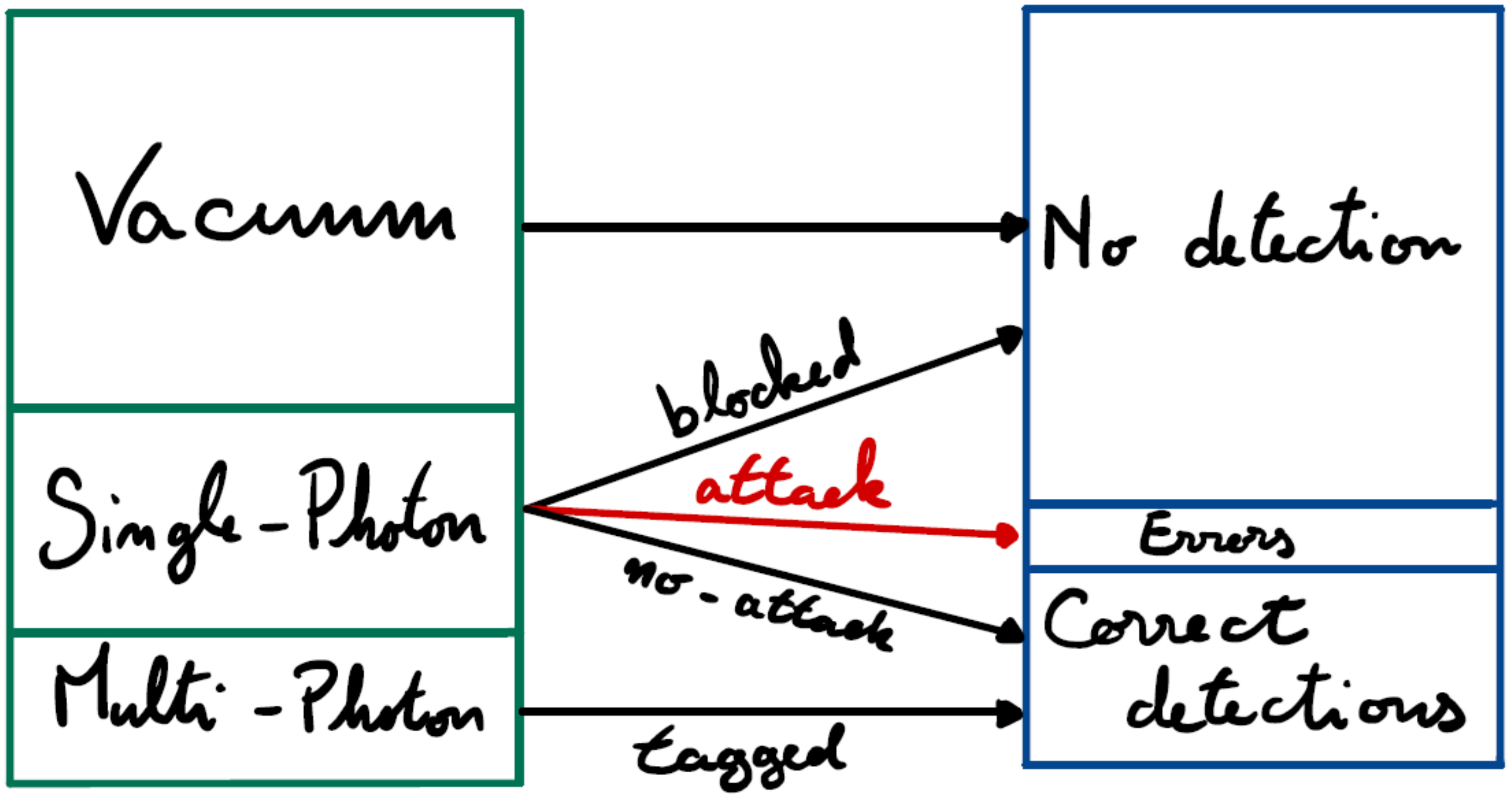
$$\rho_\alpha = \frac{1}{2\pi}\int_{-\infty}^{+\infty} d\phi \, |e^{-i\phi}\alpha\rangle\langle e^{-i\phi}\alpha| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|$$

Photon number splitting attack



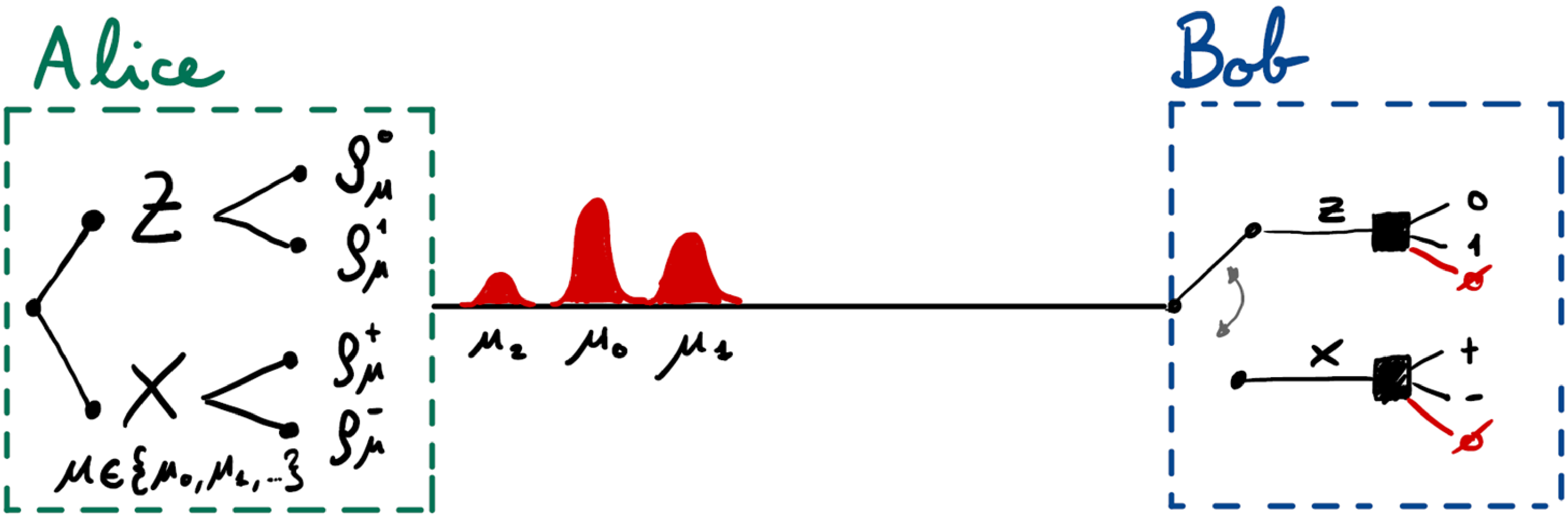
G. Brassard et al., Phys. Rev. Lett. 85, 1330-1333 (2000)

PNS Attack



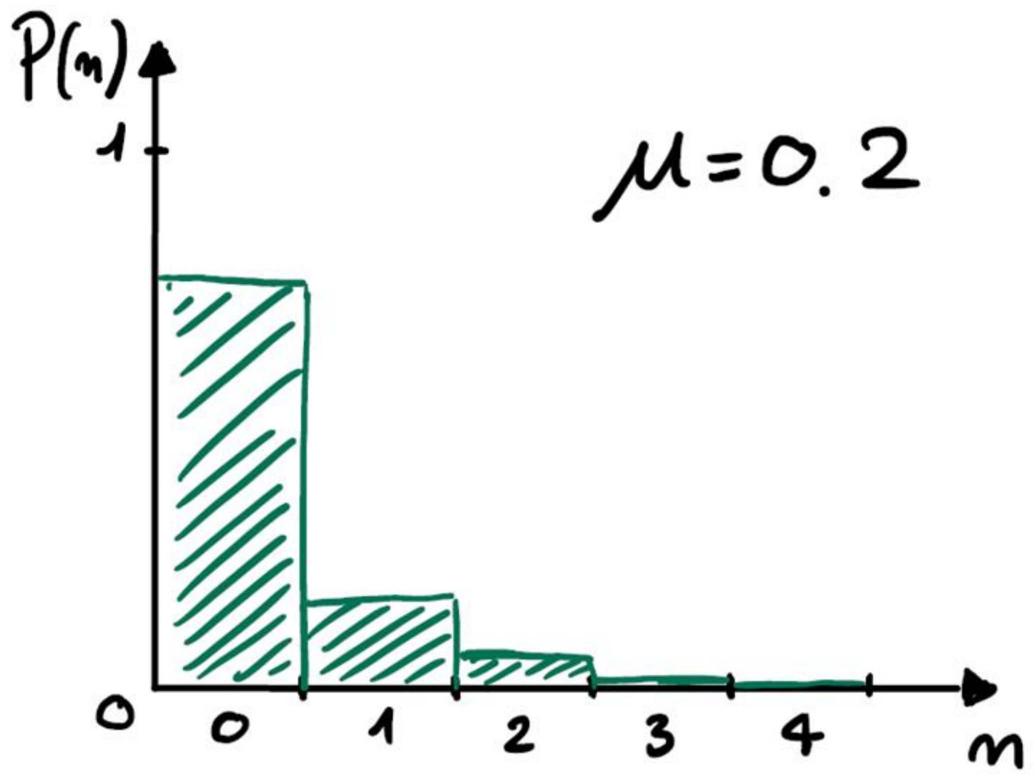
If $P_{multi} \geq P_{det}$ Eve can steal the whole key.

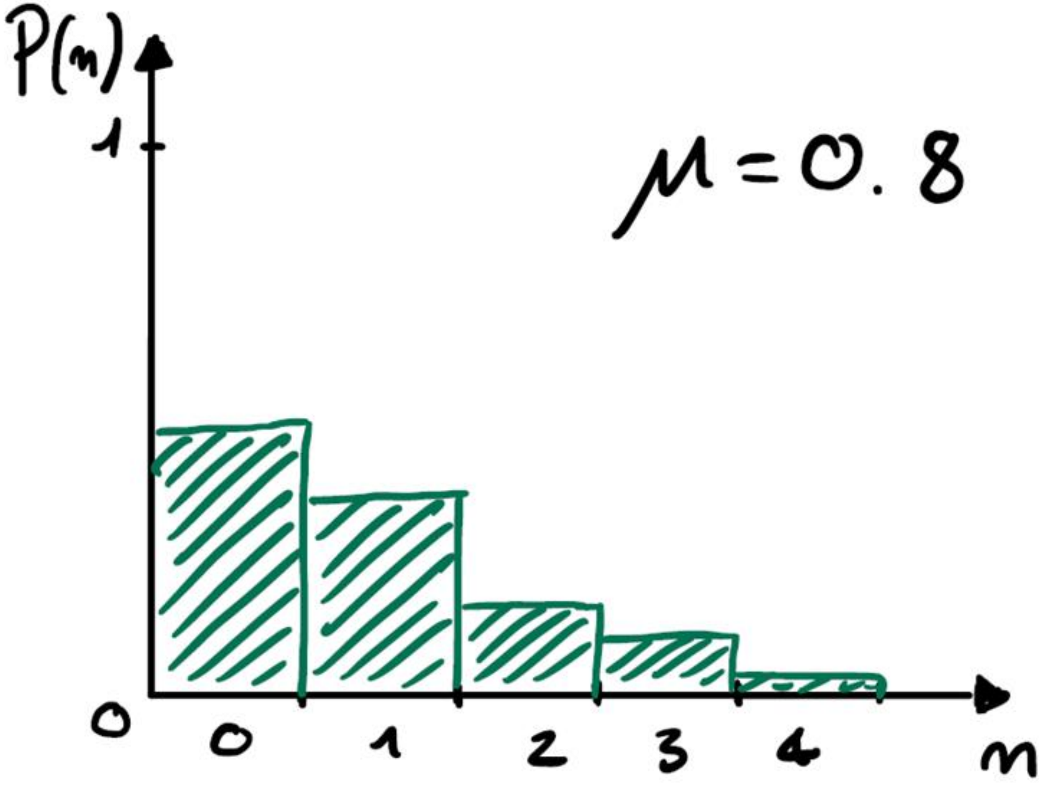
Decoy State BB84



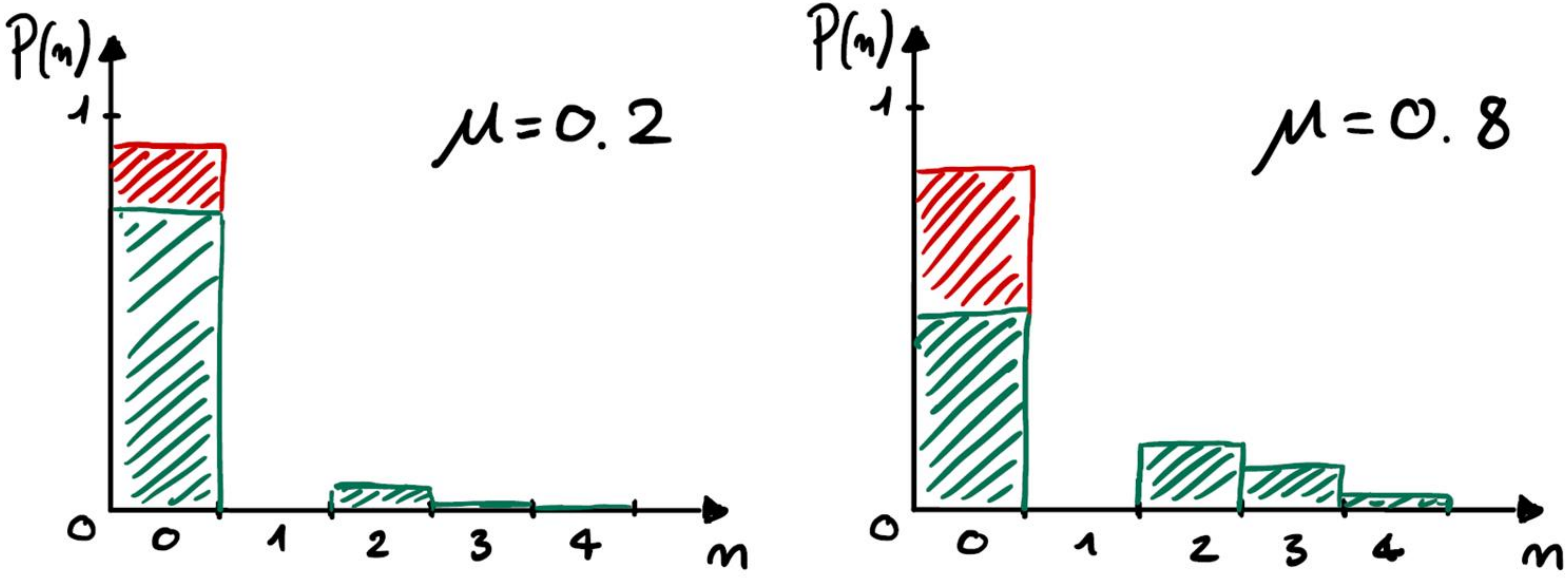
We can modulate the intensity of the phase-randomized coherent pulses

Decoy State BB84





Decoy State BB84



In this case a PNS attack changes the probability of detection with respect to the decoy intensity -> it can be spotted.

Decoy State BB84

By preparing a set of phase randomized coherent state we can estimate how many event Bob detected due to Alice sending a single photon state, i.e. s_1

$$n_{\mu 1} = \sum_n p_{\mu 1|n}\, s_n$$

$$n_{\mu 2} = \sum_n p_{\mu 2|n}\, s_n$$

$$\vdots$$

$$n_{\mu i} = \sum_n p_{\mu i|n}\, s_n$$

$$\vdots$$

$\Longrightarrow$

$$s_0$$

$$s_1$$

$$s_2$$

$$\vdots$$

$$s_n$$

$$\vdots$$

$$l \leq s_{Z,0} + s_{Z,1}\big(1 - h(e_x)\big) - leak_{EC}$$

Decoy State BB84

If the set of intensities is finite, we can have only a bound on the different s_n

$$n_{\mu 1} = \sum_n p_{\mu 1|n}\, s_n \qquad\qquad s_0^l \leq s_0 \leq s_0^u$$

$$n_{\mu 2} = \sum_n p_{\mu 2|n}\, s_n \qquad \Longrightarrow \qquad s_1^l \leq s_1 \leq s_1^u$$

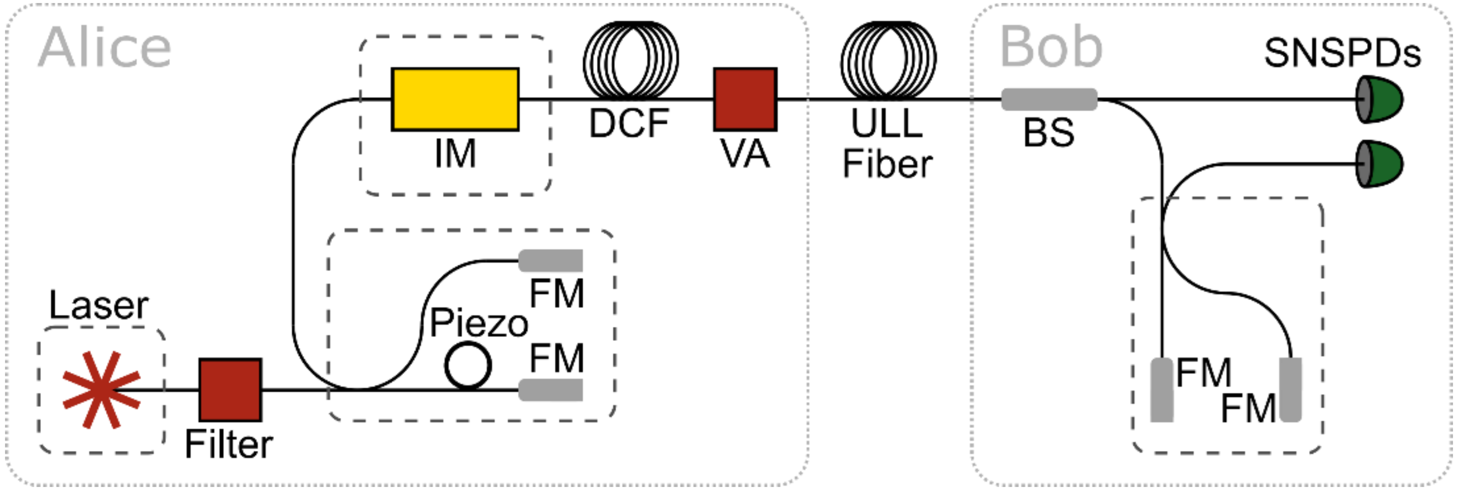
$$n_{\mu 3} = \sum_n p_{\mu 3|n}\, s_n \qquad\qquad s_m^l \leq s_m \leq s_m^u$$

$$l \leq s_{Z,0}^l + s_{Z,1}^l\left(1 - h\left(e_{X,1}^u\right)\right) - leak_{EC}$$

Content

- Introduction
- Single Photon Prepare and Measure QKD
- Coherent states QKD
- **Implementation a simplified DS-BB84**
    - **States preparation**
    - **Measurement**
    - **SKR performance**
    - **Free space link**
- Implementation security of QKD
- Measurement device independent QKD

Implementation of a Decoy-State BB84

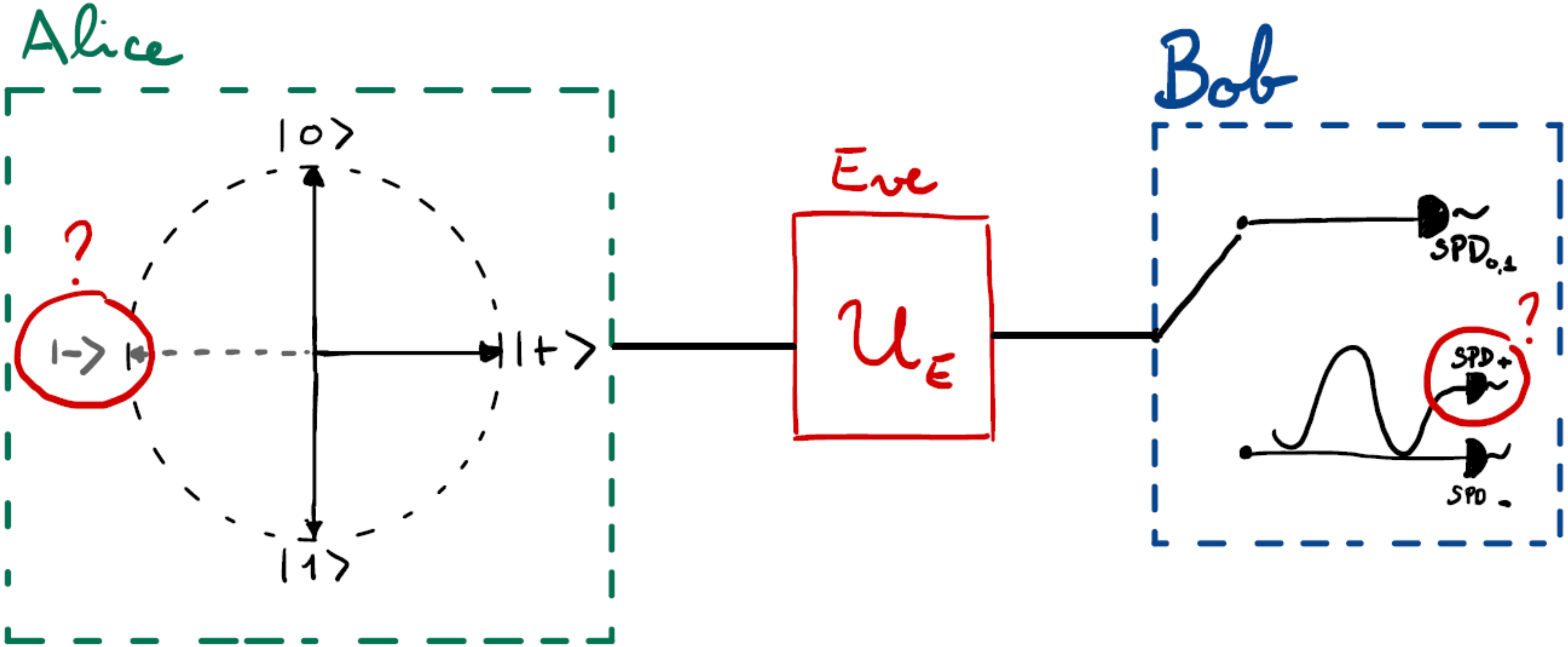


basis, bit	state	μ_1	μ_2
Z, 0	$\|0\rangle$		
Z, 1	$\|1\rangle$		
X, 0	$\|+\rangle$		

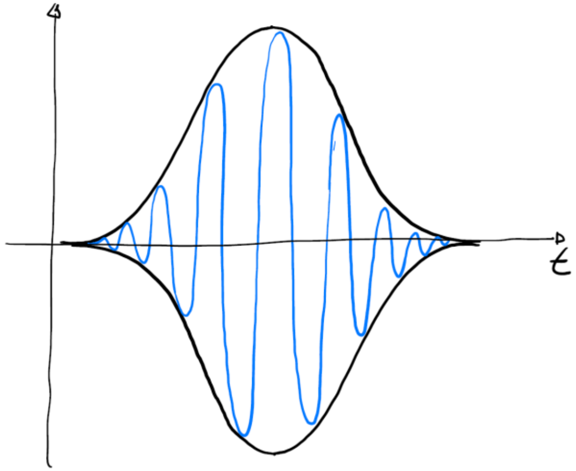
Simplified decoy-state BB84 with 3 states and 1 decoy

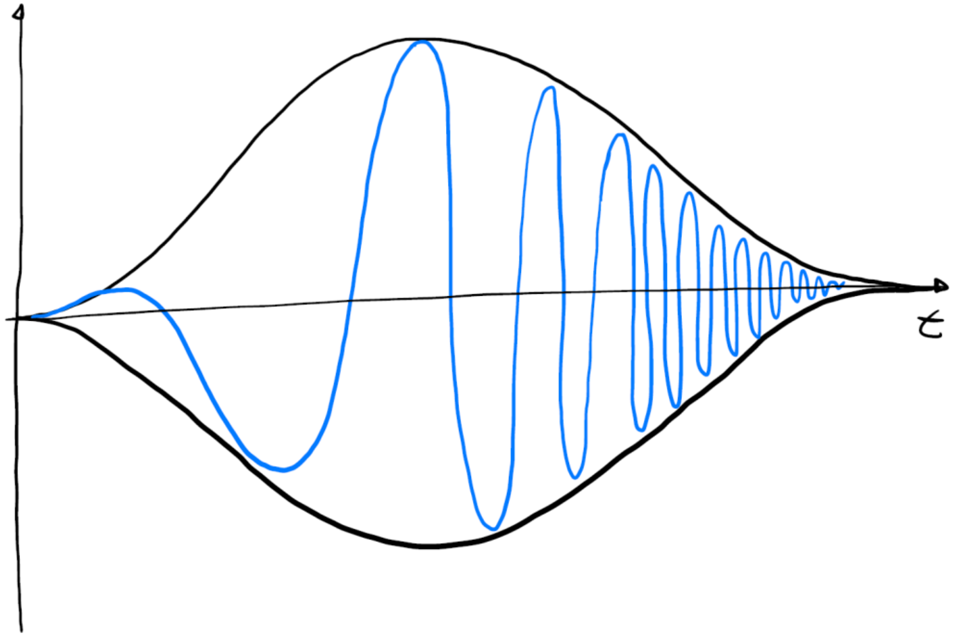
A. Boaron et al., Phys. Rev. Lett. 121, 190502 (2018)

Implementation of a Decoy-State BB84



Chromatic mode dispersion



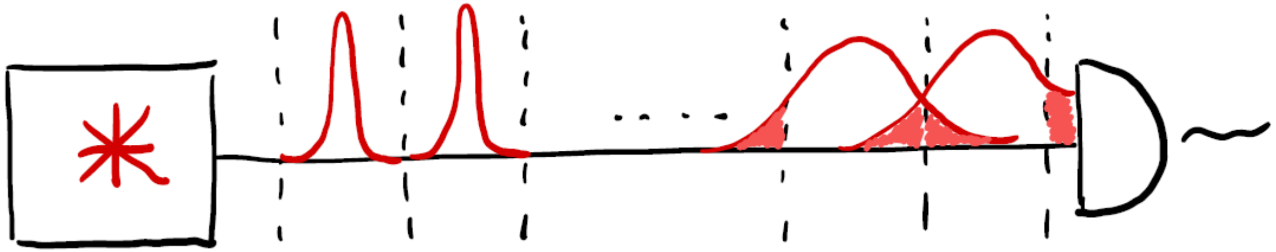


$$\frac{\partial k}{\partial \omega} = \frac{1}{v_g}$$

$$k(\omega) = k_0 + \frac{\partial k}{\partial \omega}(\omega - \omega_0) + \frac{\partial^2 k}{\partial \omega^2}(\omega - \omega_0)^2 + \cdots$$

$$D = -\frac{2\pi c}{\lambda}\frac{\partial^2 k}{\partial \omega^2}$$

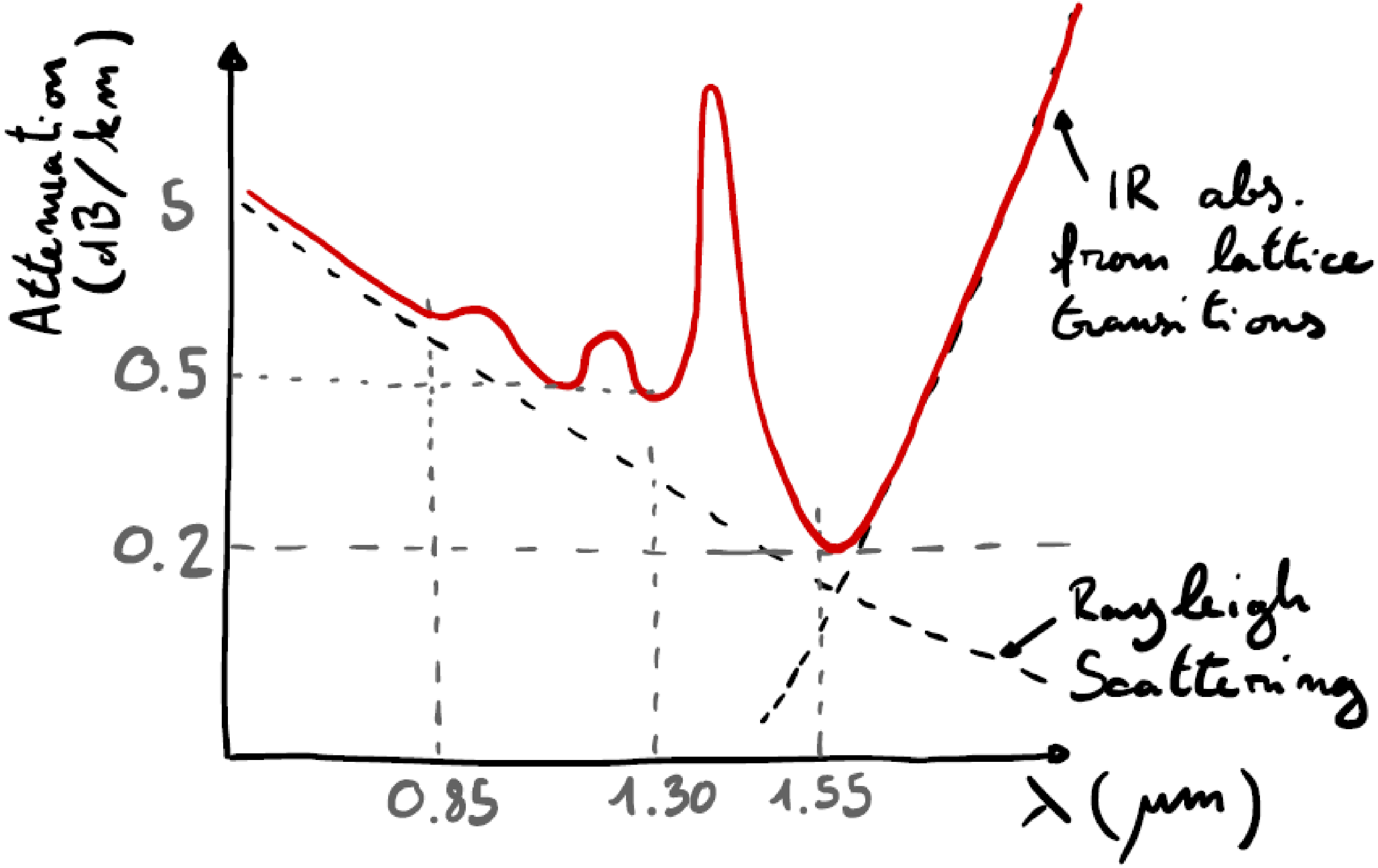
Chromatic mode dispersion



Typical dispersion for ULL Corning fiber: 17 ps/(nm*km)

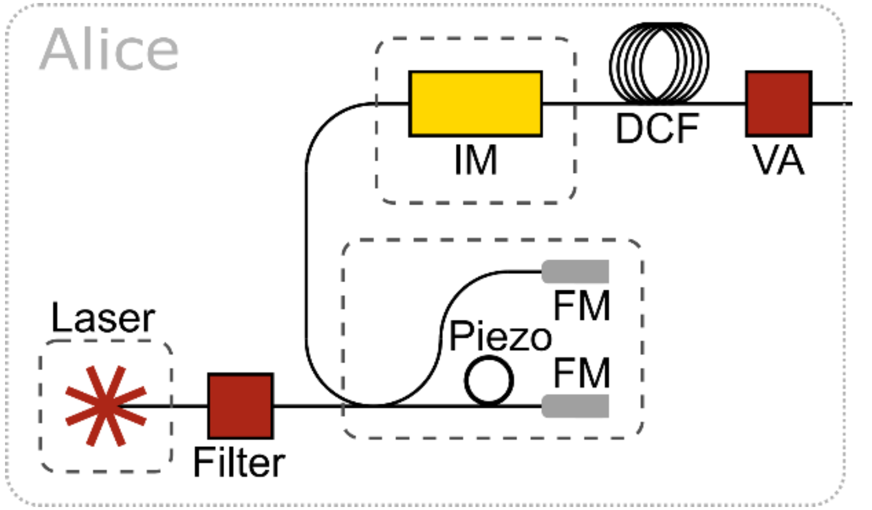
To compensate for that we use dispersion compensating Fiber: -140 ps/(nm*km)

Fiber transmission spectrum

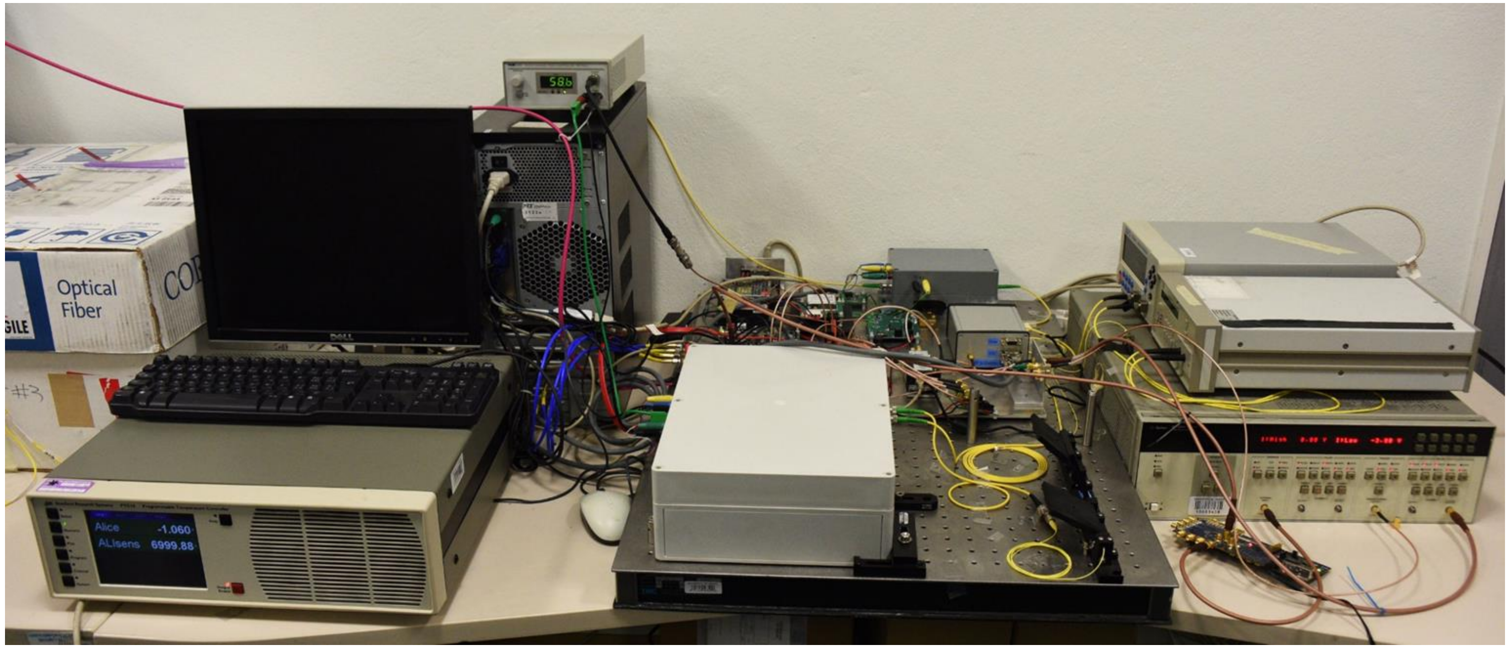


Fibred high repetition rate source

- Phase-randomized DFB laser at 1550 nm:
  - Repetition rate: 2.5 GHz
  - Pulse duration: 30 ps
- High speed integrated intensity modulator: 5 GHz



→ requires dispersion compensation fibre: -140 ps/nm/km



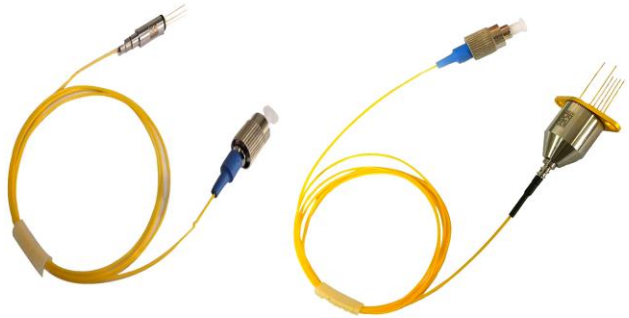
Quantum channel: ultra low-loss fibres

Corning ULL-28® ultra low loss fibre: 0.16 dB/km

Attenuation including connectors and splices: 0.17 dB/km

CORNING

Single photon detectors: SPAD



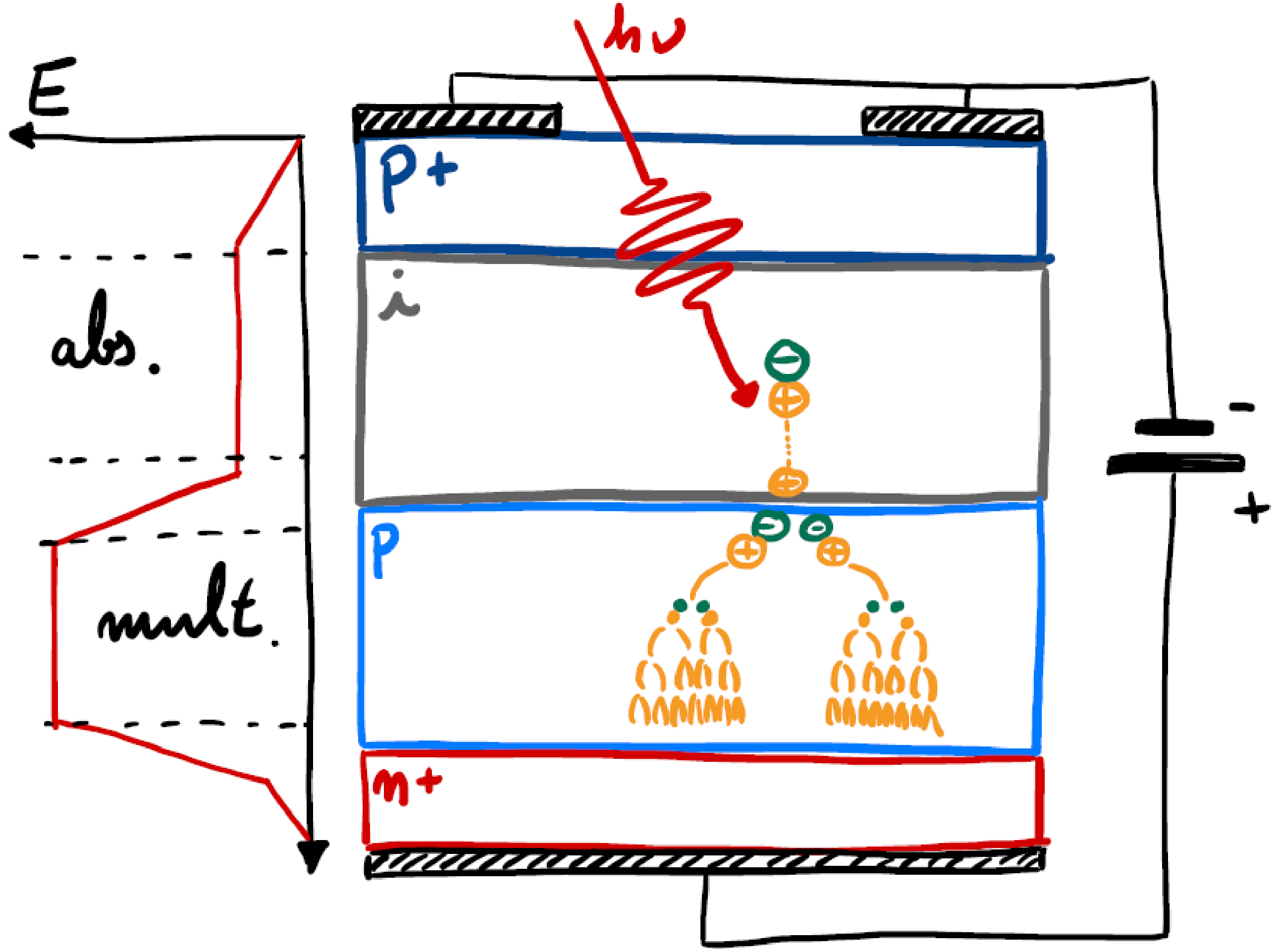
Single photon avalanche photodiode (SPAD):

Temperature (170 K to 250 K)

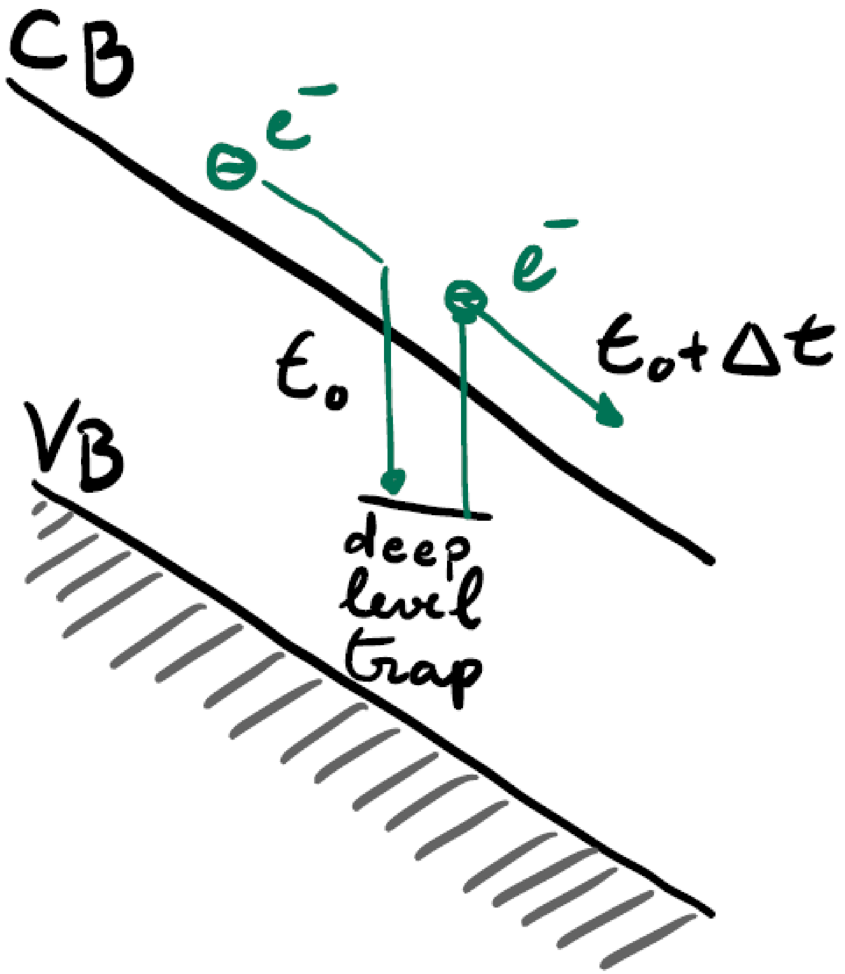
Silicon:
Dark counts: 10/s to 1000/s at 250k
Efficiency: 70% at 550 nm, 25% at 730 nm
Timing jitter: 40 ps

InGaAs:
Dark counts: 50/s to 1000/s at 180k
Efficiency: 25% at 1550 nm
Timing jitter: 40 ps

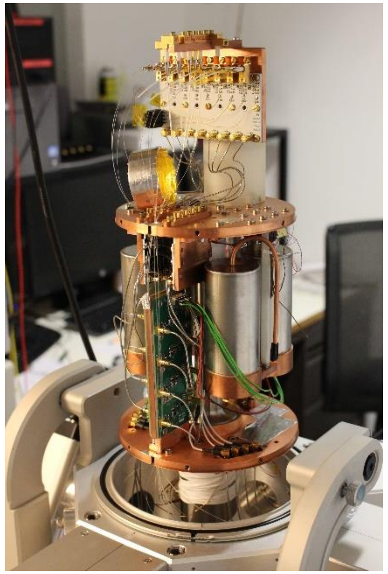
Single photon detectors: SPAD



SPAD: aftrpulsing



Single photon detectors: SNSPD



Superconducting nanowire single-photon detectors

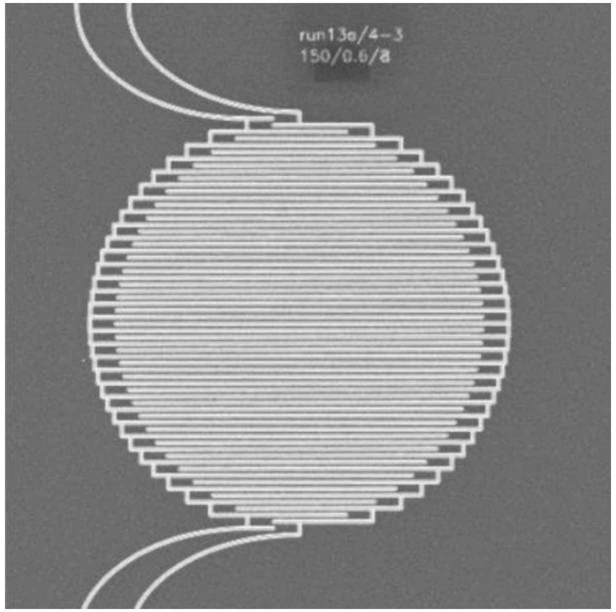
Amorphous molybdenum silicide

Temperature: 0.8 K

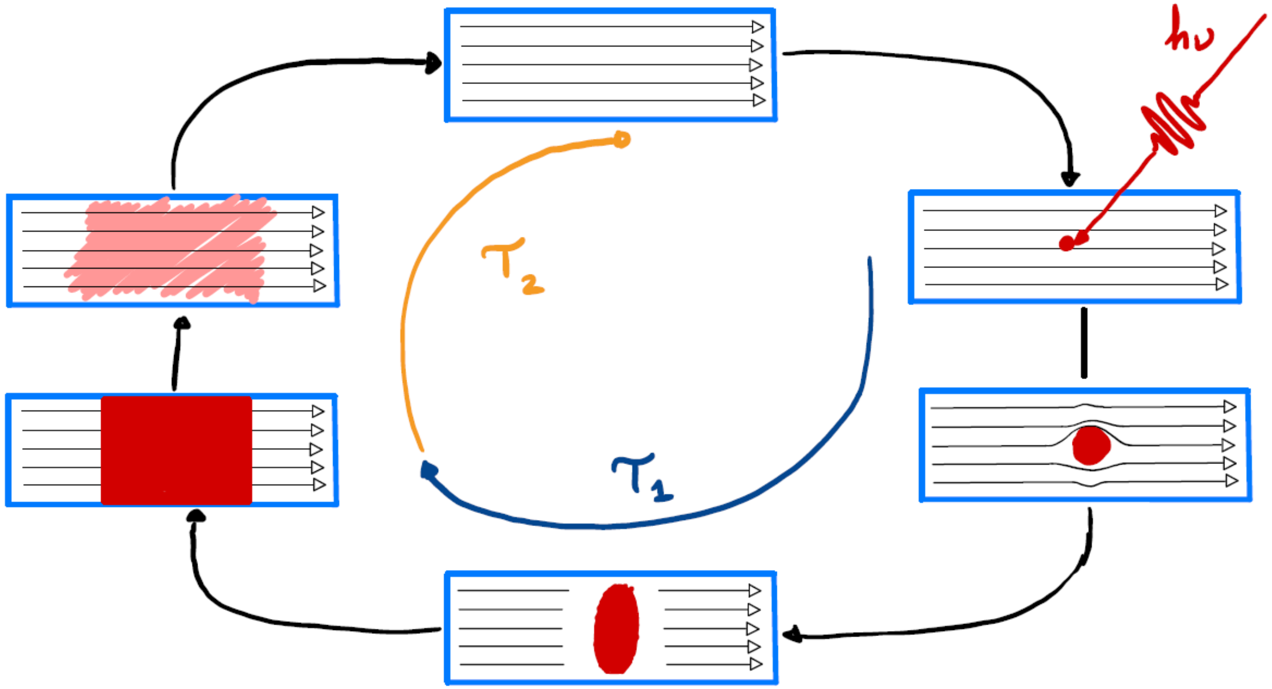
Dark counts: < 0.3 count/s

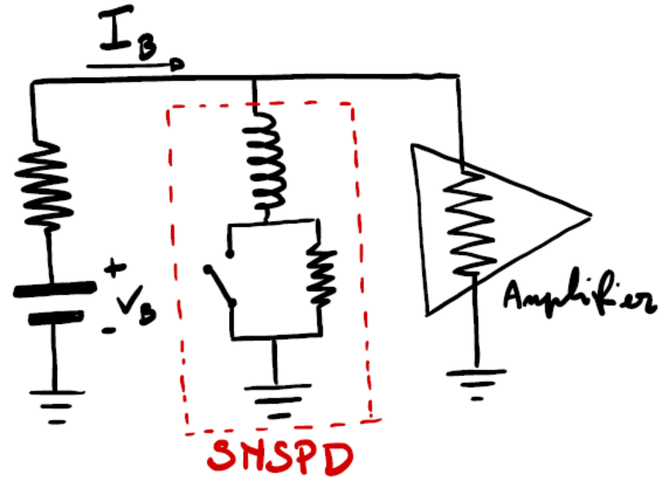
Efficiency: 50% (at low dark counts rates)

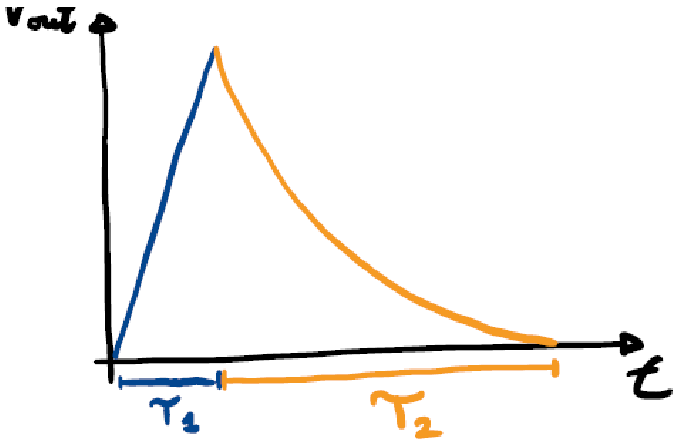
Timing jitter: 30 ps



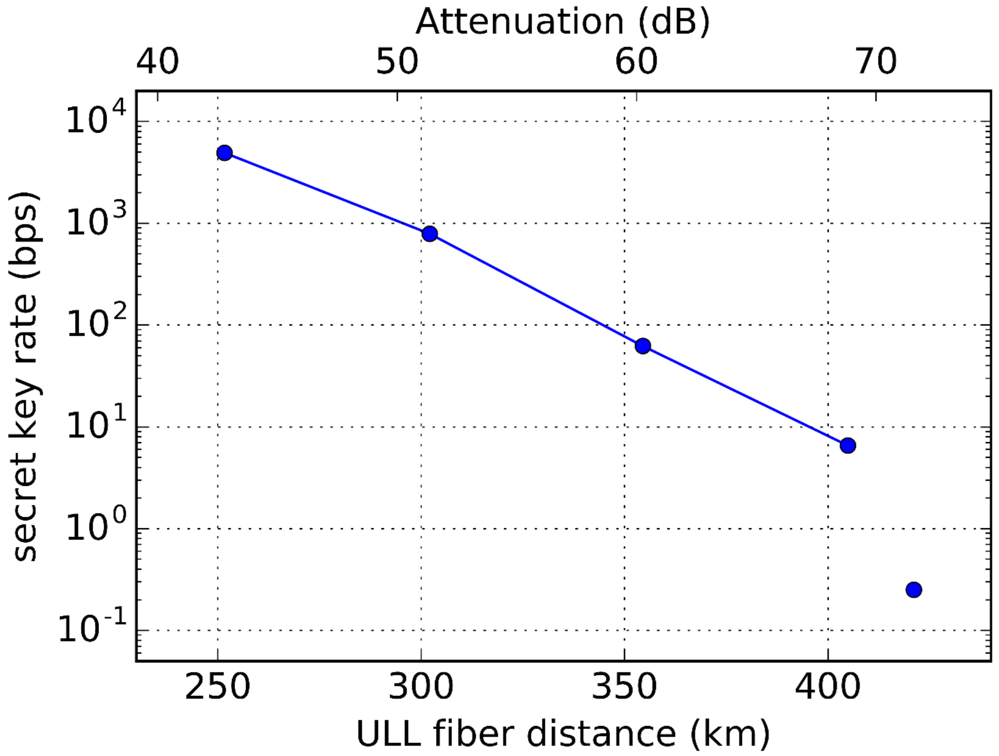
Single photon detectors: SNSPD







Secret key rate vs distance



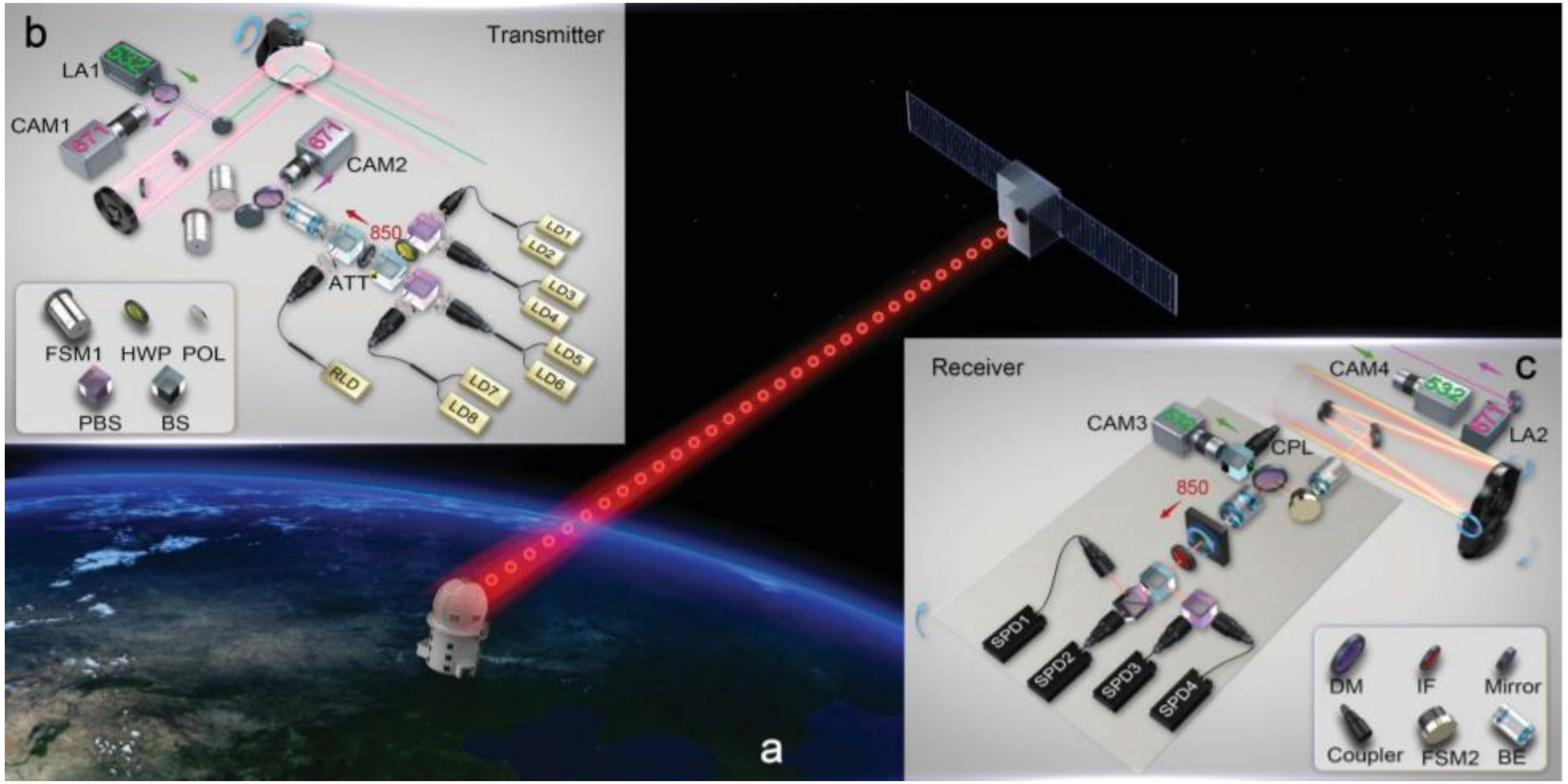
421 km | 71.9 dB

24.2 h overall acquisition time

12.7 h of data used

length (km)	attn (dB)	μ_1	μ_2	block size	block time (h)	QBER Z (%)	ϕ_Z (%)	RKR (bps)	SKR (bps)
251.7	42.7	0.49	0.18	$8.2 \cdot 10^6$	0.20	0.5	2.2	$12 \cdot 10^3$	$4.9 \cdot 10^3$
302.1	51.3	0.48	0.18	$8.2 \cdot 10^6$	1.17	0.4	3.7	$1.9 \cdot 10^3$	$0.79 \cdot 10^3$
354.5	60.6	0.35	0.15	$6.2 \cdot 10^6$	14.8	0.7	1.8	117	62
404.9	69.3	0.35	0.15	$4.1 \cdot 10^5$	6.67	1.0	4.3	17	6.5
421.1	71.9	0.30	0.13	$2.0 \cdot 10^5$	24.2 (12.7*)	2.1	12.8	2.3 (4.5*)	0.25 (0.49*)

Satellite QKD



Decoy state BB84 protocol

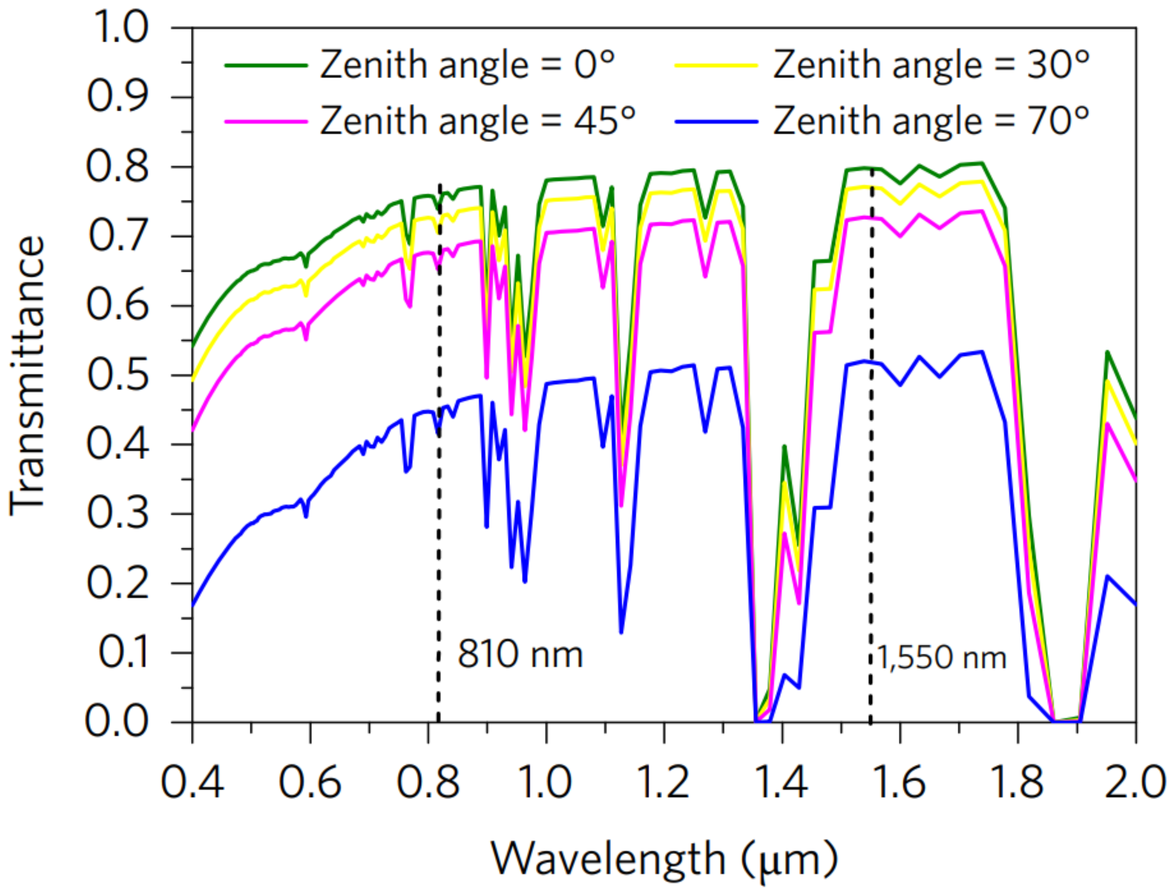
Polarization encoding.

Laser wavelength: 850 nm.

SKR transmission up to 1200 km.

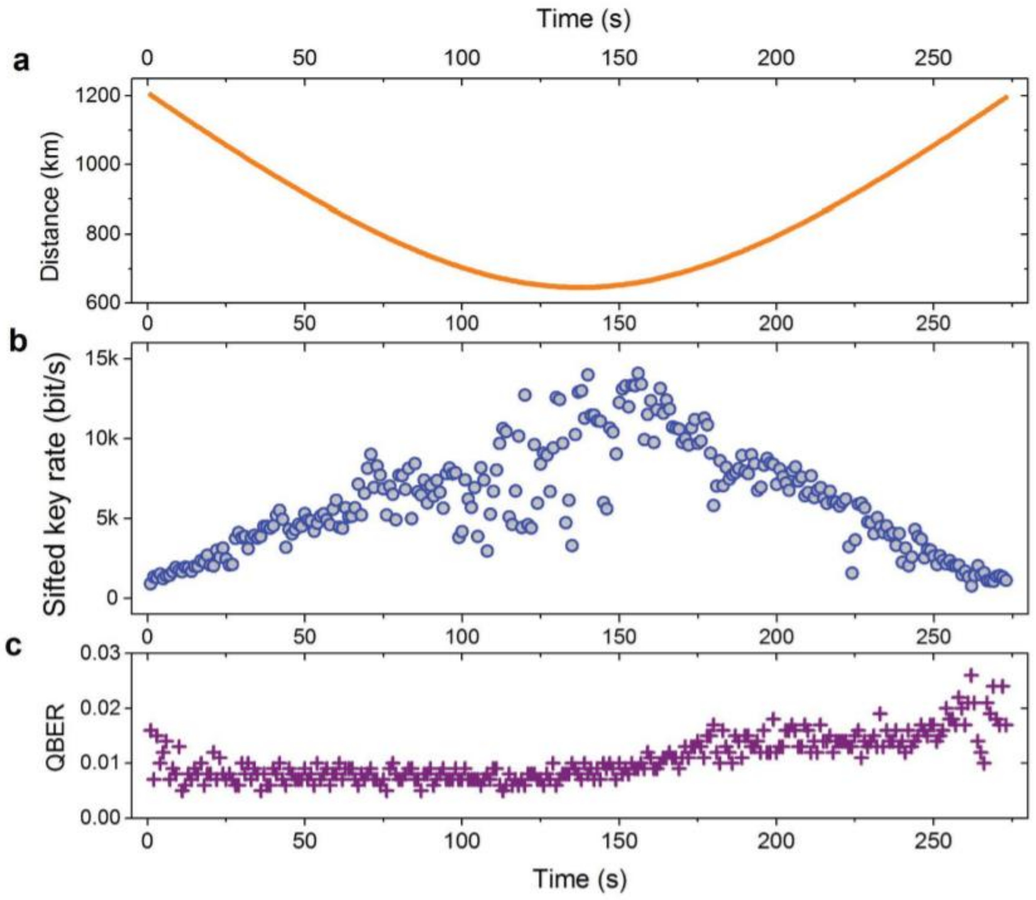
S.-K. Liao et al., Nature volume 549, pages43–47 (2017)

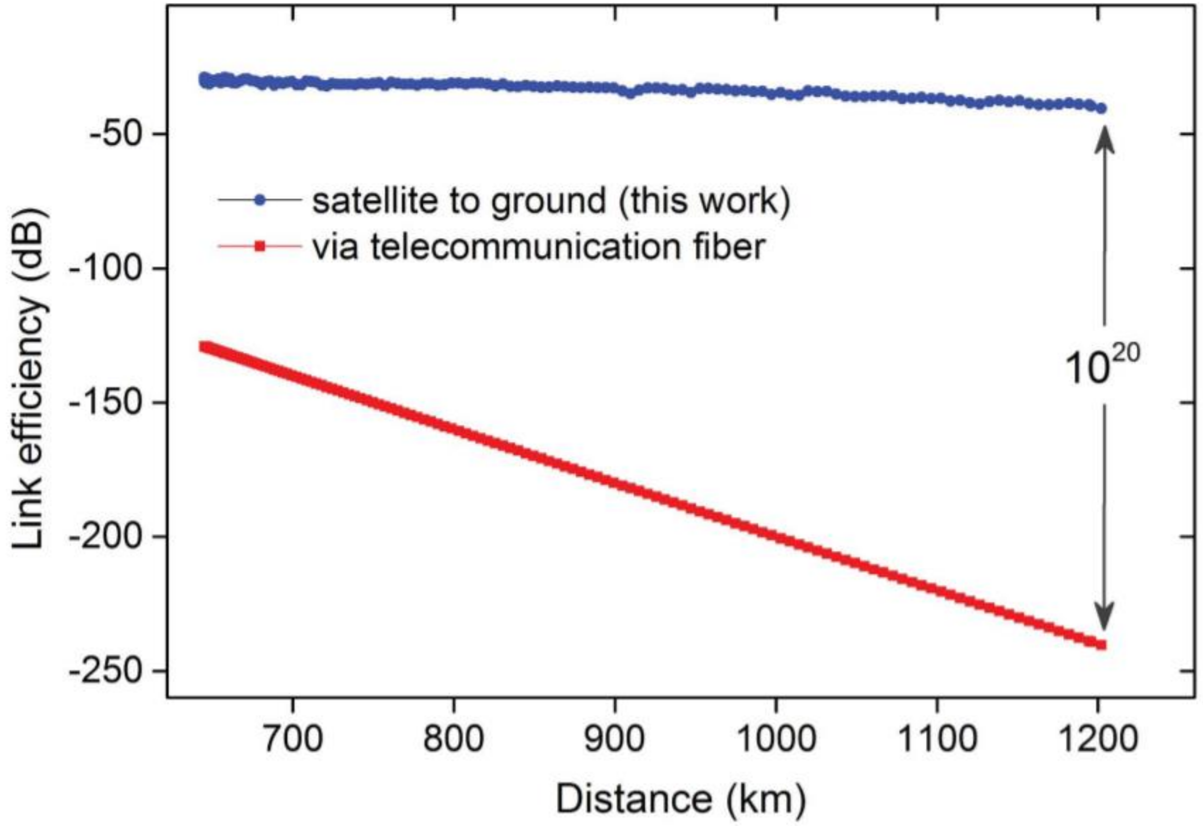
Satellite QKD



S.-K. Liao et al., Nature Photonics , (2017)

Satellite QKD





Content

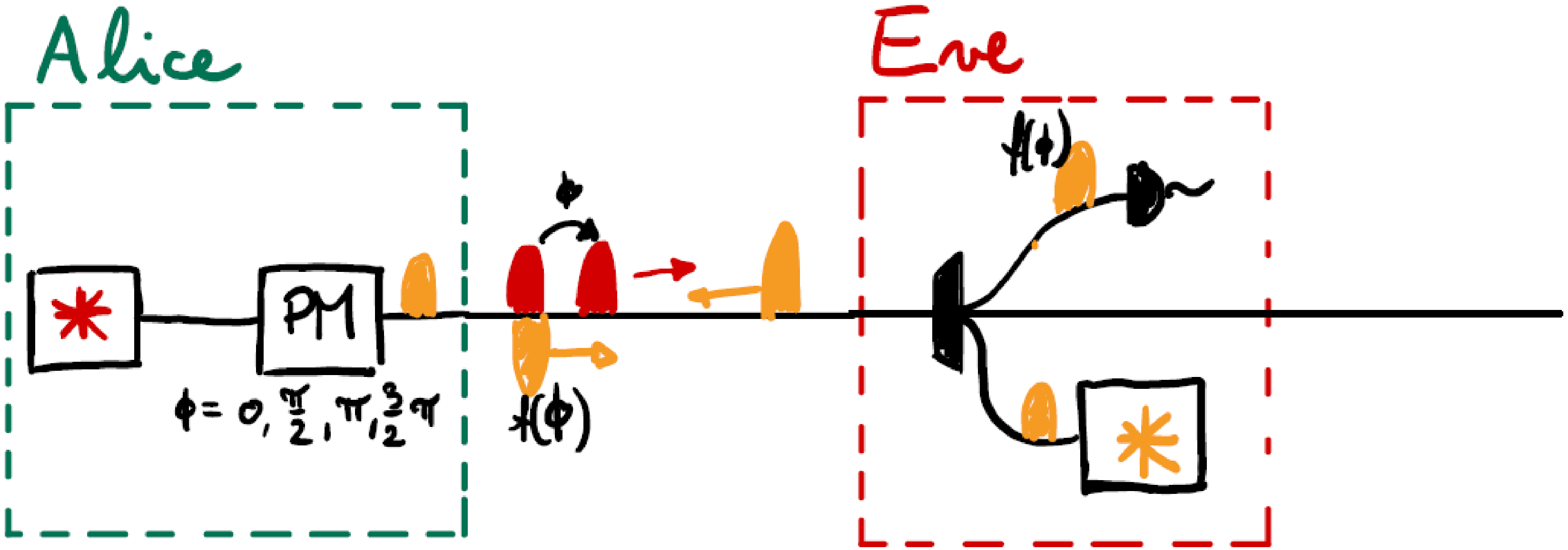
- Introduction
- Single Photon Prepare and Measure QKD
- Coherent states QKD
- Implementation a simplified DS-BB84
- **Implementation security of QKD**
  - **Trojan horse attack on the source**
  - **Blinding attack on the detectors**
- Measurement device independent QKD

Practical security

- What happens if some assumptions are not respected?

- There is a difference between proving the security of an ideal protocol and the security of its implementation.

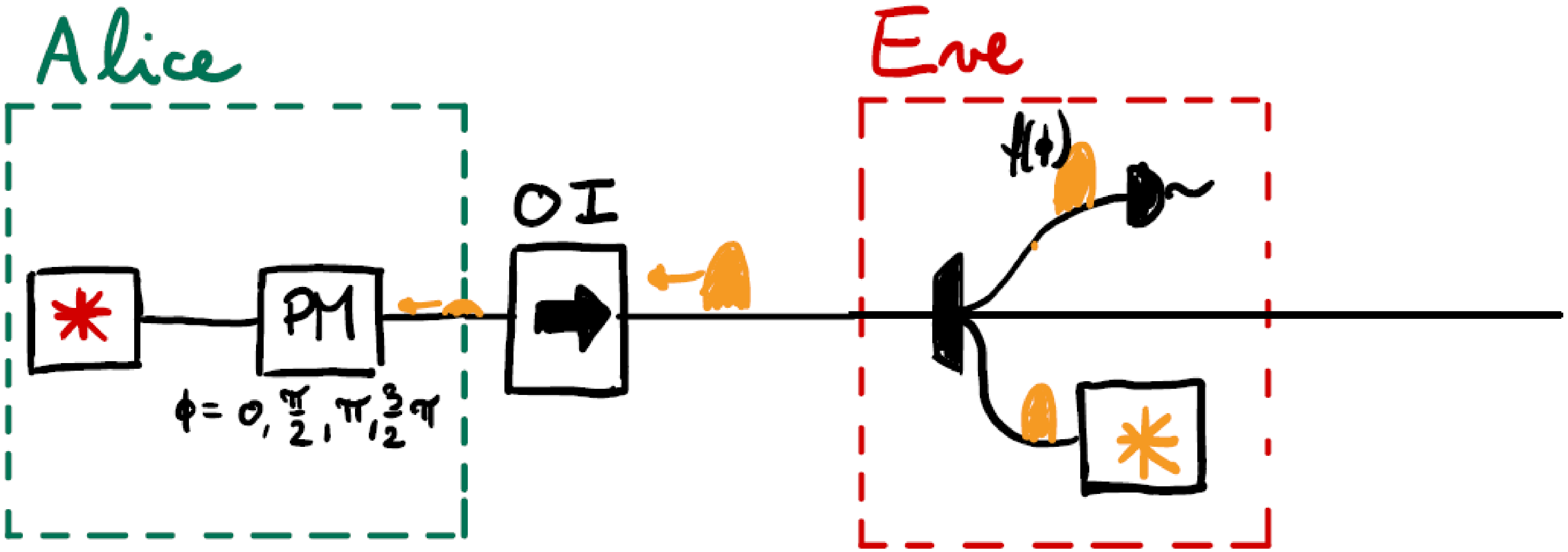
Trojan horse attacks



Eve sends light inside Alice lab.
Tries to steal information of the state preparation.

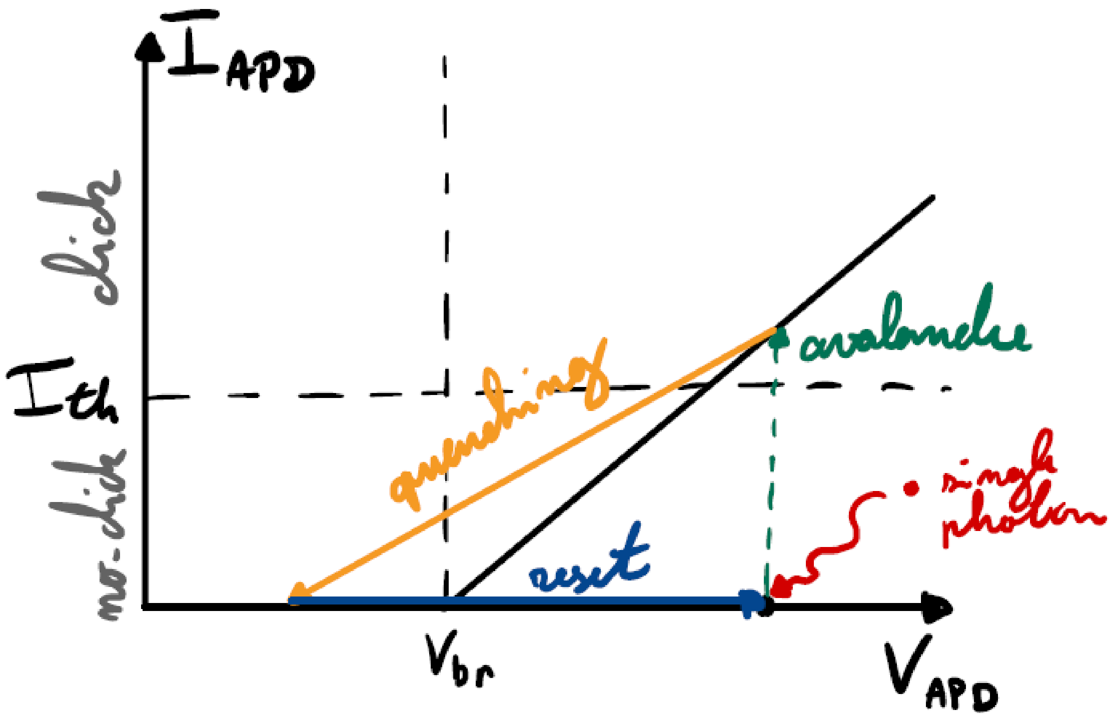
N. Gisin et al., Phys. Rev. A 73, 022320 (2006)

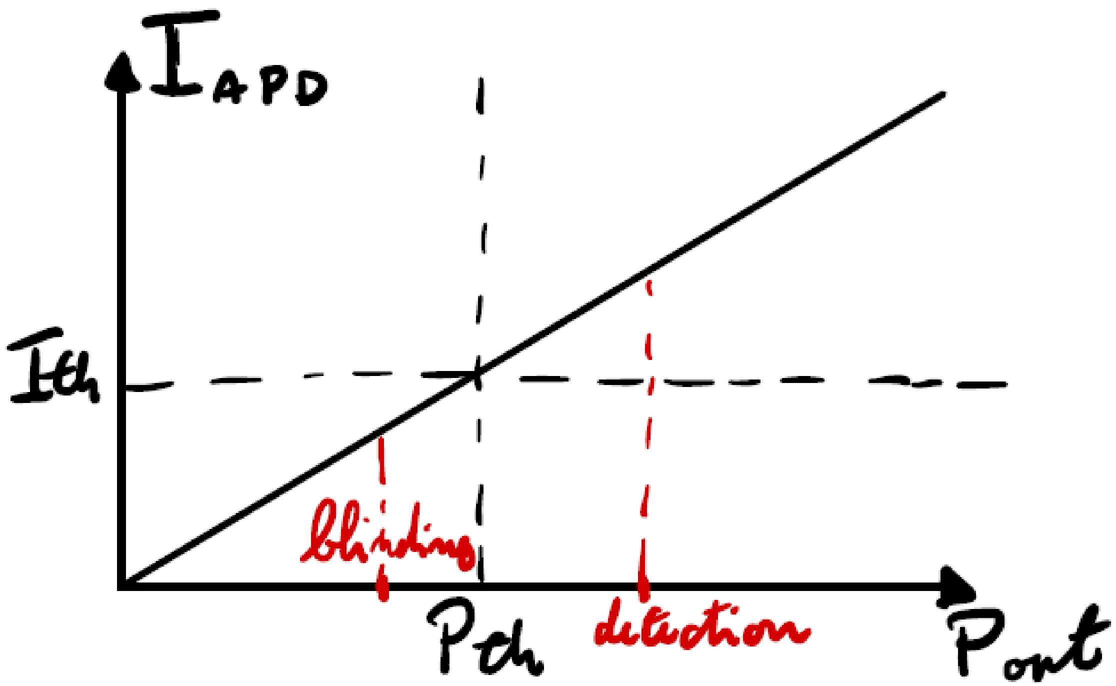
Trojan horse attacks



An easy countermeasure is using an optical isolator

Blinding Attacks

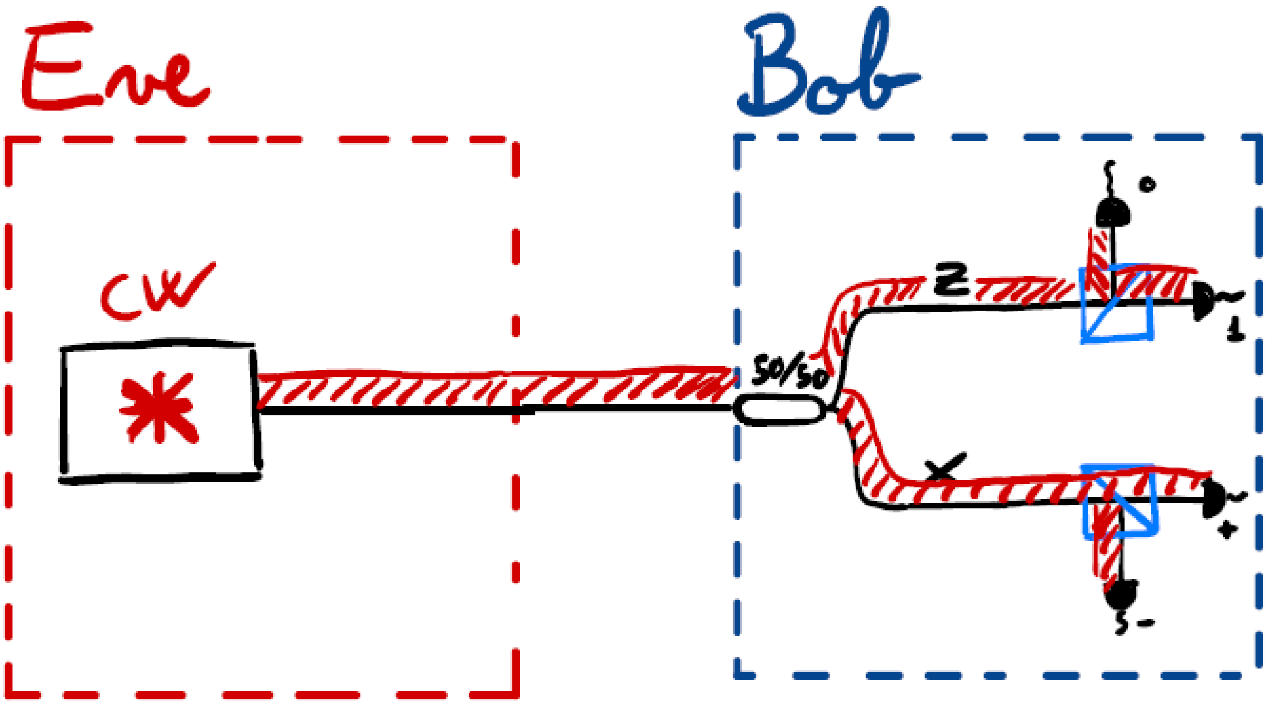




By shining continuous light in Bob’s detector, Eve can make the avalanche photodiodes work in a linear regime.

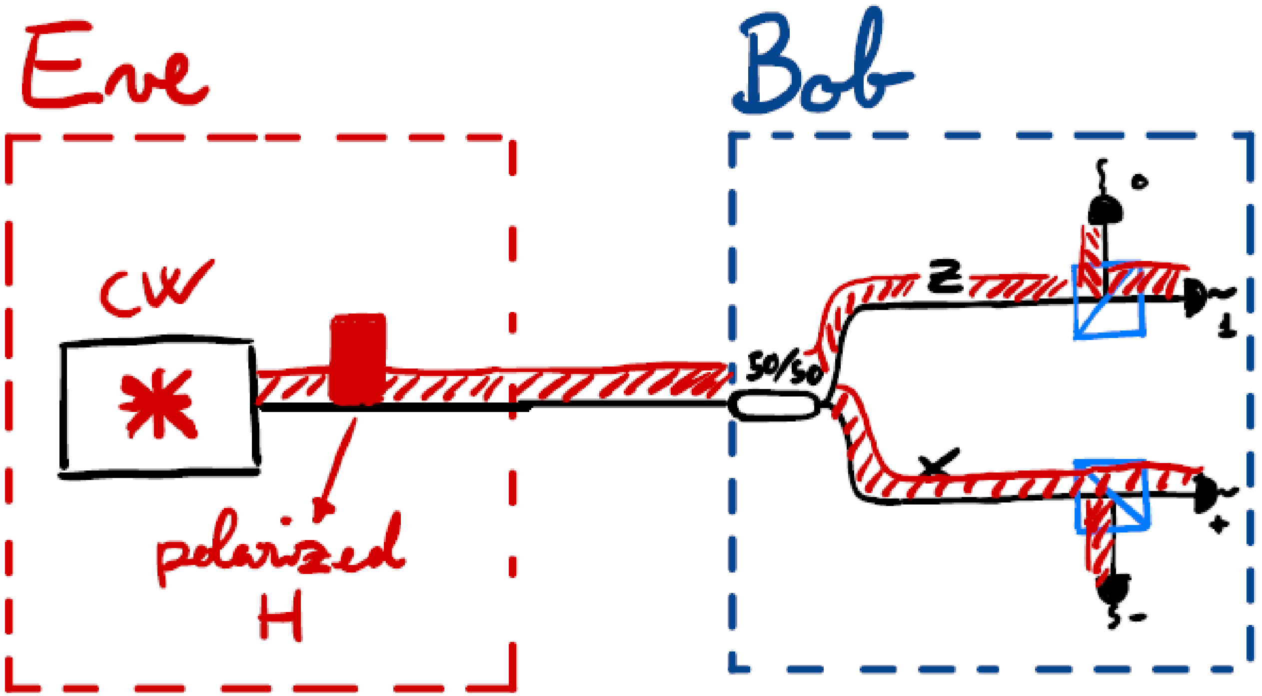
I. Gerhardt et al., Nat. Commun. 2, 349 (2011)

Blinding Attacks



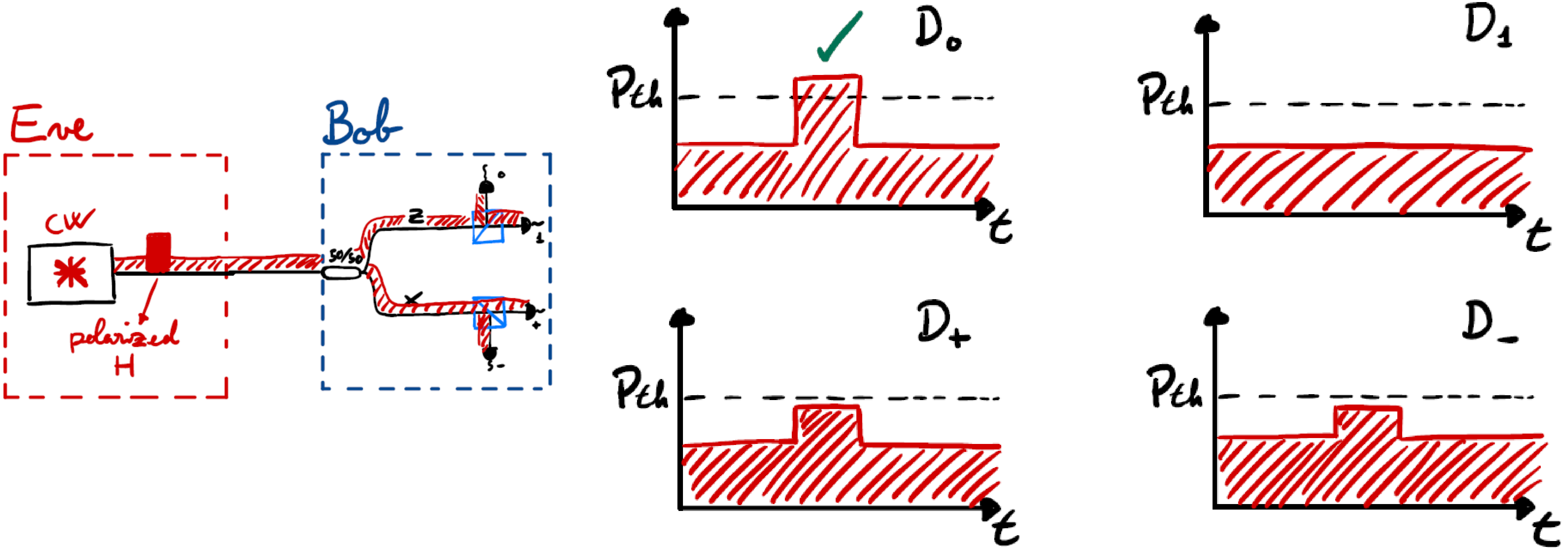
Eve shines circular polarized light in Bob detectors to blind them with the same power.

Blinding Attacks



By adding power in a chosen polarization, Eve can induce a detection in the respective detector.

Blinding Attacks



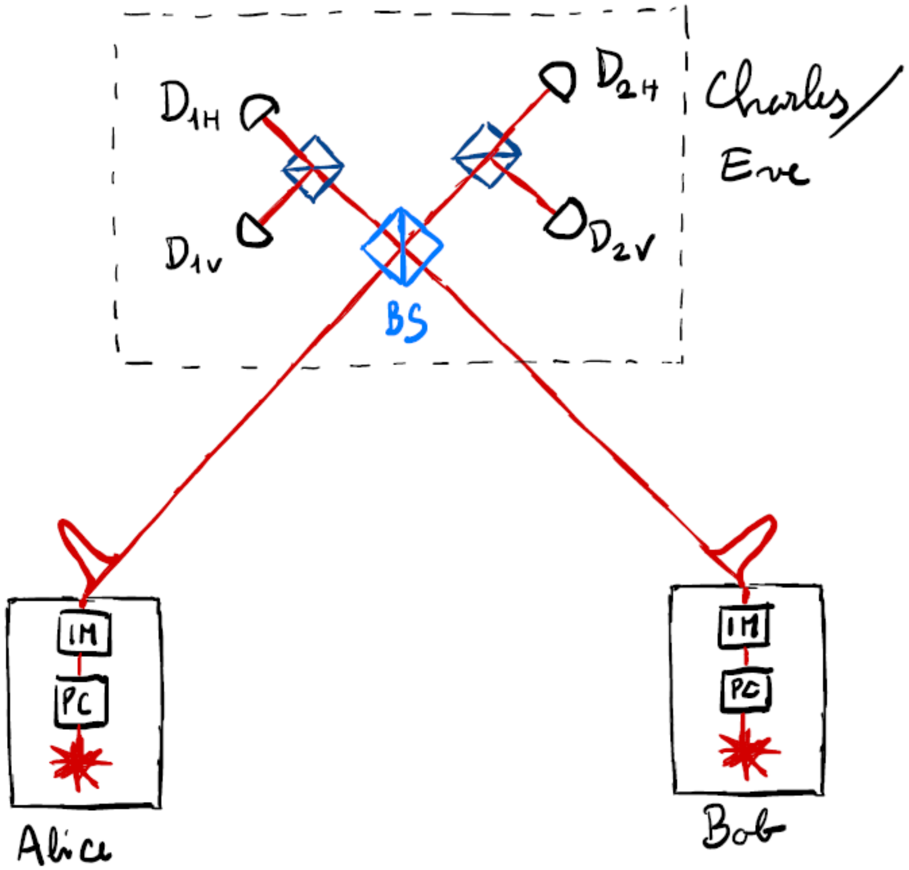
Blinding Attacks: possible countermeasures

- Power monitoring at Bob.
- Test of the single photon sensitivity.
- Active basis choice.
- Coincidence counting by redundancy of detectors.

Content

- Introduction
- Single Photon Prepare and Measure QKD
- Coherent states QKD
- Implementation a simplified DS-BB84
- Implementation security of QKD
- **Measurement device independent QKD**
    - **MDI QKD: two photon interference**
    - **Twin field QKD: single photon interference**

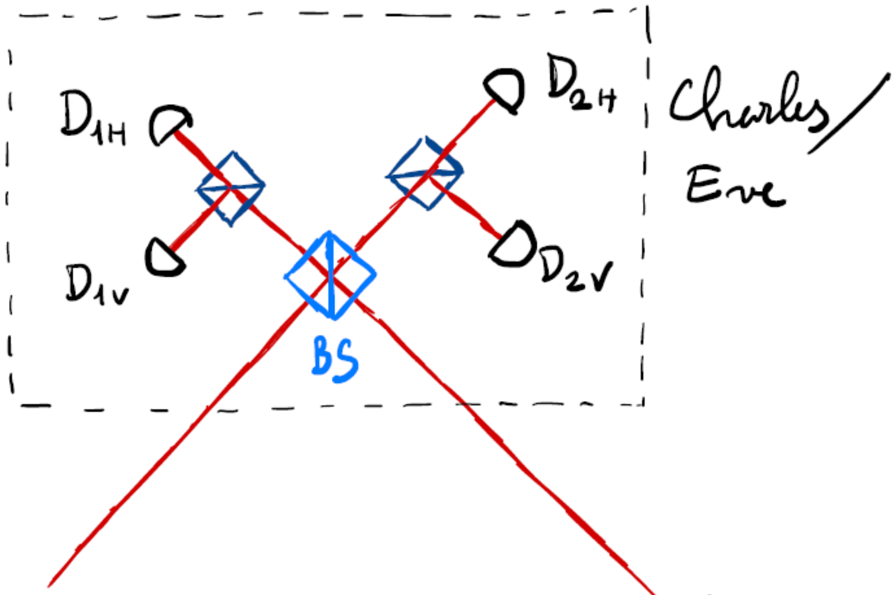
Measurement device independent-QKD



- The central node can be considered malicious.
- Requires a coincidence measure (at least two photons arriving)
- Scales with distance as a direct link QKD.
- It is more resilient against dark counts.

H.-L. Yin et al., Phys. Rev. Lett. 117, 190501 (2016)

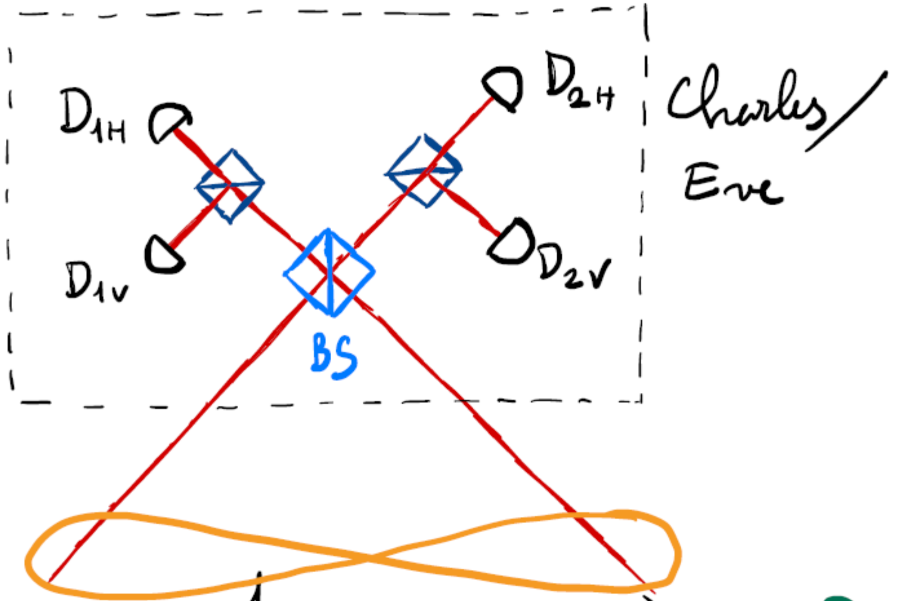
Measurement device independent-QKD



$$|0\rangle = |H\rangle$$
$$|1\rangle = |V\rangle$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

$$|0\rangle = |H\rangle$$
$$|1\rangle = |V\rangle$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Measurement device independent-QKD



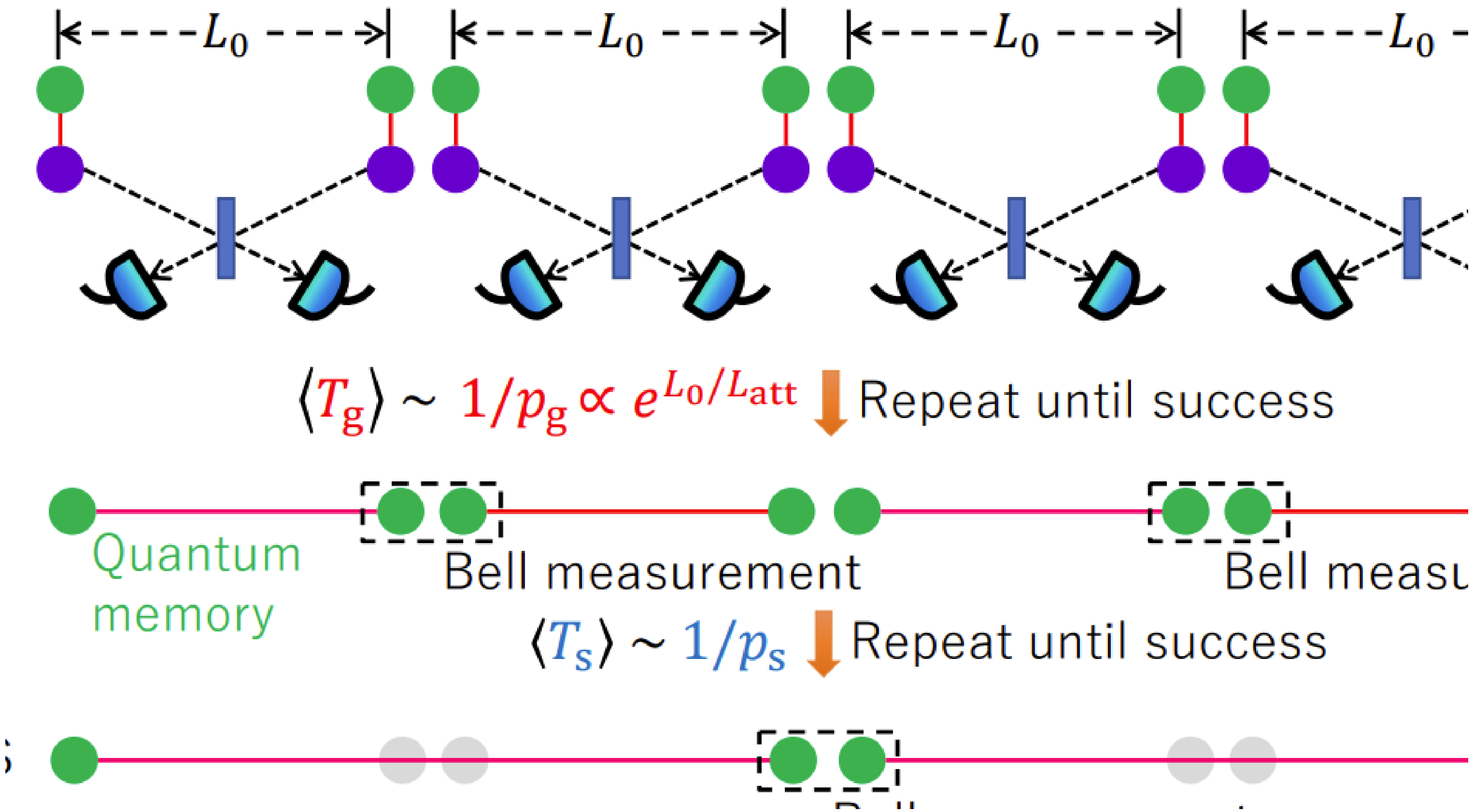
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle + |VH\rangle\right) \Rightarrow D_{1H}D_{1V} \text{ or } D_{2H}D_{2V}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right) \Rightarrow D_{1H}D_{2V} \text{ or } D_{2H}D_{1V}$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right) \rightarrow \emptyset$$

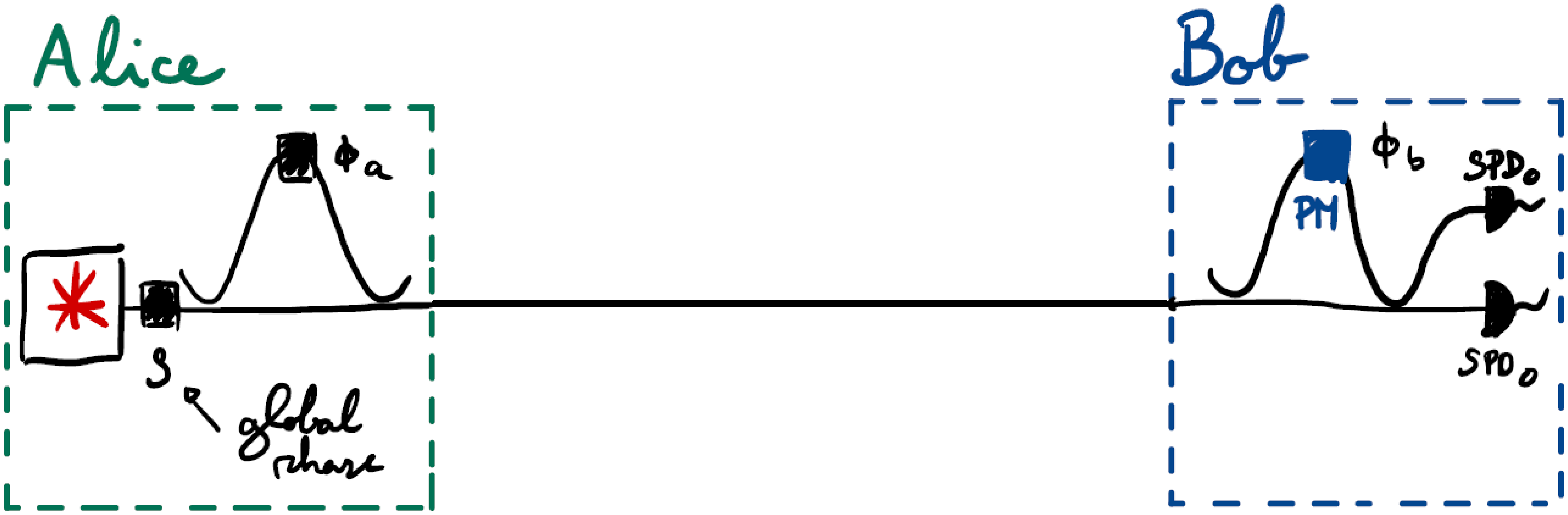
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle - |VV\rangle\right) \rightarrow \emptyset$$

Quantum repeaters for QKD

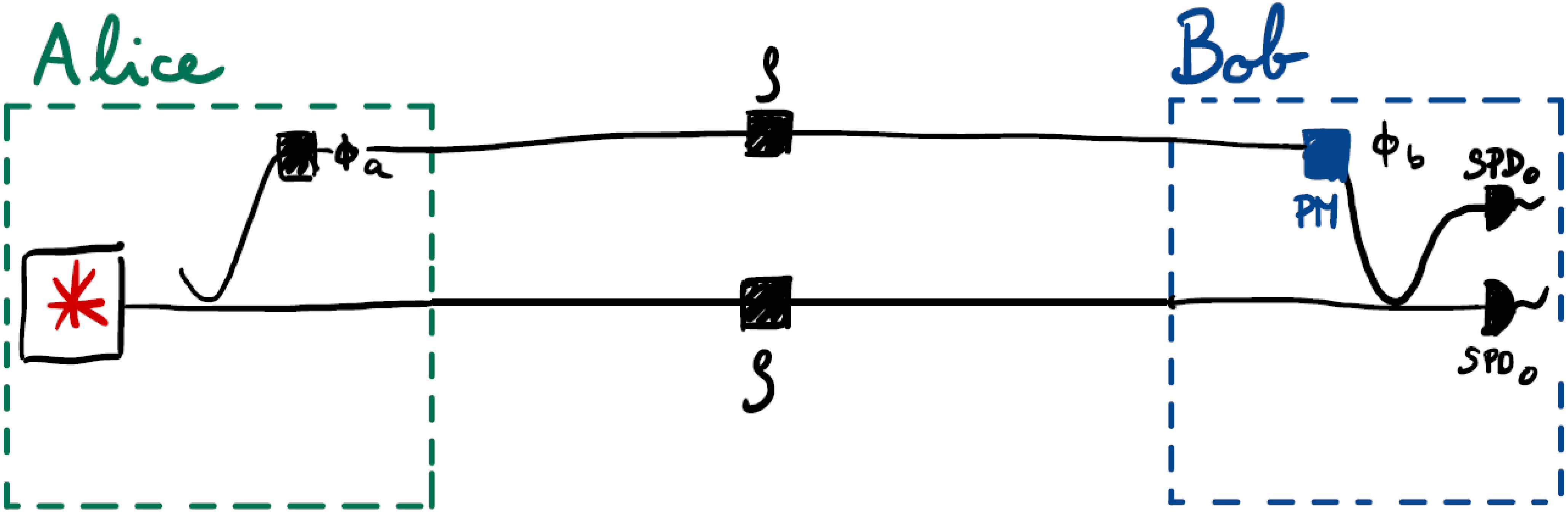


K. Azuma et al., Rev. Mod. Phys. 95, 045006 (2023)

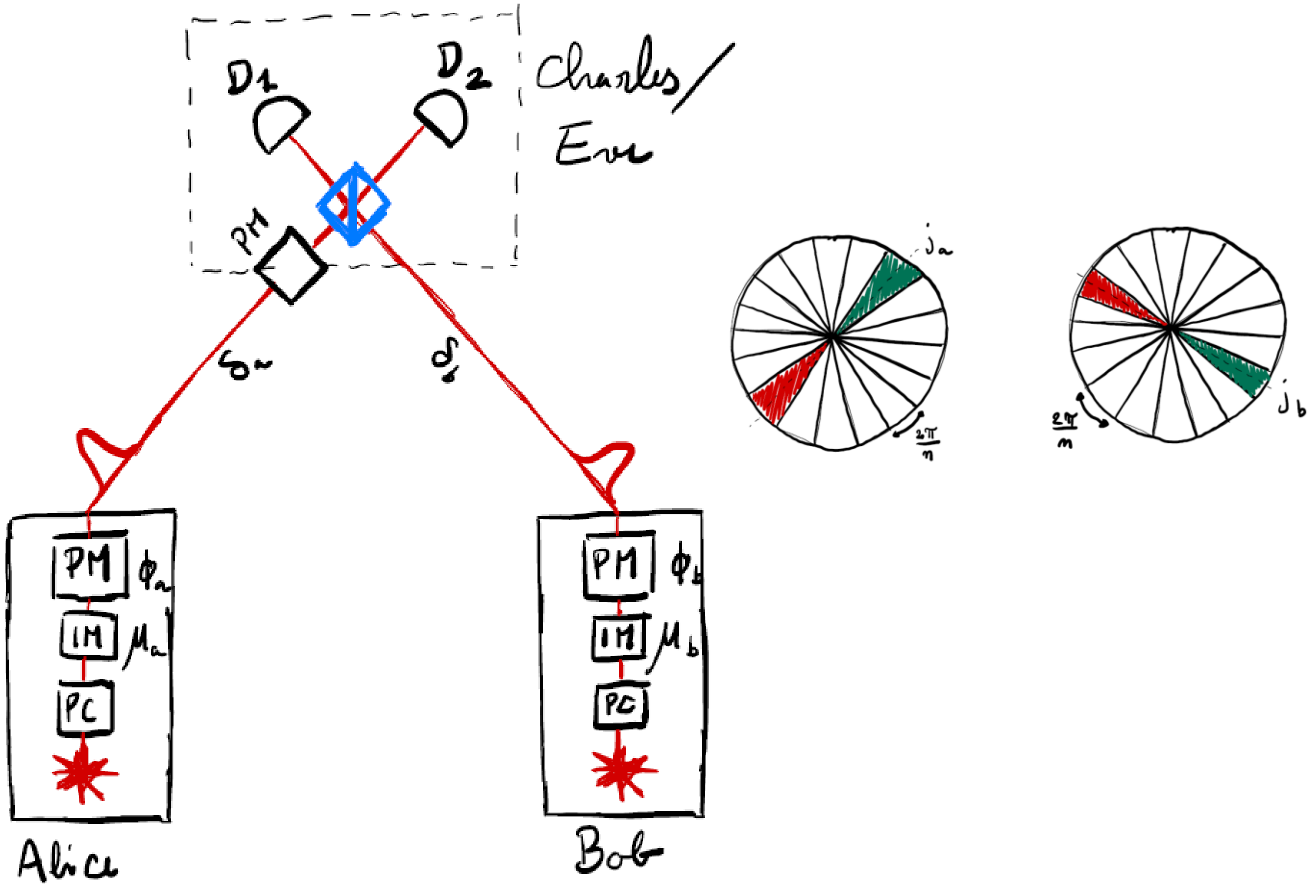
Repeater-less long distances



Repeater-less long distances



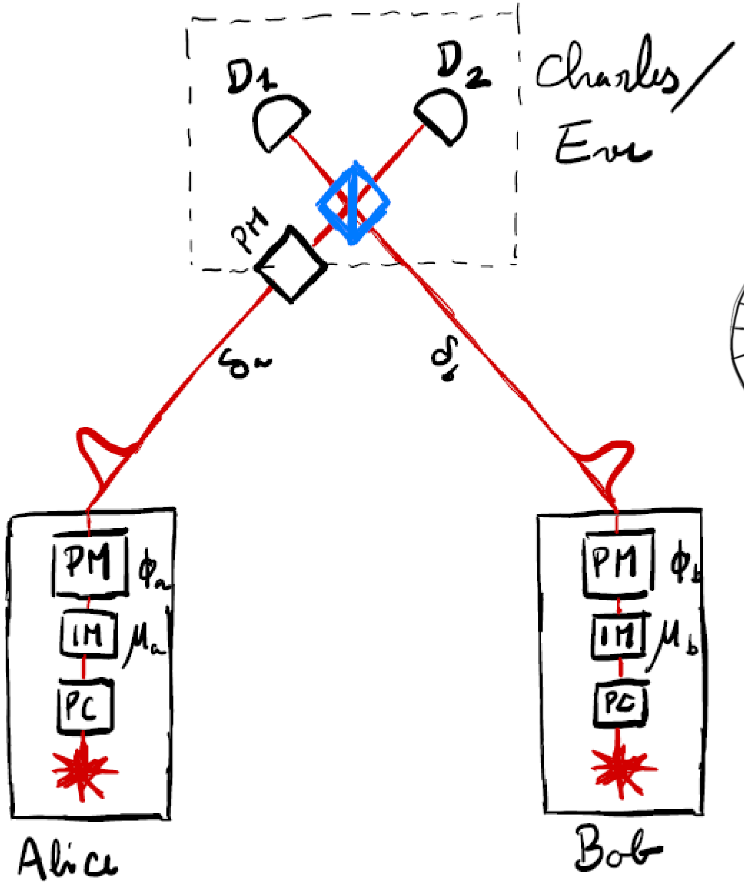
Twin-Field QKD

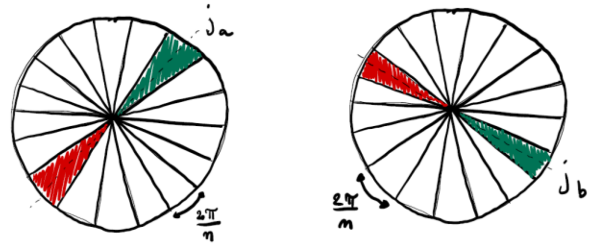


- The central node can be considered malicious.
- Requires a single photon measurement
- SKR scales as $\sqrt{loss}$
- It is complicated to implement due to the phase locking of the two remote lasers.

M. Pittalunga et al., Nat. Phot. 15, 530–535 (2021)

Twin-Field QKD





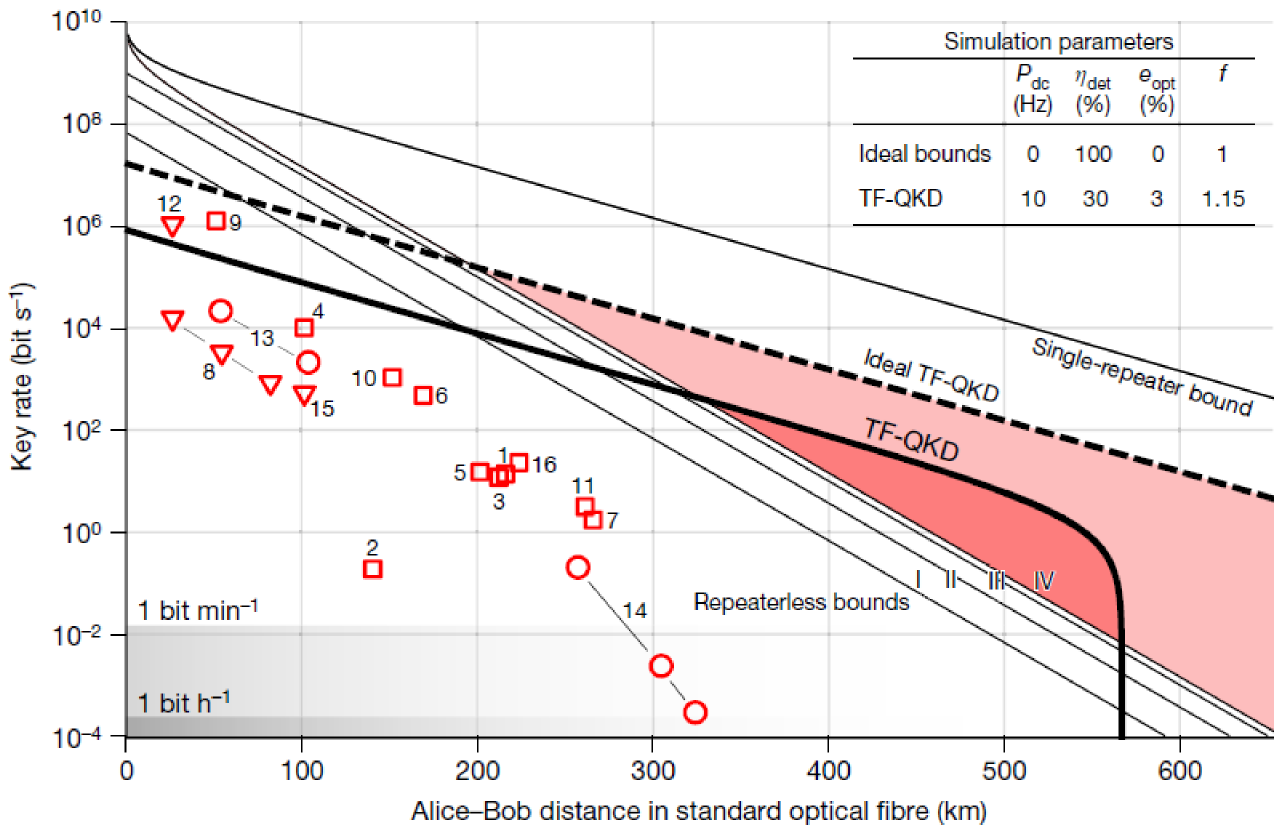
$$|0\rangle = |0\rangle$$

$$|1\rangle = a^{+}|0\rangle$$

$$|+\rangle = \frac{1}{\sqrt{2}}(1 + a^{+})|0\rangle$$

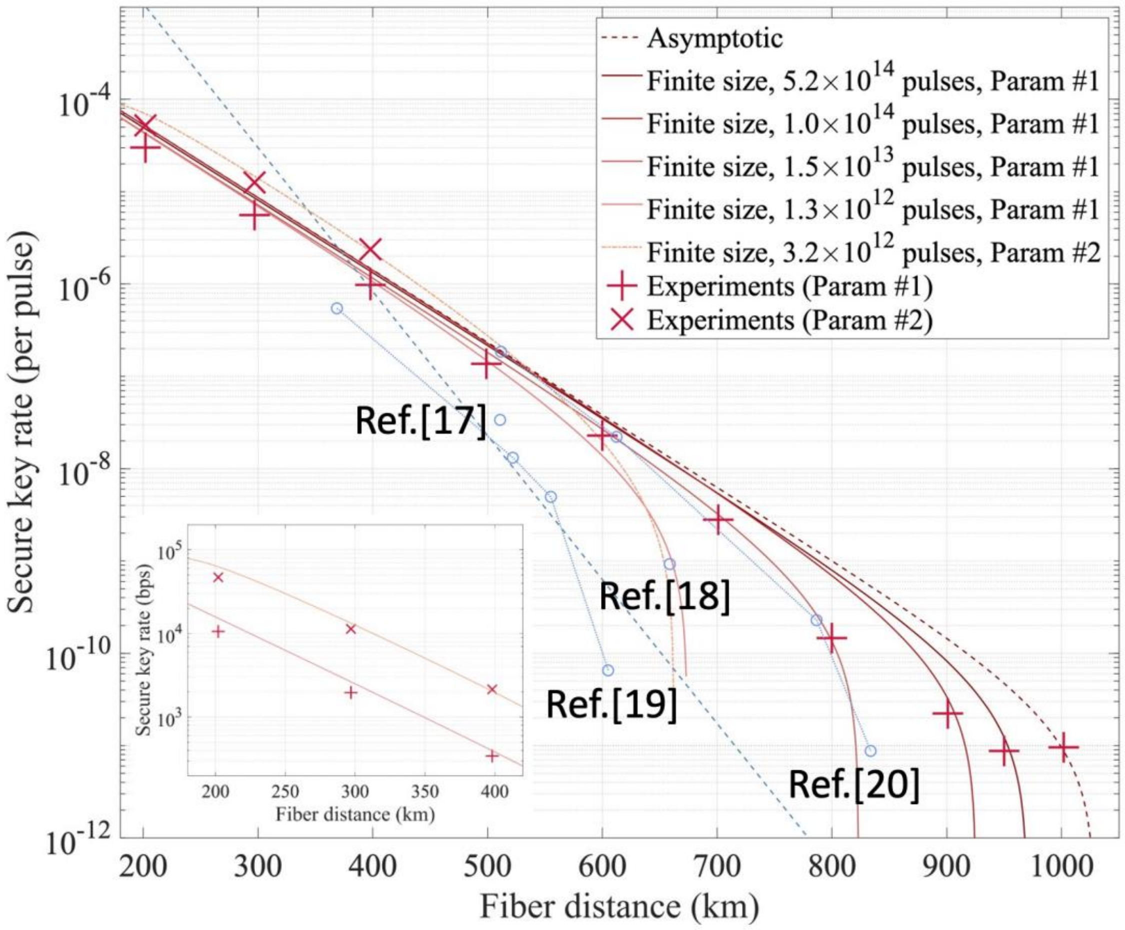
$$|-\rangle = \frac{1}{\sqrt{2}}(1 - a^{+})|0\rangle$$

Twin-Field QKD



M. Lucamarini et al., **Nature 557, pages 400–403 (2018)**

Twin-Field QKD



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

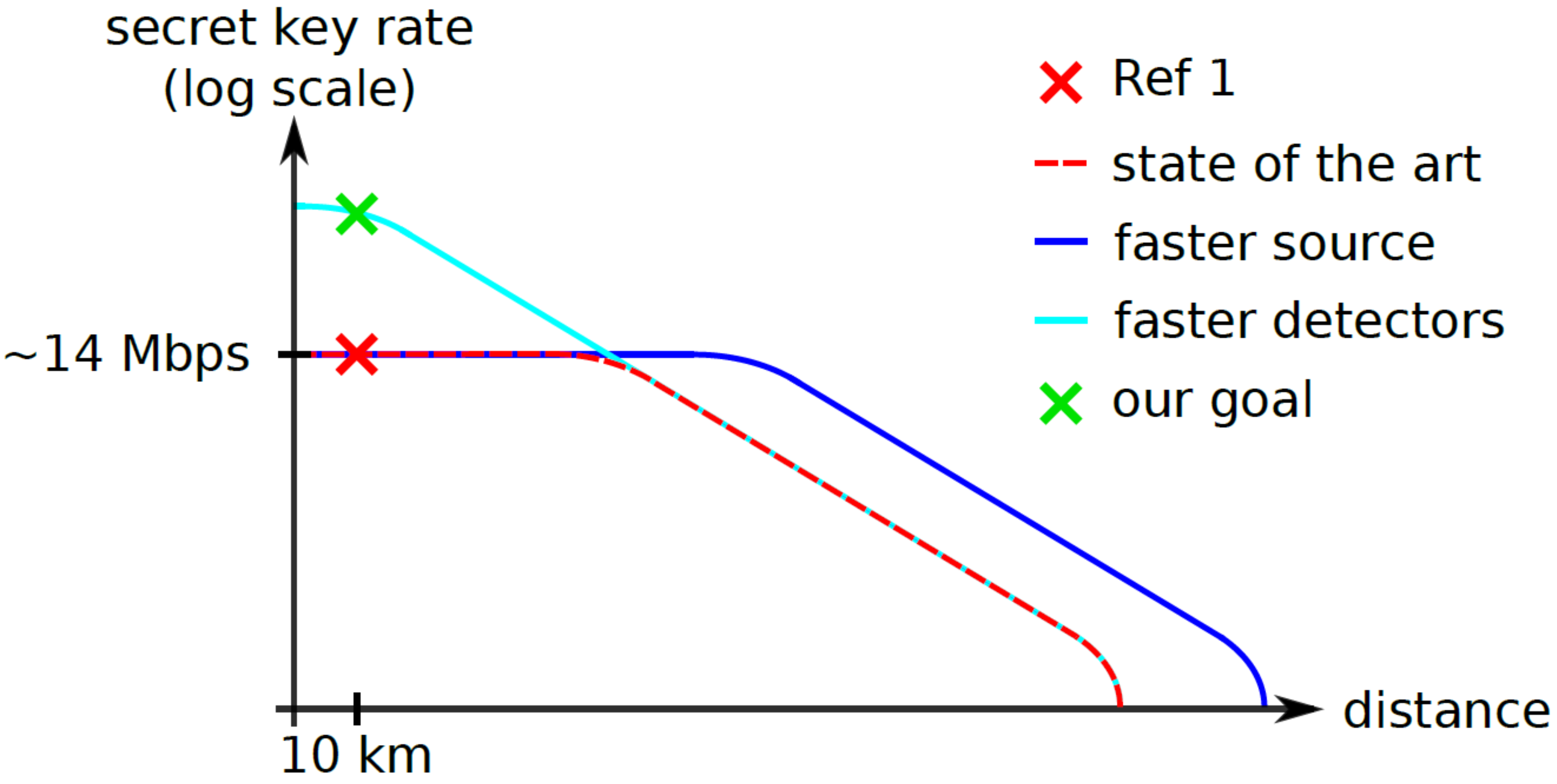
Summary

- We showed:
  - How a QKD protocol is structured (not only quantum but also classical post-processing).
  - How to use coherent states for QKD.
  - That protocol security does not correspond to implementation security.
  - Recent developments in the QKD technology

Bonus slides

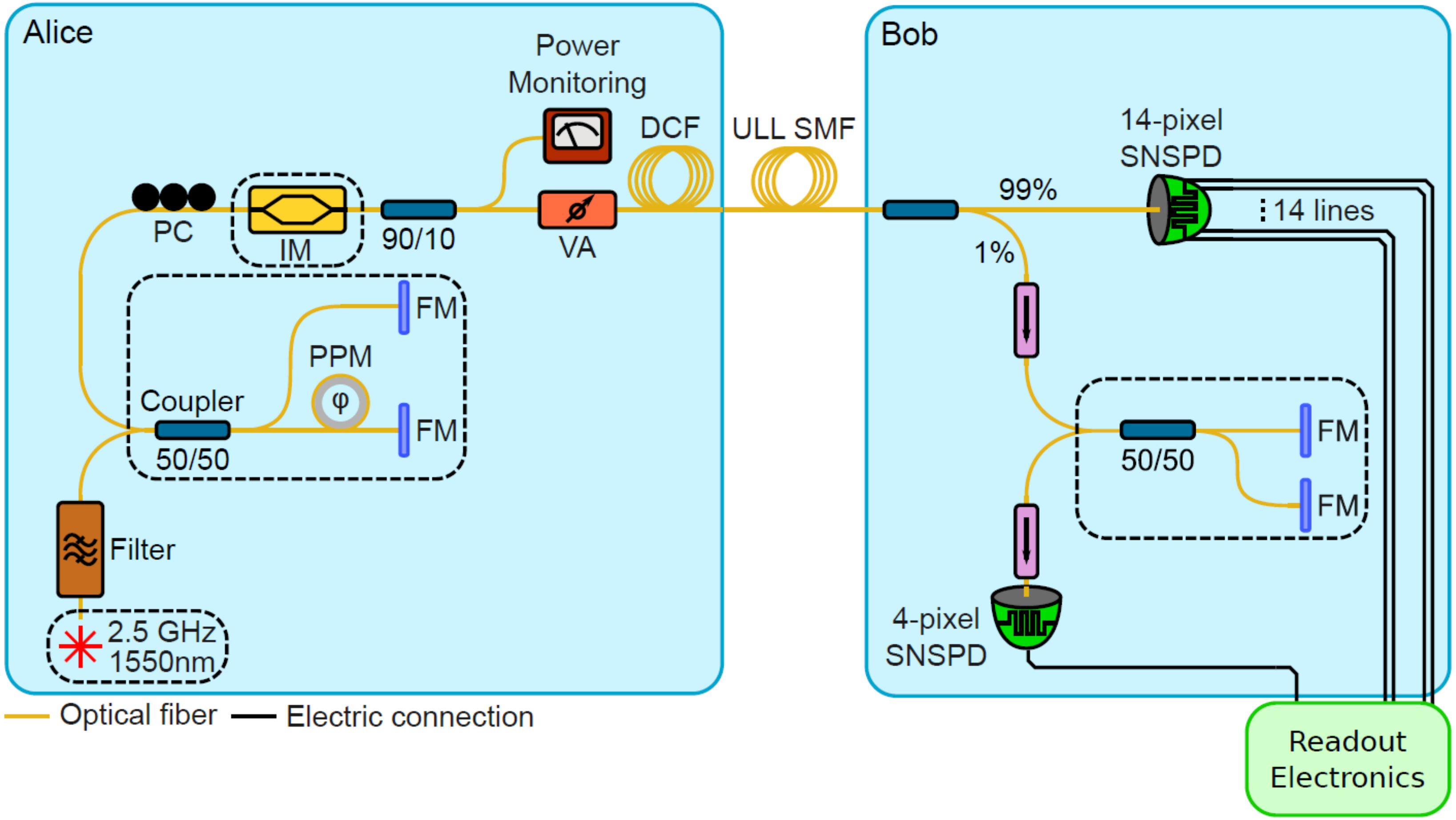
Fast quantum key distribution

Goal of the experiment

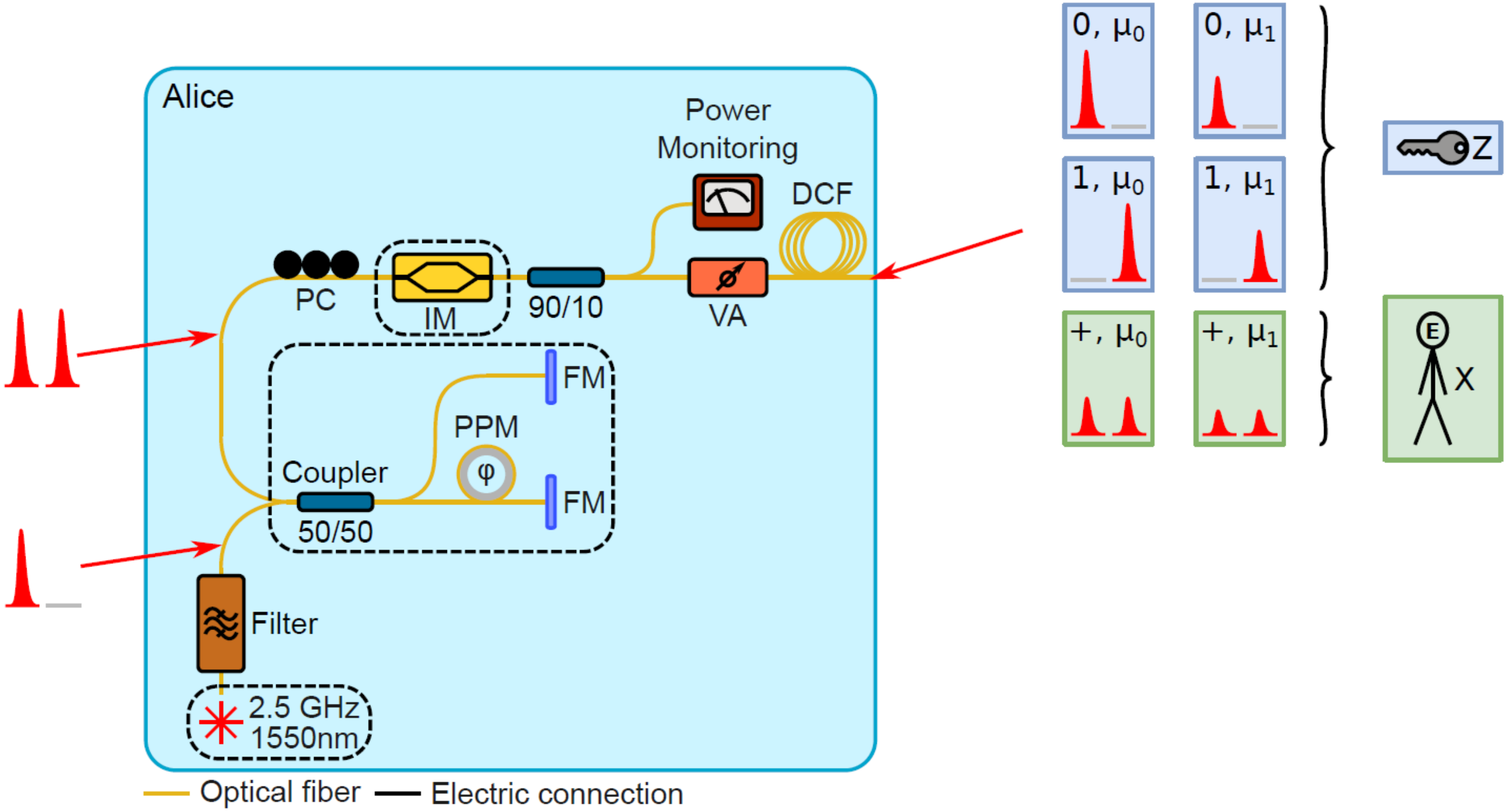


Z. Yuan et al.,Journal of Lightwave Technology, vol. 36, no. 16, pp. 3427-3433,(2018)

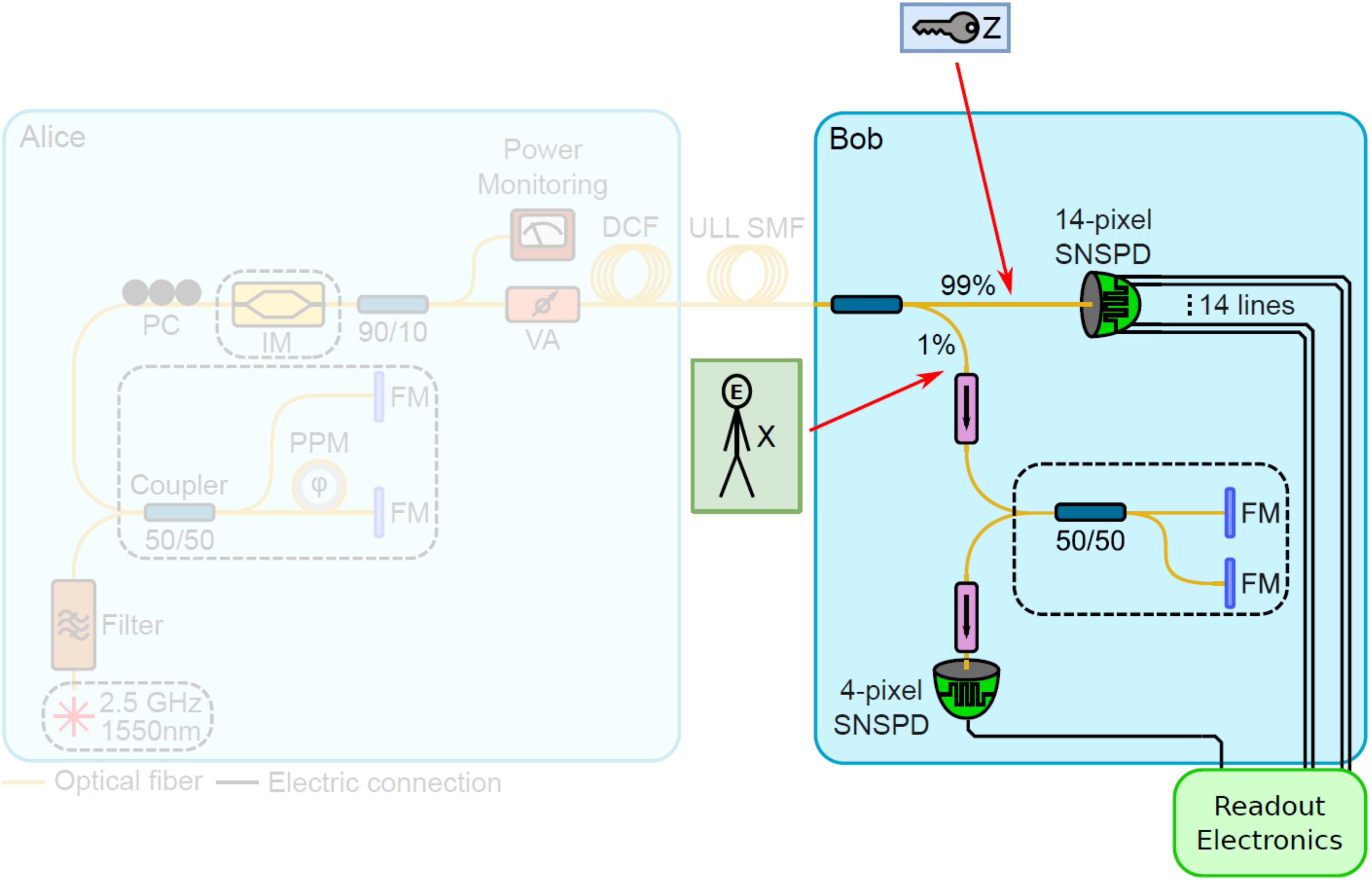
Setup


Alice
Power Monitoring
DCF
ULL SMF
PC
IM
90/10
VA
FM
PPM
φ
Coupler
FM
50/50
Filter
2.5 GHz
1550nm
Bob
14-pixel SNSPD
99%
14 lines
1%
50/50
FM
FM
4-pixel SNSPD
Readout Electronics
Optical fiber
Electric connection

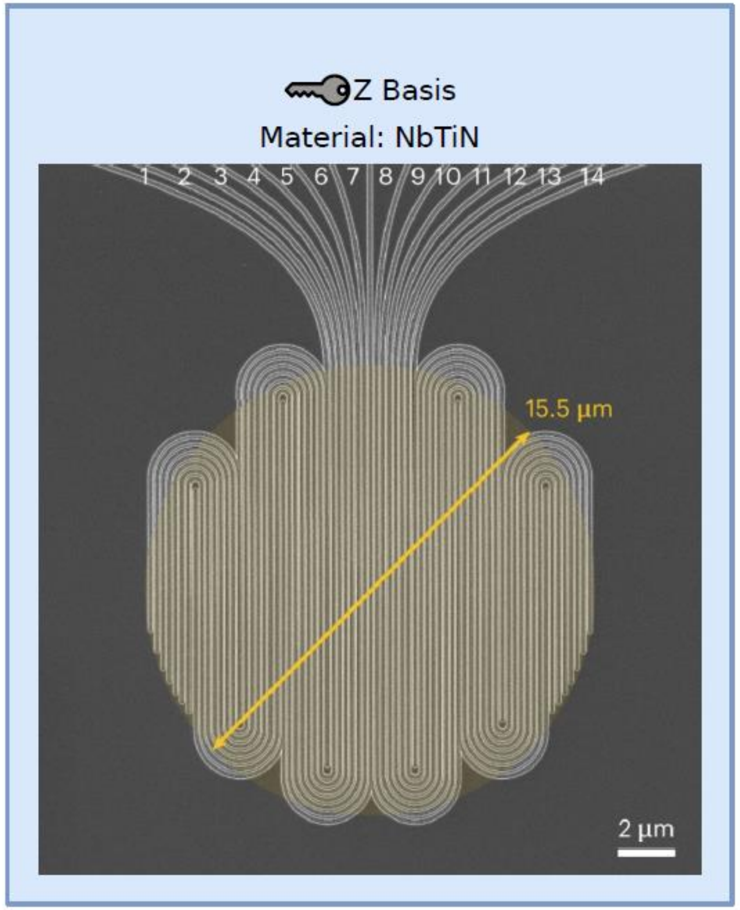
Setup


Alice
Power Monitoring
DCF
PC
IM
90/10
VA
FM
PPM
φ
Coupler
50/50
FM
Filter
2.5 GHz
1550nm
Optical fiber
Electric connection
0, μ0
0, μ1
1, μ0
1, μ1
+, μ0
+, μ1
Z
E
X

Setup


Z
Alice
Power
Monitoring
DCF
ULL SMF
PC
IM
90/10
VA
FM
PPM
Coupler
50/50
FM
Filter
2.5 GHz
1550nm
Optical fiber
Electric connection
Bob
14-pixel
SNSPD
99%
14 lines
1%
E
X
50/50
FM
FM
4-pixel
SNSPD
Readout
Electronics

SNSPD design



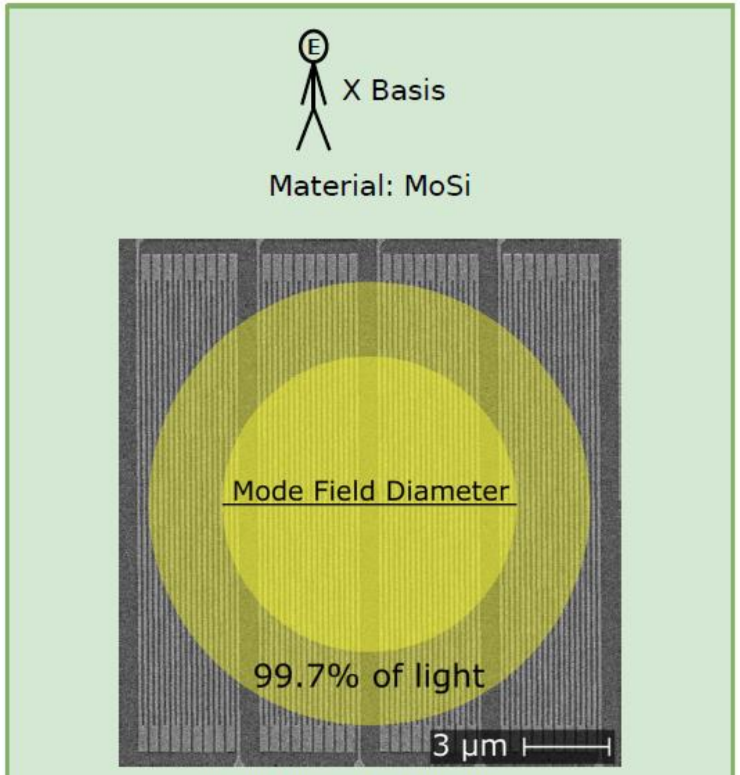


Image: Courtesy of Lorenzo Stasi

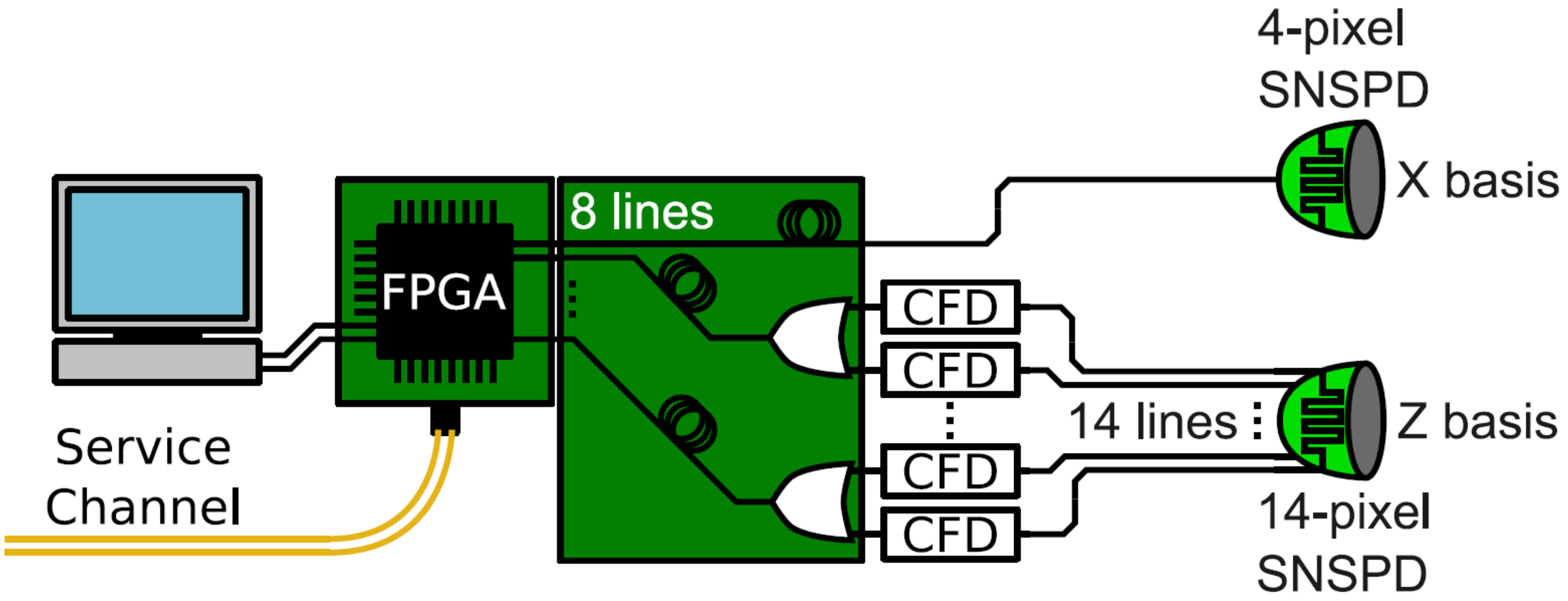
Z Basis:

- System detection efficiency = 0.65
- Jitter = 47 ps
- Count rate = 350 Mbps

X Basis:

- System detection efficiency = 0.82
- Jitter = 55 ps
- Count rate = 2.5 Mbps

Detection electronics



Secret key exchange

	Q_Z (%)	ϕ_Z (%)	sifted key rate (Mbps)	**SKR (Mbps)**
	0.3	1.0	7.8	**3.0**
	0.4	0.8	159.4	**63.6**